INFOSEC YEAR IN REVIEW 1997 to mid-2006

as of 2006-05-31

M. E. Kabay, PhD, CISSP-ISSMP
mkabay@norwich.edu

Assoc. Prof. Information Assurance
Program Director, BSc in Information Assurance
Division of Business Management

Program Director, MSc in Information Assurance
School of Graduate Studies
Norwich University

01 Introduction

Category 01 *Introduction*

2006-06-12 **Introduction**

M. E. Kabay, PhD, CISSP-ISSMP

WELCOME

Welcome to the June 2006 edition of the Information Security Year in Review (IYIR) project.

In 1993 and 1994, I was an adjunct professor in the Institute for Government Informatics Professionals in Ottawa, Canada under the aegis of the University of Ottawa. I taught a one-semester course introducting information security to government personnel and enjoyed the experience immensely. Many of the chapters of my 1996 textbook, _The NCSA Guide to Enterprise Security_ published by McGraw-Hill were field-tested by my students.

In 1995, I was asked if I could run a seminar for graduates of my courses to bring them up to date on developments across the entire field of information security. Our course had twenty students and I so enjoyed it that I continued to develop the material and teach the course with the NCSA (National Computer Security Association; later called ICSA and then eventually renamed TruSecure Corporation, its current name) all over the United States, Canada, Europe, Asia and the Caribbean.

After a few years of working on this project, it became obvious that saving abstracts in a WordPerfect file was not going to cut it as an orderly method for organizing the increasing mass of information that I was encountering in my research. I developed a simple database in 1997 and have continued to refine it ever since then. The database allows me to store information in an orderly way and -- most important -- to _find_ the information quickly. For that purpose, I put in as many keywords as I can think of quickly; I also classify each topic using a taxonomy that has grown in complexity and coverage over the years (more about the taxonomy in the next section).

In 2004, I was privileged to begin working with Norwich students Karthik Raman (project leader), Krenar Komoni and Irfan Sehic as my research assistants. These excellent students have provided invaluable assistance in transferring data from NewsScan, NIPC/DHS reports and other sources into the database and have also done the first cut of classification and keyword generation. They have enormously improved the coverage of the field and are continuing their work with me to expand the database to further sources in the coming year. It is difficult to estimate the hundreds of hours of time they have saved me.

I teach the IYIR course as a two-day workshop for my graduate students in the Master of Science in Information Assurance at Norwich University every June during their graduate week and then periodically during the year at different institutions as the occasion arises.

The IYIR reports are posted on my Web site now; see the introductory page at < http://www2.norwich.edu/mkabay/index.htm > and click on the IYIR button for a list of PDF files you can read on screen, search, or print out at will.

02 Taxonomy of INFOSEC Issues

Category 02 *Taxonomy of INFOSEC Issues*

2006-06-12 **Introduction**

INTRODUCTION

TAXONOMY

The taxonomy (classification scheme) of INFOSEC issues has grown over the years since I began the IYIR project. This taxonomy in now way represents a structurally sound classification with unambiguous, non-overlapping, atomic concepts; it is simply an organic development of my wish to present information in an orderly way in my courses and to be able to find examples of specific issues when I need them for teaching or writing.

The taxonomy changes almost every time I use it; the current taxonomy is listed here and is used throughout this edition of the IYIR report as well as in the INFOSEC UPDATE course based on the IYIR.

Code Description
0 Unclassified
01 Introduction
02 Taxonomy of INFOSEC Issues
03 Sources of Information
04 Copyright
05 Using IYIR
06 The INFOSEC UPDATE Course
07 Acknowledgements
08 About the Editor
10 Computer Crimes (cases, indictments, convictions, sentences)
11 Breaches of confidentiality
11.1 Data leakage
11.2 Unauthorized disclosure
11.3 Data theft
11.4 Covert channels
12 Wiretapping, interception (not jamming; not govt/law enforcement)
12.1 Wiretapping
12.2 Interception
12.3 Injection
13 Data diddling, data corruption, embezzlement
13.1 Data diddling
13.2 Data corruption & destruction
13.3 Embezzlement
13.4 Obsolescence
14 Viruses, virus-hoaxes, Trojans (assembly level or macro: not ActiveX or Java)
14.1 Viruses
14.2 Worms
14.3 Virus/worms
14.4 Trojans
14.5 Virus hoaxes
15 Fraud (not embezzlement), extortion, slamming
15.1 Fraud
15.2 Extortion
15.3 Slamming
16 INFOWAR, industrial espionage, hacktivism
16.1 Industrial espionage
16.2 Industrial information systems sabotage
16.3 Infrastructure protection & homeland security
16.4 Military & government perspectives on INFOWAR
16.5 Hacktivism
16.6 Disinformation, PSYOPS
17 Penetration, phreaking, cramming, uncapping (entering systems, stealing telephone or other services)
17.1 Penetration
17.2 Web vandalism
17.3 Phreaking, cramming, uncapping, theft of services
18 Theft/loss of equipment (laptops, ATMs, computers, cables, network components)
18.1 Theft of equipment
18.2 Loss of equipment

19 Counterfeits, forgery (including commercial software/music piracy)
19.1 Software piracy
19.2 Music piracy
19.3 Movies / TV piracy
19.4 Books / e-books piracy
19.5 Games piracy
19.6 Counterfeit currency, credit-cards, other negotiable tokens
19.7 Counterfeit legal or business documents
19.8 Plagiarism
19.9 Counterfeit products (hardware, clothing etc.)
1A Criminal hacker scene (conventions, meetings, testimony, biographies, publications)
1A1 Criminal hacker conventions and meetings
1A2 Criminal hacker testimony in court or committees
1A3 Biographical notes on individual criminals (including arrests, trials)
1A4 Criminal hacker publications
1A5 Criminal hacker organizations
1A6 Criminal hacker psychology
1B Pornography, Net-harm, cyberstalking, gambling, online auctions
1B1 Adult pornography
1B2 Child pornography
1B3 Pedophilia, kidnapping, Net-adoption fraud
1B4 Stalking & harassment
1B5 Gambling
1B6 Auctions
1B7 Hate groups, speech
1B8 Traffic in women, slavery
1B9 Non-virus hoaxes, urban myths
1C Identity, impersonation, spoofing
1C1 Impersonation
1C2 Identity theft
1C3 Pseudonymity
1C4 Anonymity
1C5 Phishing
1D Law Enforcement & Forensics (technology, organizations, proposals, litigation, rulings, judgements)
1D1 Organizations, cooperation for law enforcement
1D2 Technology for law enforcement
1D3 Litigation, legal rulings, judgements affecting law enforcement
1D4 Government funding for law enforcement
1E Homeland Security
20 Emerging Vulnerabilities & Defenses
21 Quality assurance failures including design flaws
21.1 General QA failures
21.2 Security product QA failures
21.3 Embedded processors
21.4 SCADA (supervisory control and data acquisition) systems, vehicle controls
21.5 Robots
22 Availability problems
22.1 DoS attacks
22.2 DDoS attacks
22.3 DoS countermeasures
22.4 Accidental availability disruptions
23 Internet tools
23.1 Java
23.2 Javascript
23.3 ActiveX
23.4 HTML, XML
23.5 E-mail & instant messaging or chat
23.6 Web-site infrastructure, general Web security issues
23.7 VoIP
23.8 SMS
24 Operating systems, network operating systems,TCP/IP problems (alerts & improvements)
24.1 Windows 9x/Me
24.2 Windows NT/2K/XP
24.3 UNIX flavors
24.4 TCP/IP, HTTP, DNS
24.5 LAN OS

24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax
24.7 SWDR (Software-defined radio)
24.8 MAC OS
24.9 Peer-to-peer networking
24.A Secure processors
24.B Robust systems (hw / sw)
25 Computer remote control & disruption
25.1 Remote control, RATs, reprogramming, auto-updates
25.2 Jamming
25.3 RFI, HERF, EMP/T
26 Health effects of electronic equipment (phones, screens, etc.)
26.1 Radiation
26.2 Toxic materials
26.3 Heat
27 Security tools
27.1 Vulnerability assessment
27.2 Port scans
27.3 Intrusion detection systems
27.4 Firewalls & other perimeter defenses
27.5 Honeypots
27.6 Honeynets
27.7 Anti-malware technology
28 Automated surveillance
28.1 Spyware, Web bugs & cookies
28.2 Scumware
28.3 Keystroke loggers
28.4 Cell/mobile phones/GPS/cameras
28.5 Serial numbers
28.6 RFID tags
29 Sociology of cyberspace
29.1 Addiction, games & violence
29.2 Cyberdating & cybersex
29.3 Digital divide
29.4 Online & electronic voting
29.5 Online legal proceedings
29.6 Flash crowds, social e-links
29.7 Outsourcing
30 Management & Policy
31 The state of information security & technology
31.1 Surveys, studies, audits of security
31.2 Estimates, guesses, predictions, forecasts concerning security
31.3 New technology with security implications
31.4 Outsourcing
32 Censorship, indecency laws, 1st amendment (law)
32.1 Censorship in the USA
32.2 Censorship outside the USA
33 Policies, risk analysis, risk management
33.1 Acceptable use policies
33.2 Spam, spim, spit & splogs
33.3 Antispam
33.4 Authorization, access controls
33.5 Risk analysis & management
34 Net filters, monitoring (technologies)
34.1 Net filters
34.2 Usage monitoring, audit trails (employees, children)
35 DNS conflicts, trademark violations (Net, Web)
35.1 Cybersquatting
35.2 Trademarks vs DNS
35.3 Politics of the DNS
36 Responses to intrusion
37 Education in security & ethics
37.1 Elementary & middle school
37.2 High school
37.3 Undergraduate degrees
37.4 Master's degrees
37.5 Doctoral degrees

37.6 Industry courses
37.7 Conferences
37.8 Web sites
37.9 White papers
38 Consumer/employee privacy, profiling, trade in personal information
38.1 Consumer profiling
38.2 Trade in personal information
38.3 Industry efforts for privacy protection
38.4 International agreements on security, privacy, Net law
38.5 EU legislation & regulation concerning privacy
38.6 US legislation & regulation concerning privacy
38.7 Other legislation & regulation concerning privacy
38.8 Law enforcement & privacy
38.9 Surveillance
38.A Medical / HIPAA
40 Defensive Technology, Law of E-commerce, Intellectual Property
41 Cryptanalysis techniques & tools
42 Crypto algorithms (weakness, brute-force attacks, implementation flaws)
42.1 Crypto algorithm weaknesses
42.2 Brute-force attacks
42.3 Crypto product implementation flaws
43 I&A products (tokens, biometrics, passwords, Kerberos)
43.1 Tokens
43.2 Biometrics
43.3 Passwords
43.4 Kerberos
43.5 Single sign-on
43.6 E-mail authentication (e.g., SPF & SenderID)
44 Encryption algorithms, products (including steganography)
44.1 Crypto algorithms
44.2 Crypto products
44.3 Steganography
45 E-commerce security, digital signature, products, digital cash, e-payments
45.1 PKI (Digital signatures / certificates)
45.2 Digital cash
45.3 Micropayments
45.4 E-payments / e-wallets / credit-cards
45.5 Watermarks / digital-rights management / copy protection
45.6 Smart cards and other e-commerce security measures
45.7 Sales taxes on Internet commerce
45.8 E-commerce laws
45.9 E-shopping carts
46 Cryptography exports from US; Key escrow
47 US computer-crime laws
48 Foreign cyberlaws (not cases or sentences)
48.1 Non-US cryptography laws
48.2 Non-US computer-crime laws
48.3 Non-US intellectual property laws
49 Privacy, government surveillance, legislation, agreements
4A Evolution of Net law: framing, pointing, linking, jurisdiction
4A1 Framing
4A2 Pointing, linking, deep linking, metatext
4A3 Jurisdiction
4A4 Blocking
4A5 Archives
4A6 Libel
4A7 Spam
4A8 Liability
4B Intellectual property: patents, copyrights (law)
4B1 Copyrights
4B2 Patents
4B3 Reverse engineering
4B4 EULA (End-user license agreements)
4B5 Trademarks
4C Security paradigms, risk management, site-security certification, professional certification
4C1 Paradigms, security standards

4C2 Risk management methodology & tools
4C3 Certification of site security, privacy protection
4C4 Professional certification in security, auditing
4C5 Academic/Industry/Vendor/Govt efforts
4D Funny / miscellaneous

03 Sources of Information

Category 03 *Sources of Information*

2006-06-12 **Introduction**

INTRODUCTION

In the early days, I wrote all the abstracts myself. As the size of the database grew, this practice became a terrible and limiting burden. I was thrilled -- and still am -- to get permission to quote the superb abstracts written by John Gehl and Suzanne Douglas, original editors of EDUPAGE and now of the daily _NewsScan_ and weekly _Innovation_ e-publications. At this point, their work is a major component of the IYIR.

In addition, I have been quoting (with attribution) many of the contributors to Peter G. Neumann's RISKS Forum Digest. I regret that I have fallen behind in summarizing this publication since about 2004 but hope to get back on track with the help of volunteers and assistants.

Lately, the Daily Reports from NIPC (National Infrastructure Protection Center) (now the DHS daily report) have proven valuable in supplementing the material at hand.

Bruce Schneier, famed cryptographer and a valued commentator on all matters of security, has kindly allowed me to include excerpts from his monthly columns in his Crypto-Gram newsletter.

I also naturally continue to write my own abstracts of interesting articles when necessary.

For a list of news sources that cover information security news, see < http://www2.norwich.edu/mkabay/overviews/infosec_ed.pdf >.

For more information about NewsScan and Innovation, see < http://www.newsscan.com >.

For more information about RISKS Forum Digest, see the archives at <http://catless.ncl.ac.uk/Risks/ > for HTML versions or at < http://the.wiretapped.net/security/textfiles/risks-digest/ > for text versions.

Dr Neumann asks that reprints from RISKS include the following note and the following should be considered as a blanket notification for all verbatim republication of RISKS materials throughout this database:

* * *
From the
FORUM ON RISKS TO THE PUBLIC IN COMPUTERS AND RELATED SYSTEMS (comp.risks)
ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator
See < http://www.csl.sri.com/users/risko/risksinfo.html > for full information.
Reused without explicit authorization under blanket permission granted for all Risks-Forum Digest materials. The author(s), the RISKS moderator, and the ACM have no connection with this reuse.
* * *

Information Security Magazine is at < http://www.infosecmag.com > and subscriptions to the Security Wire Digest are available through < http://infosecuritymag.bellevue.com >.

The NIPC Daily Report is available through < http://www.nipc.gov/ >.

For free subscriptions to Bruce Schneier's Crypto-Gram, see < http://www.counterpane.com/crypto-gram.html >.

04 Copyright

Category 04 *Copyright*

2006-06-12 **Introduction**

INTRODUCTION

As you can see at the bottom of every page of the IYIR report and the INFOSEC UPDATE, I assert copyright over this presentation (only) of the information my research team and I have collected. This is called a _compilation copyright_ and in no way derogates the copyrights of all original copyright holders. My contribution is primarily the organization and presentation of this information. I do hold the copyright on my own abstracts and on the keywords. I assert copyright purely to prevent scoundrels from SELLING what is supposed to be available FREE. The PDF version of the book you are looking at will be posted on my Web site for anyone to use.

05 Using IYIR

Category 05 *Using IYIR*

2006-06-12 **Introduction**

INTRODUCTION

Anyone who wants to refer to these IYIR and INFOSEC UPDATE documents is completely welcome to do so freely _provided_ that no one tries to make other people pay for the materials. You are welcome to reprint the documents provided that each page you choose to print is in the original format (that's why I use Acrobat PDF files to distribute the information). Just remember, if I ever find out that someone has charged somebody for what I freely give away I am going to be really, really mad!

You may, of course, use the _original_ documents as you and the copyright owners agree.

As for posting these files on your own Web sites, DON'T! I update the files constantly and absolutely do not want to have to hunt down old copies of the work and replace them with newer versions. So you're welcome to link to the files, but please do _not_ copy them to any other Web sites.

06 The INFOSEC UPDATE Course

Category 06 *The INFOSEC UPDATE Course*

2006-06-12 **Introduction**

INTRODUCTION

The INFOSEC UPDATE course is usually a two-day workshop that brings participants up to date on topics across the entire field of information security. The four half-day sessions cover the following broad areas:

Day 1:
AM: Computer Crime Update
PM: Emerging Vulnerabilities

Day 2:
AM: Management , Corporate Policy
PM: Cryptography, Law, Public Policy

For full details, see section 2 on Taxonomy.

I used to prepare slides based on the abstracts so that the students would have a workbook consisting of keywords in the slide and the details at the bottom of the page. However, this approach became unmanageable by the time I reached workbook lengths of 475 pages. It was simply too much effort for relatively minor benefits. I have therefore tried a different, much simpler approach over the last few years. I mark selected topics in my database and created the workbook from a report file. The whole thing takes me a few minutes and allows me to keep the workbook absolutely up to date. I hope that course participants will find it a useful resource and an acceptable format for the course.

Starting in 2005, I spared my MSIA graduate students the agony of sweltering through two solid days of this stuff and shrank their version of the INFOSEC UPDATE to a single day. However, if we ever get air conditioning, watch out!

07 Acknowledgements

Category 07 *Acknowledgements*

2006-06-12 **Introduction**

INTRODUCTION

ACKNOWLEDGEMENTS

I would like to acknowledge the encouragement and support of many colleagues who have contributed to this project over the years. In particular, John Gehl and Suzanne Douglas, original editors of EDUPAGE and then later of NEWSSCAN and INNOVATION, stand out for their kindness in so generously allowing me to quote them verbatim in so many hundreds of stories. Thanks guys -- I simply could not do this without your help.

The editors of EDUPAGE kindly continued the tradition and have allowed me to include occasional abstracts from their publication.

My colleagues at NCSA / ICSA / TruSecure / CyberTrust Corporation were always supportive and encouraging during the years I continued this work until 2000; I especially thank my favorite curmudgeon, David Kennedy, Director of Resarch for CyberTrust, for many years of continuing friendship.

I also want to thank my colleagues Phil Susmann and COL Tom Aldrich at Norwich University and the National Center for the Study of Counterterrorism and Cybercrime for their encouragement and support and the opportunity to teach the two-day INFOSEC Update for several years at the annual e-ProtectIT Conference (http://www.e-protectIT.org).

My sincere thanks to my Norwich University research assistants, Karthik Raman (Chief Boss Man and Gang Leader), Krenar Komoni, Michael Martell, and Chris Aldrich. Thanks also to MSIA alumni volunteers Clark Cummings and Steve Lovaas for their contributions. Josh Durdin and Lofton Newton, although newcomers to the project, have started their contributions well and I look forward to further work with them.

The School of Graduate Studies, under the leadership of Founding Dean Fred Snow and of Dean Bill Clements, has generously funded the research assistantships that have permitted the project to progress without imposing total exhaustion on me. Many thanks.

Thanks to Dr Fred Snow, former Dean of Online Graduate Studies and to Dr Bill Clements, current Dean, for their support (moral and financial) in building the research team that has made this project easier.

And finally, as always, I thank my wife, Deborah Black, light of my life, for all her infinitely varied support over many years and in all ways.

08 About the Editor

Category 08 *About the Editor*

2006-06-12 **Introduction**

INTRODUCTION

Here's a little information about me. For exhaustive, not to say exhausting, details, you can visit my Web site at < http://www2.norwich.edu/mkabay > and click on my CV link.

I began programming in assembler at age 15 in 1965. In 1976, I received his PhD from Dartmouth College in applied statistics and invertebrate zoology. Joined a compiler team in 1979 for a new 4GL and RDBMS in the U.S. and then joined Hewlett-Packard Canada in 1980, winning the Systems Engineer of the Year Award in 1982. Have published over 850 technical papers in operations management and security, a 1996 textbook on security, was Technical Editor of the 4th Edition of the _Computer Security Handbook_ (Wiley, 2002) and am working on the 5th edition with Senior Editor Sy Bosworth and new third editor Eric Whyne. Have lectured on security and information warfare at the US Army War College, NATO HQ, NATO Counterintelligence, and in the UK, France, Germany, Japan and China. Returned to academia full time in July 2001 and am Associate Professor of Information Assurance in the Division of Business & Management at Norwich University, Northfield, VT 05663-1035 USA as well as the Director of the Master's Program in Information Assurance (http://www.msia.norwich.edu/) and of the Bachelor's program in IA (http://www.norwich.edu/academics/business/informationassurance.html).

V: 802-479-7937
E: mkabay@norwich.edu
W: http://www2.norwich.edu/mkabay

11 Breaches of confidentiality

Category 11 *Breaches of confidentiality*

2005-10-01 **data theft identity theft terminology dataflation privacy law court proof**

Information Security Magazine; http://tinyurl.com/9aanv

STEPHEN COBB COINS NEW TERM: DATAFLATION

Security expert Stephen Cobb writes,

>I think most people would agree that 2005 has not been, so far, a good year for information security. Indeed, when you add up the total number of personal data records reported as compromised in the first six months you get a figure that some people justly consider alarming: 66 million. But I suggest that this number, and the phenomenon it represents, goes way beyond alarming, way out into previously uncharted territory. In fact, I respectfully suggest that we don't yet have the vocabulary needed to describe what is happening to personal data today, let alone understand all of the implications.

In an effort to remedy this situation I propose a new word for that vocabulary: dataflation. But before I offer my definition of dataflation, let me provide some context for that 66 million. In the most recent U.S. census the number of Americans aged 18 or older was 210 million. If you factor in the numerous compromises of personal data records that occurred in 2004, it is entirely possible that data relating to one in three American adults is now "out there," available to be abused. <

[More in the complete article.]

11.1 Data leakage

Category 11.1 *Data leakage*

1997-02-23 **medical data confidentiality**

PA News

In Sheffield, England, a hospital handed over 50,000 confidential gynecological records to a data processing firm that hired people off the street and set them to work transcribing the unprotected data. The scandal resulted in withdrawal of the contract, but thousands of records were exposed to a wide variety of people with no background checking to ascertain their reliability.

Category 11.1 *Data leakage*

1997-07-02 **medical informatics telemedicine**

Australian

A report by Trudy Harris in _The Australian_ reviewed risks of telemedicine, a technology of great value in Australia because of great distances and sparse population. Risks included interception of unencrypted medical information, modification of critical parameters for patient care, and unauthorized access to confidential patient records.

Category 11.1 *Data leakage*

1997-07-10 **hacker password attack**

Wall Street Journal

Mark Abene, a security expert formerly known to the underground as Phiber Optik, launched a command to check a client's password files — and ended up broadcasting the instruction to thousands of computers worldwide. Many of the computers obligingly sent him their password files. Abene explained that the command was sent out because of a misconfigured system and that he had no intention of generating a flood of password files into his mailbox. Jared Sandberg, Staff Reporter for the The Wall Street Journal, wrote, "A less ethical hacker could have used the purloined passwords to tap into other people's Internet accounts, possibly reading their e-mail or even impersonating them online." Mr Abene was a member of the Masters of Deception gang and was sentenced to a year in federal prison for breaking into telephone company systems. The accident occurred while he was on parole.

Category 11.1 *Data leakage*

1997-07-19 **confidentiality error**

Telecomworldwire

A firm of accountants received passwords and other confidential codes from British Inland Revenue. Government spokesmen claimed it was an isolated incident. [How exactly did they know that it was an isolated incident?]

Category 11.1 *Data leakage*

1997-08-07 **privacy journalists Internet**

Reuters; RISKS 19 28

The ICSA's David Kennedy reported on a problem in Hong Kong, where Reuters described a slip that revealed personal details about hundreds of journalists at the end of June. Passport and identity-card details were revealed on the government Website for a couple of days. DK commented, "I suppose that's one way to get the media interested in privacy matters."

Category 11.1 *Data leakage*

1997-08-15 **privacy credit reports database**

AP, EDUPAGE

Experian Inc. (formerly TRW Information Systems & Services), a major credit information bureau, discontinued its online access to customers' credit reports after a mere two days when at least four people received reports about other people.

Category 11.1 *Data leakage*

1999-01-29 **data leakage privacy confidentiality control Web**

RISKS 20 18

The Canadian consumer-tracking service Air Miles inadvertently left 50,000 records of applicants for its loyalty program publicly accessible on their Web site for an undetermined length of time. The Web site was offline as of 21 January until the problem was fixed.

Category 11.1 *Data leakage*

1999-02-03 **data leakage Web script QA vulnerability confidentiality**

WIRED via PointCast

An error in the configuration or programming of the F. A. O. Schwarz Web site resulted paradoxically in weakening the security of transactions deliberately completed by FAX instead of through SSL. Customers who declined to send their credit-card numbers via SSL ended up having their personal details — address and so forth — stored in a Web page that could be accessed by anyone entering a URL with an appropriate (even if randomly chosen) numerical component.

Category 11.1 *Data leakage*

2000-02-06 **bank financial system leak confidentiality windfall investors market**

RISKS 20 78

An error at the Reserve Bank of Australia caused e-mail to be sent to 64 subscribers of the bank's alert service informing them of a planned 0.5% increase in the prime interest rate. However, the message was sent out six minutes early, allowing some of those traders to sell A$3B of treasury bill and bond futures — and making some people a great deal of money.

Category 11.1 *Data leakage*

2000-02-06 **confidentiality human factors workstations home computer Web browsing**

RISKS, New York Times 20 78
http://www.nytimes.com/yr/mo/day/news/washpol/cia-impeach-deutch.html

The former director of the CIA, John Deutch, kept thousands of highly classified documents on his unsecured home Macintosh computer. Critics pointed out that the system was also used for browsing the Web, opening the cache of documents up to unauthorized access of various kinds.

Category 11.1 *Data leakage*

2000-02-20 **confidentiality Web site**

RISKS, CNet 20 80
http://news.cnet.com/category/0-1005-200-1550948.html

H&R Block had to shut down its Web-based online tax-filing system after the financial records of at least 50 customers were divulged to other customers.

Category 11.1 *Data leakage*

2000-04-28 **covert channel discover discarded data trash recycle access confidentiality**

RISKS 20 88

Conrad Heiney noted in RISKS that network-accessible shared trashcans under Windows NT have no security controls. Anyone on the network can browse discarded files and retrieve confidential information. [Moral: electronically shred discarded files containing sensitive data.]

Category 11.1 *Data leakage*

2000-06-18 **privacy confidentiality anonymity**

RISKS 20 93

A RISKS correspondent reported on a new service in some hotels: showing the name of the guest on an LCD-equipped house phone when someone calls a room. Considering the justified reluctance to reveal the room number of a guest or to give out the name of a room occupant if one asks at the front desk, this service seems likely to lead to considerable abuse, including fraudulent charges in the hotel restaurant.

Category 11.1 *Data leakage*

2000-06-24 **confidentiality concealment error vulnerability**

RISKS, Wired http://www.wired.com/news/politics/0,1283,37205,00.html 20 93

New York Times Web-site staff chose an inappropriate mechanism for obscuring information in an Adobe Acrobat PDF document that contained information about the 1953 CIA-sponsored coup d'état in Iran. The technicians thought that adding a layer on top of the text in the document would allow them to hide the names of CIA agents; however, incomplete downloading allowed the supposedly hidden information to be read. Moral: change the source, not the output, when obscuring information.

Category 11.1 *Data leakage*

2000-07-07 **e-mail domain name system DNS confusion similarity**

NewsScan, Wall Street Journal
http://interactive.wsj.com/articles/SB962887042191508928.htm

One of Spain's largest banks — and its most aggressive in terms of moving operations onto the Internet — is suffering from an identity crisis that has resulted in thousands of messages being routed to Bulletin Board VA, run by a rural Virginia man who publishes a weekly shopper with a circulation of 10,000. Banco Bilboa Vizcaya Argentaria, which goes by the acronym BBVA after Banco Bilbao Vizcaya merged with Argentaria SA last fall, is the owner of the "grupobbva.com" domain name, but many employees, customers and outside vendors mistakenly send their sometimes-sensitive e-mail to "bbva.com," a domain name owned by Bulletin Board VA. "When all this e-mail started coming in, I didn't know who to contact. I didn't know who to talk to," says Bulletin Board VA owner Jim Caldwell. "To me it is beyond the stage of funny." Some of the messages contain bank account numbers and balances, and at least one contained confidential information about a possible bank acquisition. BBVA says it's in the process of changing its domain name to "bbva.es," and hopes that will solve the problem. Caldwell certainly hopes so — he says he spends up to two hours a day clearing his server of the mislabeled messages. (Wall Street Journal 7 Jul 2000)

Category 11.1 *Data leakage*

2000-07-13 **data spill confidentiality privacy e-mail address banner advertisement HTML Web page transfer**

NewsScan, Los Angeles Times
http://www.latimes.com/business/20000713/t000065732.html

Microsoft . . . acknowledged that a flaw in its Hotmail program . . . [was] inadvertently sending subscribers' e-mail addresses to online advertisers. The problem, which is described as a "data spill," occurs when people who subscribe to HTML newsletters open messages that contain banner ads. "The source of the problem is that Hotmail includes your e-mail address in the [Web address], and if you read an e-mail that has banner ads," the Web address will be sent to the third-party company delivering the banner, says Richard Smith, a security expert who alerted Microsoft to the problem in mid-June. Data spills are common on the Web, says Debra Pierce of the Electronic Frontier Foundation. "This isn't just local to Hotmail; we've seen hundreds of instances of data spills over the course of this year." Smith estimates that more than a million addresses may have been transferred to ad firms, but most of the big agencies, including Engage and DoubleClick, are discarding the information. (Los Angeles Times 13 Jul 2000)

Category 11.1 *Data leakage*

2000-07-24 **confidentiality phone access control design flaw**

RISKS 20 97

AT&T allowed extensive details of a phone account to be revealed to anyone entering a phone number into their touch-tone interface for the Credit Management Center.

Category 11.1 *Data leakage*

2000-08-01 **confidentiality customer data Web site flaw upgrade QA quality assurance**

RISKS, BBC 21 01
http://news.bbc.co.uk/hi/english/business/newsid_860000/860104.stm

Peter Morgan-Lucas reported to RISKS, "Barclays Bank yesterday had a problem with their online banking service - at least four customers found they could access details of other customers. Barclays are claiming this to be an unforeseen side-effect of a software upgrade over the weekend."

Category 11.1 *Data leakage*

2000-08-14 **confidentiality Web site disclosure flaw error QA quality assurance**

RISKS, SecurityFocus http://www.securityfocus.com/news/074 21 01

Kevin Poulson of SecurityFocus reported "Verizon's twenty-eight million residential and business telephone subscribers from Maine to Virginia had portions of their private telephone records exposed on a company web site. . . ." The system was designed to permit customers to file and track their repair reports, but entering any phone number generated HTML code containing the legitimate number's registered user information such as name and address.

Category 11.1 *Data leakage*

2001-02-16 **proprietary document formats hidden information concealed data confidentiality Web**

RISKS 21 25

Paul Henry noted that the well-known problem of hidden information in MS Word documents continues to be a source of breaches of confidentiality. Writing in RISKS, he explained, "I received an MS Word document from a software start-up regarding one of their clients. Throughout the document the client was referred to as 'X', so as not to disclose the name. However I do not own a copy of Word, and was reading it using Notepad of all things, and discovered at the end the name of the directory in which the document was stored -- and also the real name of the client! I checked on a number of other word documents I had for hidden info, especially ones from Agencies who are looking to fill positions -- and yes, again I was able to tell who the client was from the hidden information in the documents."

Mr Henry concluded, "Risks: What potentially damaging information is hidden in published documents in Word, PDF and other complex formats? Mitigation: Use RTF when you can -- no hidden info, no viruses."

Category 11.1 *Data leakage*

2001-06-22 **e-mail vulnerability holes bug confidentiality**

NewsScan

E-MAIL SECURITY BREACHES: EVERYONE IS VULNERABLE
The e-mail of Dennis Tito, the investment banker who paid to become the first tourist in space, was insecure for more than a year -- as were the communications of his entire company, Wilshire Associates. . . . Although there is no evidence that anyone took advantage of the breaches, they allowed access by outsiders to confidential company business, including financial data, passwords, and the personal information of employees. However, security experts say Wilshire's problem is not an isolated one, and warn that American companies are not taking computer security issues seriously. Peter G. Neumann, principal scientist in the computer science lab at SRI International, says that the security breach discovered at Wilshire is just "one of thousands of vulnerabilities known forever to the world. Everybody out there is vulnerable." (Washington Post 22 Jun 2001)
http://washingtonpost.com/wp-dyn/articles/A7642-2001Jun15.html

---

Category 11.1 *Data leakage*

2001-07-05 **confidentiality compromise e-mail CC BCC error medical information drug prescription**

RISKS 21 51

The drug company Eli Lilly sent out an e-mail reminder to renew their prescriptions for Prozac to 600 clients -- and used CC instead of BCC, thus revealing the entire list of names and e-mail addresses to all 600 recipients.

Category 11.1 *Data leakage*

2001-11-26 **confidentiality search engine data leakage**

NewsScan

SEARCH ENGINES DIG TOO DEEP
Search engines increasingly are unearthing private information such as passwords, credit card numbers, classified documents, and even computer vulnerabilities that can be exploited by hackers. "The overall problem is worse than it was in the early days, when you could do AltaVista searches on the word 'password' and up come hundreds of password files," says Christopher Klaus, founder and CTO of Internet Security Systems, who notes that a new tool built into Google to find a variety of file types is exacerbating the problem. "What's happening with search engines like Google adding this functionality is that there are a lot more targets to go after." Google has been revamped to sniff out a wider array of files, including Adobe PostScript, Lotus 1-2-3, MacWrite, Microsoft Excel, PowerPoint, Word, and Rich Text Format. Google disavows responsibility for the security problem, but the company is working on ways to limit the amount of sensitive information exposed. "Our specialty is discovering, crawling and indexing publicly available information," says a Google spokesman. "We define 'public' as anything placed on the public Internet and not blocked to search engines in any way. The primary burden falls to the people who are incorrectly exposing this information. But at the same time, we're certainly aware of the problem , and our development team is exploring different solutions behind the scenes." (CNET News.com 26 Nov 2001)
http://news.cnet.com/news/0-1005-200-7946411.html?tag=lh

Category 11.1 *Data leakage*

2002-02-20 **search engine spider web-bot exclusion cache**

RISKS 21 92

RISKS correspondent Diomidis Spinellis cogently summarized some of the problems caused by search engines on the Web: "The aggressive indexing of the Google search engine combined with the on-line caching of the pages in the form they had when they were indexed, is resulting in some perverse situations.

A number of RISKS articles have already described how sensitive data or supposedly non-accessible pages leaked from an organization's intranet or web-site to the world by getting indexed by Google or other search engines. Such problems can be avoided by not placing private information on a publicly accessible web site, or by employing metadata such as the robot exclusion standard to inform the various web-crawling spiders that specific contents are not to be indexed. Of course, adherence to the robot exclusion standard is left to the discretion of the individual spiders, so the second option should only be used for advisory purposes and not to protect sensitive data."

Category 11.1 *Data leakage*

2002-03-22 **design QA quality assurance confidentiality Web URL**

RISKS 22

Paul van Keep reported in RISKS, >Christine Le Duc, a dutch chain of s*xshops, and also a mail & Internet order company, suffered a major embarrassment last weekend. A journalist who was searching for information on the company found a link on Google that took him to a page on the Web site with a past order for a CLD customer. He used the link in a story for online newspaper nu.nl. The full order information including name and shipping address was available for public viewing. To make things even worse it turned out that the classic URL twiddling trick, a risk we've seen over and over again, allowed access to ALL orders for all customers from 2001 and 2002. The company did the only decent thing as soon as they were informed of the problem and took down the whole site.<

http://nu.nl/document?n=53855

[Note: * included to foil false positive exclusion by crude spam filters.]

Category 11.1 *Data leakage*

2002-04-22 **data leakage surveillance privacy Web cameras Webcam hijack wireless**

RISKS 22 04ff

Dave Farber noted in RISKS:

Thousands of people who have installed a popular wireless video camera, intending to increase the security of their homes and offices, have instead unknowingly opened a window on their activities to anyone equipped with a cheap receiver. The wireless video camera, which is heavily advertised on the Internet, is intended to send its video signal to a nearby base station, allowing it to be viewed on a computer or a television. But its signal can be intercepted from more than a quarter-mile away by off-the-shelf electronic equipment costing less than $250. [...] [Source: John Schwartz, *The New York Times*, 14 Apr 2002 http://www.nytimes.com/2002/04/14/technology/14SPY.html?ex=1019744700&ei=1&en=cfeb1e93a276b9ee]

Marc Roessler commented:

"This is nothing new. Such cameras are even installed in some public restaurants and shops. Note that this basically voids all claims of the shop owners concerning privacy and data protection -- ANYONE can receive that data. And, as more and more cameras are installed, the risk of malicious "camera takeovers" rises significantly. Think about webcams, cams integrated into notebooks/cellular phones, car dashboards (detect the driver falling asleep).. Those are easily tapped (or subverted, such as by installing trojan software/ firmware).. this has some enormous potential. The case of the Nanny-Cams shows the deviousness of this kind of attack: as the devices are not suspected to be used to spy on their owner ("I own that device; that makes it trusted"), they function more or less as hidden cameras. For more "camera takeover" scenarios take a look at my paper "How to find hidden cameras" [1].

[1] http://www.franken.de/users/tentacle/papers/hiddencams.pdf

---

Category 11.1 *Data leakage*

2002-06-10 **QA quality assurance Web confidentiality breach customer activity**

RISKS; http://www.msnbc.com/news/758979.asp 22 12

Monty Solomon wrote in RISKS, "A design flaw at a Fidelity Investments online service accessible to 300,000 people allowed Canadian account holders to view other customers' account activity. The problem was discovered over the weekend by Ian Allen, a computer studies professor at Algonquin College in Ottawa. Fidelity said it had fixed the problem and was offering customers the option of changing account numbers."

Category 11.1 *Data leakage*

2003-01-16 **data leakage remanence**

NewsScan

JUNKED HARD DRIVES YIELD LOTS OF PERSONAL DATA
MIT graduate students Simson Garfinkel and Abhi Shelat bought 158 hard drives at second hand computer stores and eBay over a two-year period, and found that more than half of those that were functional contained recoverable files, most of which contained "significant personal information." The data included medical correspondence, love letters, pornography and 5,000 credit card numbers. The investigation calls into question PC users' assumptions when they donate or junk old computers — 51 of the 129 working drives had been reformatted, and 19 of those still contained recoverable data. The only surefire way to erase a hard drive is to "squeeze" it — writing over the old information with new data, preferably several times — but few people go to the trouble. The findings of the study will be published in the IEEE Security & Privacy journal Friday. (AP 16 Jan 2003) http://apnews.excite.com/article/20030116/D7OJBBBG0.htm

---

Category 11.1 *Data leakage*

2003-02-10 **discarded computer disk data leakage confidential information medical**

NewsScan

SURPLUS COMPUTER IN KENTUCKY HELD 'DELETED' AIDS FILES
A state auditor found that at least one computer used by staffers counseling clients with AIDS or HIV was ready to be offered for sale to the public even though it still contained files of thousands of people. Auditor Ed Hatchett said: "This is significant data. It's a lot of information lots of names and things like sexual partners of those who are diagnosed with AIDS. It's a terrible security breach." Health Services Secretary Marcia Morgan, who has ordered an internal investigation of that breach, says the files were thought to have been deleted last year. (AP/USA Today 7 Feb 2003)

Category 11.1 *Data leakage*

2003-04-17 **CNN obituraries famous people blunder**

NewsScan

CNN GLITCH REVEALS PREMATURE OBITS
A glitch on the CNN.com Web site accidentally made available draft obituaries written in advance for Dick Cheney, Ronald Reagan, Fidel Castro, Pope John Paul II and Nelson Mandela. "The design mockups were on a development site intended for internal review only," says a CNN spokeswoman. "The development site was temporarily publicly available because of human error." The pages were yanked about 20 minutes after being exposed. (CNet News.com 17 Apr 2003)

Category 11.1 *Data leakage*

2003-05-29 **hacker vulnerability Cingular Adrian Lamo website line LLC random finding Sacremento California dumpster customer records exploit**

NIPC/DHS

May 29, Wired — Hacker exposes vulnerability in Cingular claims site.

Hacker Adrian Lamo found a security hole in a website run by lock\line LLC, which provides claim management services to Cingular customers. Lamo discovered the problem last weekend through a random finding in a Sacramento, CA dumpster, where a Cingular store had discarded records about a customer's insurance claim for a lost phone. By simply typing in a URL listed on the detritus, Lamo was taken to the customer's claim page on the lock\line website. Lamo was able to access individual claims pages containing customer's name, address and phone number, along with details on the insurance claim being made. Altering the claim ID numbers in the URL gave Lamo access to some 2.5 million Cingular customer claims dating back to 1998. Lamo said he had no intent of profiting from the exploit, just pointing out a security flaw. Cingular and lock\line closed the hole by Wednesday morning.

Category 11.1 *Data leakage*

2003-06-16 **CERT Linux PDF flaw hacker tips confidential vulnerability hack4life Unix Jeffrey Carpenter**

NIPC/DHS

June 16, IDG News Service — Hacker tips CERT's hand on Linux/PDF flaw.

Confidential vulnerability information managed by the CERT Coordination Center has again been leaked to the public. The latest report was posted to a vulnerability discussion list by an individual using the name "hack4life." The latest information concerns a flaw in Adobe Systems Inc.'s PDF (Portable Document Format) readers for Unix and could allow a remote attacker to trick users into executing malicious code on their machines, according to a copy of the leaked vulnerability report. The leaked information was taken from communication sent from CERT to software vendors affected by the PDF problem, according to Jeffrey Carpenter, manager of the CERT Coordination Center. The information appears to be from a vulnerability report submitted to CERT by a Cincinnati security researcher by the name of Martyn Gilmore. Adobe's Acrobat Reader 5.06 and the open-source reader Xpdf 1.01 are affected by the problem, according to the report.

Category 11.1 *Data leakage*

2003-06-30 **PetCo security hole storefront 500000 credit card numbers open Jeremiah Jacks computer SQL security**

NIPC/DHS

June 30, SecurityFocus — PetCo plugs security hole.

Pet supply retailer PetCo.com plugged a hole in its online storefront over the weekend that left as many as 500,000 credit card numbers open to anyone able to construct a specially-crafted URL. Twenty-year old programmer Jeremiah Jacks discovered the hole. He used Google to find active server pages on PetCo.com that accepted customer input and then tried inputting SQL database queries into them. "It took me less than a minute to find a page that was vulnerable," says Jacks. The company issued a statement Sunday saying it had hired a computer security consultant to assist in an audit of the site.

Category 11.1 *Data leakage*

2003-09-15 **data leakage remanence used equipment confidentiality personal financial consumer customer information auction**

http://www.thestar.com/NASApp/cs/ContentServer?pagename=thestar/Layout/Article_PrintFriendly&c=Article&cid=1063577414565&call_pageid=968332188492

Two Bank of Montreal computers containing hundreds, potentially thousands, of sensitive customer files narrowly escaped being sold on eBay.com late last week, calling into question the process by which financial institutions dispose of old computer equipment.

Information in one of the computers included the names, addresses and phone numbers of several hundred bank clients, along with their bank account information, including account type and number, balances and, in some cases, balances on GICs, RRSPs, lines of credit, credit cards and insurance.

Many of the files were dated as recently as late 2002, while some went back to 2000. The computers appeared to originate from the bank's head office on St. Jacques St. in Montreal, but customers, many of them also bank employees, had addresses ranging from Victoria, B.C., to St. John's, Nfld.

Category 11.1 *Data leakage*

2004-01-05 **Danish Prime Minister accidental information disclosure leakage MS Word PDF**

RISKS 23 12

DANISH PM'S PRIVATE COMMUNICATIONS DISCLOSED BY MS WORD

Contributor Theodor Norup reports that a press-release Word document from the Danish Prime Minister's Office unintendedly revealed its real source and all its revisions. As a result of this incident, ministry spokesman Michael Kristiansen said the Prime Minister's office would "distribute speeches as PDF files…" Norup believes the risk still is trusting "high echelons of governments" will know a little about information security.

Category 11.1 *Data leakage*

2004-03-16 **Microsoft leaked code Internet vulnerability exploit hacker attacker defense**

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1548988,00.asp

March 14, eWEEK — Leaked code still could bear malicious fruit.

A portion of Windows source code was leaked last month, and researchers are saying that hackers have uncovered several previously unknown vulnerabilities in the code. Immediately following the code's posting on the Internet, members of the security underground began poring over the code, searching for undocumented features and flaws that might give them a new way to break into Windows machines. The real danger isn't the vulnerabilities that this crowd finds and then posts; it's the ones that they keep to themselves for personal use that have researchers worried. Experts said there has been a lot of talk about such finds on hacker bulletin boards and Internet Relay Chat channels of late, indicating that some hackers are busily adding new weapons to their armories. Another concern for Microsoft and its customers is that even though the leaked code is more than 10 years old, it forms the base of the company's current operating system offerings, Windows XP and Windows Server 2003. This means that any vulnerabilities found in Windows NT or Windows 2000 could exist in the newer versions as well.

Category 11.1 Data leakage

2004-10-19 **spyware Google data leakage shared computers confidentiality**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A43548-2004Oct18.html

GOOGLE'S PC SEARCH TOOL MIGHT PROVE THE 'PERFECT SPY'

Google Desktop Search, released last Thursday in a "beta" test phase, may prove a boon to disorganized PC users who need assistance in finding data on their computers, but it also has a downside for those who use public or workplace computers. Its indexing function may compromise the privacy of users who share computers for such tasks as processing e-mail, online shopping, medical research, banking or any activity that requires a password. "It's clearly a very powerful tool for locating information on the computer," says one privacy consultant. "On the flip side of things, it's a perfect spy program." The program, which is currently available only for Windows PCs, automatically records any e-mail read through Outlook, Outlook Express or the Internet Explorer browser, and also saves pages viewed through IE and conversations conducted via AOL Instant Messenger. In addition, it finds Word, Excel and PowerPoint files stored on the computer. And unlike the built-in cache of recent Web sites visited that's included in most browser histories, Google's index is permanent, although individuals can delete items individually. Acknowledging potential privacy concerns, a Google executive says managers of shared computers should think twice about installing the tool before advanced features like password protection and multi-user support are available.

Category 11.1 Data leakage

2005-02-07 **iPods medical imaging UCLA Osirix radiologists Macintosh security**

EDUPAGE; http://news.com.com/2100-1041_3-5566145.html

USING IPODS FOR MEDICAL IMAGING AT UCLA

Physicians at the University of California, Los Angeles (UCLA), are using iPods in conjunction with an open source application developed in-house to avoid some of the steep costs of medical imaging. Physicians Osman Ratib and Antoine Rosset created Osirix, an open source tool that allows radiologists to participate in teleconferences and see high-resolution medical images on desktop Macintosh computers, rather than the $100,000 workstations that were previously required. Files for the 3D images are too large for many media, so Ratib and his team turned to the iPod, which offers a portable storage medium of 60GB. Although some cautioned that using iPods for storage presents a security risk, Ratib said the risk is no greater than with any other medium. "It's not the device, it's how you use it," he said. "When [users] are outside the institution, they can be compliant or not."

Category 11.1 Data leakage

2005-04-07 **German police hard drive sale confidential information eBay encryption password protection absent**

DHS IAIP Daily; http://www.scmagazine.com/news/index.cfm?fuseaction=newsDetails&newsUID=023c9f0f-7295-49c5-b349-847df8e174b2&newsType=Latest%20News

GERMAN POLICE HARD DRIVE CONTAINING CONFIDENTIAL INFORMATION SOLD ON EBAY

A hard drive full of confidential police data has been sold on eBay, for only $25. Germany's Spiegel newspaper reported earlier this week that the 20GB hard drive contained a raft of information about Brandenburg police, including details of political security situations. "This week's exposure of leaked and highly critical information from the Brandenburg police in Germany reinforces how important it is to never let mobile devices or hard drives leave the office without being adequately protected with encryption and strong password protection -- even after they have been discarded," said Peter Larsson, CEO of mobile technology company Pointsec. The drive was eventually bought by a student from Potsdam who alerted police once he realized what it contained.

Category 11.1 *Data leakage*

2005-06-10 **personal information privacy confidentiality control banks magnetic tapes customer data loss theft secure electronic channels**

RISKS; http://www.nytimes.com/2005/06/09/business/09data.html?th&emc=th 23 90

THE SKY HAS *ALREADY* FALLEN

In Feb 2004, a Japanese division of Citibank had a mag tape disappear during shipment by truck from its data management center in Singapore, with information on about 120,000 customers. The tape has never been found. This week it happened again to a box of tapes sent by United Parcel Service, with info on nearly 4,000,000 American customers. Citigroup is apparently in the process of responding to the Singapore case with the company-wide introduction of "secure electronic channels" -- although that process is not yet complete. [Tom Zeller Jr., *The New York Times*, 9 Jun 2005; abstract by PGN]

Zeller's article has more on ChoicePoint, 10 million consumers falling victim to identity theft each year, discussion of the 2003 California law that mandates reporting, and this delightful quote from Mike Gibbons (former FBI chief of cybercrime investigations, now a consultant for Unisys): "I think there are some people who dismiss this as a sky-is-falling problem. But the sky has already fallen and it's just a matter of when a piece hits you in the head."

Also a quote from Bruce Schneier: "There are social expectations about security that can't be met, but the practices are still so shoddy."

Category 11.1 *Data leakage*

2005-07-31 **data leakage discarded systems data software wiping erasure scavenging backups**

RISKS; http://www.geoffreyhuntley.com/news/data-security-101/ 23 95

WIPE YOUR DISKS BEFORE SELLING YOUR COMPUTERS -- AND DON'T INCLUDE BACKUP TAPES

The State Transit Authority of New South Wales in Australia sold 18 IBM RS/6000 E30 servers to the company where Geoffrey Huntley works. He found that "[T]he systems contained not only the complete software used by the SAT-NSW but also employee data including PIN information used to 'secure' the system against unauthorized access, and ticketing data including incident reports filed by customers. For good measure, the backup tapes were also included."

[Abstract by Florian Liekweg]

Category 11.1 *Data leakage*

2005-11-21 **hurricane Katrina disaster lost records encryption backups critical**

DHS IAIP Daily; http://fcw.com/article91509−11−21−05−Print

LOST RECORDS CONVINCE OFFICIALS THAT ENCRYPTED DIGITAL BACKUPS ARE CRUCIAL

After Hurricane Katrina devastated the Gulf Coast region, along with many vital records, federal officials realized they needed to digitize such records to prevent future data loss. But storage analysts say federal agencies are behind the curve when it comes to safeguarding digitized records stored elsewhere. Federal agencies are not encrypting their off-site data, said Jon Oltsik, a senior analyst at research firm Enterprise Strategy Group. Katrina's destruction demonstrated the importance of electronic backup copies of documents such as health records and flood maps. But by keeping copies of critical information, agencies also create new opportunities for data theft. Oltsik is the author of a recent survey that asked 388 agencies and companies whether they encrypt backup data as they copy it to tape. "Of the five industry segments we looked at, [the local/federal] government was the worst," he said. Only three percent of government organizations said they always encrypt backup data, and 77 percent said they never do. Overall, only seven percent of the organizations surveyed said they always encrypt backup data, despite the fact that vendors have offered backup encryption tools for at least 15 years, Oltsik said.

Category 11.1 *Data leakage*

2005-12-23 **Microsoft Vista metadata operating system files tags IT document information security privacy risk**

DHS IAIP Daily; http://www.newsfactor.com/news/Gartner−Warns−About−Vista−Met adata/story.xhtml?story_id=113003ORER88

Gartner warns about Microsoft Vista metadata problem.

Windows Vista, the next version of Microsoft's Windows client operating system, will give users the ability to search for files by looking for information in the file's metadata tags. However, a report by IT research firm Gartner warned that allowing users to search for metadata tags in this manner could result in private information being inadvertently disclosed. Metadata consists of "data about data." It is supplementary information about the author of a document, its various revisions, and any changes that have been made, explained Neil MacDonald, Gartner's vice president and distinguished analyst of information security, privacy, and risk. The Gartner report, "Plan To Deal with Metadata Issues with Windows Vista," written by MacDonald and Gartner analyst Michael Silver, outlines one example in which an employee might give a document about a client the metadata tag "bad client." If that document were then sent to the client, considerable embarrassment, even loss of business, could result. The Gartner report suggested that firms must have a strategy in place for dealing with metadata before adopting Windows Vista. The referenced Gartner report is available for purchase: http://www.gartner.com/

Category 11.1 *Data leakage*

2005-12-28 **data loss personal data employees customers tapes SSN Social Security Numbers**

RISKS; Boston Globe; http://tinyurl.com/nnrxl 24 14

MARRIOTT LOSES CONTROL OF DATA ON BACKUP TAPES

The timeshare unit of Marriott International Inc. is notifying more than 200,000 people that their personal data are missing after backup computer tapes went missing from a Florida office. The data relates to 206,000 employees, timeshare owners and timeshare customers of Marriott Vacation Club International, the company said in a statement Tuesday. The computer tapes were stored in Orlando, where the unit is based.

The company did not say when the tapes disappeared. They contained Social Security numbers, bank and credit card numbers, according to letters the company began sending customers on Saturday. . . . [Abstract by Monty Solomon]

Category 11.1 *Data leakage*

2006-01-12 **bank tape Social Security Numbers SSN loss data leakage confidentiality privacy**

RISKS; http://tinyurl.com/qy29o 24 15

PEOPLE'S BANK LOSES TAPE WITH PERSONAL DATA ABOUT 90,000 CUSTOMERS

According to John Christoffersen of Associated Press, "A tape containing the Social Security numbers and other confidential data of 90,000 People's Bank customers was lost recently while en route to a credit reporting bureau, state and bank officials said Wednesday [11 Jan 2006]."

As usual, bank employees cheerfully asserted that there was no reason to be concerned by the loss. "People's has no reason to believe the data has been used inappropriately and has received no reports of unauthorized activity, officials said. Customers do not need to close accounts because the information is not sufficient to allow unauthorized access, the bank said."

Category 11.1 *Data leakage*

2006-02-10 **EFF privacy concern Google Desktop Search government subpoena**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4700002.stm 23

EFF RAISES CONCERNS OVER GOOGLE DESKTOP

The Electronic Frontier Foundation (EFF) is warning users about what it says are privacy concerns with Google's new Desktop Search application. The tool indexes files from a computer, allowing users to search that content from other machines. According to the EFF, this process poses significant risks to personal privacy, particularly in light of recent government demands for access to usage logs from Google and other companies. EFF staff attorney Kevin Bankston said, "Unless you configure Google Desktop very carefully, and few people will, Google will have copies of...whatever...text-based documents the desktop software can index." If federal authorities obtain Google's records, he said, they would have access to all of those files. Officials from Google conceded that the new tool does represent a trade-off of some measure of privacy, but said such a compromise is one that many users will be willing to make. The company also said it would encrypt those files, would place strong limits on who can access the information, and would not store it for more than 30 days.

Category 11.1 *Data leakage*

2006-04-03 **Trend Micro data leakage virus anti-virus software not installed employee computer**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/holes/story/0,10801,110142,00.html 23

TREND MICRO DATA REVEALED DUE TO VIRUS.

The failure of a Trend Micro Inc. employee to install his company's own antivirus software led to the uploading of some company reports to a popular Japanese peer-to-peer file-sharing network, the company said Monday, April 3. In disclosing the data leak, Trend Micro became the latest of a number of corporations or government agencies to report data losses as a result of viruses on the Winny network. Winny can be downloaded at no charge and is a popular way for Japanese Internet users to exchange music and video files.

Category 11.1 *Data leakage*

2006-04-28 **data leakage confidentiality privacy virus**

RISKS 24 27

JAPANESE NEWSPAPER LEAKS SUBSCRIBER INFORMATION TO INTERNET

The Mainichi Shimbun reported that information on about 66,000 subscribers (including names, addresses, phone numbers, dates of birth, and e-mail addresses) was leaked onto the Internet. This resulted from an employee copying the data onto his own computer, which was thought to have been infected with a virus that exploited a vulnerability in the *Share* file-sharing application.

[Abstract by Peter G. Neumann]

Category 11.1 *Data leakage*

2006-05-04 **Ohio University personal data disclosure Social Security numbers**

EDUPAGE; http://chronicle.com/daily/2006/05/2006050401t.htm 23

OHIO UNIVERSITY EXPOSES PERSONAL DATA

Officials at Ohio University said that a compromised server exposed personal information on about 300,000 individuals for more than a year. William Sams, CIO and associate provost for information technology at the university, said unusually high traffic tipped off IT staff that there was a problem. After investigation, it was determined that hackers had accessed a server that contained an alumni database that included more than 137,000 Social Security numbers as well as data on donations and amounts. The database did not include credit card information. Sams said the data had been exposed since March 2005. The university is working to notify individuals whose data was exposed and to offer them advice about how to minimize the risk of identity theft. Two people in the database have reported misuse of their personal information. Although one was found to be unrelated to the breach at Ohio University, officials are still trying to determine if the other incident is connected.

11.2 Unauthorized disclosure

Category 11.2 Unauthorized disclosure

1997-04-08 **QA operations security confidentiality**

AP, Reuters

The General Accounting Office lambasted the IRS for improper operations security, saying that the IRS "misplaced" 6,000 computer tapes and cartridges. Sen. John Glenn (D-OH), who released the report, also introduced a bill to define criminal penalties against IRS employees who snoop into taxpayer records without cause. Glenn said that out of 1,515 cases of unauthorized browsing identified in the 1994 and 1995 fiscal years at the IRS, only 23 employees were fired for the activity.

Category 11.2 Unauthorized disclosure

1997-04-30 **medical confidentiality AIDS database**

UPI

Greg Wentz was found guilty of anonymously mailing a list of 4,000 names of people with AIDS to two Florida newspapers. It turned out that he was acting vindictively to punish his ex-lover, William Calvert III. Calvert was also charged with a misdemeanor for misusing the list, which he obtained at work in the Pinellas County Health Department. Wentz faces up to 60 days in jail and up to $500 in fines.

Category 11.2 Unauthorized disclosure

1997-08-28 **privacy Web**

EDUPAGE

According to an independent group that monitors government activities, US federal Web sites are failing to protect user privacy. OMB Watch said, "There is no government-wide policy regarding privacy concerns on federal Web sites... Agencies collect personal information about visitors to their Web sites, but fail to tell them why that information is being collected and what it is being used for." After the report, three agencies that were collecting cookies files stopped doing so.

Category 11.2 Unauthorized disclosure

1997-09-08 **SSN privacy**

RISKS, EPIC Alert, AP 19 37

In September, six months after its ill-fated implementation of online access to the Personal Earnings and Benefits Estimate Statement (PEBES) service, the Social Security Administration announced its revised system. The most important change was that sensitive data such as the detailed earnings report would be available only by snail-mail; in addition, the system would impose a strict limit on the amount of information available online to any one requestor. Privacy advocates such as Marc Rotenberg of the Electronic Privacy Information Center (EPIC) congratulated the SSA on the improvements and praised it for consulting with the public.

Category 11.2 Unauthorized disclosure

1998-06-14 **privacy ISP AOL Navy homosexuality policy**

EDUPAGE, RISKS, POLITECH

In a spectacular blooper by both the ISP and the military in 1997, an AOL technician told a Navy investigator that seaman Timothy McVeigh (not the Oklahoma City bomber) was describing himself as gay on that network. The Navy eventually allowed McVeigh an honorable discharge plus compensation for his legal fees. AOL publicly apologized to him for violating his privacy.

Category 11.2 Unauthorized disclosure

1999-08-26 **privacy Web aggregate data collection marketing purchases preferences books**

USA Today

The "Purchase Circle" feature of <amazon.com> caused ripples of concern among some observers because it allows anyone to view aggregated purchase data broken down by city, university and organization. Critics argue that knowing which books people in a given competitor are buying may provide valuable competitive information. Amazon responded by providing a way of opting out of participation in the data collection. Legal experts noted that such corporate data collection, publication and use of aggregated data is not illegal.

Category 11.2 *Unauthorized disclosure*

1999-10-16 **privacy espionage information warfare confidentiality unlisted ex directory phone numbers government ministers**

Wired

Someone posted several confidential phone numbers for New Zealand government ministers on a home page in the GeoCities Web hosting system. The security breach rendered many home, mobile, and pager numbers unusable as a result of the disclosure.

Category 11.2 *Unauthorized disclosure*

2000-02-27 **confidentiality mail account social security number SSN**

RISKS 20 82

A couple of articles in RISKS discussed the tendency of companies to put too much personal information in a single letter to their customers, thus allowing anyone intercepting the letter to impersonate them effectively. Taylor Hutt wrote about Great West's sending out name, birthdate, social security number and account number in a change-of-address confirmation; he followed up with their response to his suggestions for improvement — they accepted them! And Bob Hofkin reported that the Cigna brokerage firm resisted his efforts to improve confidentiality by telling him — a classic non-sequitur — "You're the first person to complain about this."

Category 11.2 *Unauthorized disclosure*

2000-12-24 **privacy confidentiality breach credit-record data integrity**

RISKS 21

Beth Roberts, reporting in RISKS, discovered that credit bureaus were still identifying her by her former married name and sent her credit records with the address of her ex-husband. She pointed out that this could be a risk in cases of vindictive ex-spouses.

Category 11.2 *Unauthorized disclosure*

2001-01-23 **confidentiality Web data leakage customer information privacy fraud**

RISKS 21 21

Monty Solomon wrote in RISKS, "A security breach at Travelocity recently exposed the personal information of up to 51,000 online travel company's customers who had participated in a site promotion. Customer names, addresses, phone numbers, and e-mail addresses were revealed because of an inadequately protected directory -- possibly for up to a month. This resulted from new servers cutover from San Francisco to Tulsa. [Source: Troy Wolverton, CNET News.com, 22 Jan 2001 http://news.cnet.com/news/0-1007-200-4564919.html]"

Category 11.2 *Unauthorized disclosure*

2001-05-04 **banking financial information social engineering industrial espionage confidentiality breach**

NIPC Daily Report

About a dozen of the nation's leading banks will discuss on 4 May how to protect themselves from using information brokers who trick other banks into turning over confidential details about individuals' finances. One recommendation on the agenda is that banks insist that brokers sign contracts promising they will not use illegal pretext calls to get data about debtors' assets. Federal regulators have urged national banks to boost efforts to protect customers against information brokers and identity thieves. The banks' apparent sense of urgency on pretext calling shows how deep an impact privacy issues have had on the financial services industry in recent years. The financial institutions want to find a way to improve security and detect fraud, while providing easy telephone and Internet access for their customers.

Category 11.2 *Unauthorized disclosure*

2001-06-05 **privacy Web confidentiality adolescent harassment arrest**

NewsScan

STUDENTS CHARGED WITH WEB HARASSMENT [5 Jun 2001]
Two high school students in Chappaqua NY have been charged with sexual harassment for operating a Web site that published the secrets of several dozen girls at the school. If convicted the two teenagers could be sentenced to as much a year in jail and a $1,000 fine. One student at the school said: "You hang out with your friends and you make stupid comments but no one acts on it. No one makes a Web site." A police official said: "In many cases, there was information put out that was very sensitive, very private and information that caused a lot of anguish. All of these girls felt exploited by it." (AP/USA Today 5 Jun 2001) http://www.usatoday.com/life/cyber/tech/2001-06-05-web-sex-gossip.htm

---

Category 11.2 *Unauthorized disclosure*

2001-11-20 **confidentiality Web disclosure credit card subscribers error**

RISKS 21 77

Declan McCullagh of Wired News and moderator of the Politech list, reported, "If you subscribe to any of Ziff-Davis' computer magazines, you may want to double-check your credit-card bill next month. Ziff-Davis Media, which publishes such popular tech titles such as Yahoo Internet Life and PC Magazine, accidentally posted the personal information of about 12,500 magazine subscribers on its website. On 19 Nov 2001, ZD removed the data, which included hundreds of credit-card numbers, and said its engineers had taken steps to prevent additional security leaks."
http://www.wired.com/news/ebiz/0,1272,48525,00.html

Category 11.2 *Unauthorized disclosure*

2002-04-25 **confidential personal data storage credit card identity theft error investigation mystery**

Security Wire Digest 4 32

TOPEKA OFFICIALS STUMPED BY FILE FOUND ON WEB SITE
Topeka officials have removed a file containing personal and financial data from its official city Web site after learning the file was accessed over the Internet. Though a user would need to know the exact file name and location on a particular computer, a Washington man says he accessed the information and then contacted a local newspaper in Kansas. Using a Web browser, the man found a file listing addresses, phone numbers and, in several dozen cases, credit card numbers for participants in city recreation department programs. Officials speculate the file may have erroneously landed in the computer hosting the site during a file transfer from one computer to another as long ago as January 2000.

Category 11.2 *Unauthorized disclosure*

2002-05-08 **console log confidentiality audit trail documentation server risk management**

RISKS 22 06ff

Mark Bergman noted in RISKS that he was surprised at the detail and length of the console log record kept by a diagnostic service processor on a server; it included full details of remote reconfiguration sessions. Mr Bergman warned everyone to be aware of just how detailed an audit trail any network device keeps so that appropriate security can be imposed.

Category 11.2 *Unauthorized disclosure*

2002-11-20 **database ZIP password crack software hacker penetration ftp data leakage confidentiality**

Wired News < http://www.wired.com/news/print/0,1294,56481,00.html >

Using ftp to access a Microsoft server, criminal hackers and innocent users found many files accessible without significant security restrictions. One Gb-sized database was stored in a ZIP file and, ah, protected (?) using the password "dbms" -- easy to defeat using widely-available ZIP-archive-cracking software from the Internet. Later investigation showed that despite attempts by Microsoft managers to shut down the wide-open ftp site, employees continued to post confidential data to the publicly-accessible folders, ignoring internal security policies.

Category 11.2 *Unauthorized disclosure*

2002-11-21 **data leakage unauthorized disclosure costs prices consumers marketing**

NewsScan

WEB SITES LEAK AFTER-HOLIDAY SALE PRICES
Users of several shopping Web sites, including FatWallet.com and DealofDay.com, were treated to a sneak peek of post-Thanksgiving sale prices for items ranging from Kodak digital cameras to the "8 Mile" movie soundtrack — prices retailers had no intention of revealing until after the holiday. Now, shoppers in the market for an HP printer may as well wait until the price drops to $200 after Thanksgiving — 33% off the current price on the OfficeMax Web site. And Best Buy's price on a digital camera will drop to $99.99 from its current $149.99 listing. "Someone, somewhere is getting information they shouldn't be," says an OfficeMax spokesman. Target, Best Buy, Wal-Mart, Toys R Us and others have demanded that the Web sites take the information down. Most have complied, but in many cases readers have already copied the data and posted it elsewhere on the Web. Retailers are stumped over how the information got out, but promise to take retaliatory action when they find out: "We will take appropriate legal action as soon as we discover how the information got on the site and who posted it," says a spokesman for OfficeMax. (Wall Street Journal 21 Nov 2002)

Category 11.2 *Unauthorized disclosure*

2004-01-10 **privacy confidentiality error identity theft**

NYT http://www.nytimes.com/2004/01/10/nyregion/10identity.html?th

N.Y.U. notified about 1,800 of its students that their Social Security numbers, phone numbers, and names had been posted on the Internet in a list of students interested in sports. A computer technician in Massachusetts, Brian Ristuccia, republished the information on his Web site and gave it publicity. NYU officials blustered about launching criminal proceedings against Mr Ristuccia, who retorted that he informed the University about the security problem a month before mirroring the data and that it had been available through a search engine.

[MK comments: Although I think it was stupid of Mr Ristuccia to have posted the information himself, it is just as stupid of university officials to focus on blaming him for their own problem.]

Category 11.2 *Unauthorized disclosure*

2004-01-12 **privacy student personal information Social Security Number SSN New York University NYU**

RISKS; http://www.nytimes.com/2004/01/10/nyregion/10identity.html 23 13

STUDENTS' DATA ON WEB, AND NYU ON DEFENSIVE

Monty Solomon cites an article in _The New York Times_ about disclosure of personal information. This article said that New York University had posted the Social Security Numbers, and in some cases, phone numbers, of 1,800 of its students on the Internet. RISKS moderator Peter G. Neumann refers to Dave Farber's comment on this incident: around the time of this incident, NYU had just fired a network security manager who had been working on HIPAA compliance for the university.

Category 11.2 *Unauthorized disclosure*

2004-02-02 **identity theft fraud threat Department Motor Vehicles**

RISKS 23 16

SECURITY HOLES AT DMVS NATIONWIDE LEAD TO ID THEFT AND SAFETY CONCERNS

Contributor Monty Solomon says that a report by CDT documents "rampant internal fraud and lax security" at state DMV offices. This report finds that at DMVs, processes "to stop bribery and theft are lacking." Such activities threaten the reliability of drivers' licenses nationwide, says Solomon. The CDT report is titled, "Unlicensed Fraud: How bribery and lax security at state motor vehicle offices nationwide lead to identity theft and illegal driver's licenses"

Category 11.2 *Unauthorized disclosure*

2004-02-26 **data confidentiality snooping insider crime police database**

RISKS 23 23

FBI EMPLOYEE SNOOPS THROUGH CONFIDENTIAL POLICE DATABASES

Assistant Attorney General Christopher A. Wray of the Department of Justice Criminal Division and U.S. Attorney Roscoe C. Howard of the District of Columbia announced that Narissa Smalls, a legal technician in FBI Headquarters, was sentenced to 12 months in prison on charges stemming from her unlawful access of the FBI's Automated Case Support (ACS) computer system.

Category 11.2 *Unauthorized disclosure*

2004-08-18 **PHP-Fusion database backup information disclosure vulnerability**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Aug/1010983.html

August 18, SecurityTracker — PHP-Fusion publicly accessible database backups.

A vulnerability in PHP-Fusion 4.0 may allow malicious users to view sensitive data. Path information can be disclosed in error pages by passing invalid input or accessing scripts directly. Additionally, database backup files are placed in a publicly accessible folder with easy to guess names. A remote user can download database backup files, which contain usernames and hashed passwords. This information may allow a remote user to obtain administrative access on the target system. No solution is known at this time.

Category 11.2 *Unauthorized disclosure*

2004-09-30 **Arizona Motor Vehicle Division sensitive personal information disclosure security flaws**

DHS IAIP Daily;
http://www.tucsoncitizen.com/breaking/093004_mvd_data_securi ty.html

September 30, The Associated Press — Arizona MVD has online information security flaws.

The Arizona Motor Vehicle Division's (MVD) information security system has flaws that can expose sensitive personal information, according to a report released Thursday, September 30. The Auditor General's Office said it found no actual security breaches, but auditors detected numerous circumstances that created the potential for misuse of information. Besides data like driver's license numbers, the sensitive information included names, addresses and Social Security numbers. The MVD said it accepted all of the auditors' findings and recommendations and had already started making changes to fix noted shortcomings.

Category 11.2 *Unauthorized disclosure*

2004-09-30 **CIA information sharing intelligence community espionage initiative**

DHS IAIP Daily; http://www.fcw.com/fcw/articles/2004/0927/web−info−09−30
−04. asp

September 30, Federal Computer Week — Spies work on info sharing.

Officials in the intelligence community have started several initiatives related to information technology tagging, collaboration and acquisition to improve data-sharing among intelligence personnel. One program uses control interfaces to share classified and unclassified data among employees, the Department of Defense, and civilian agencies, according to Alan Wade, chief information officer for the CIA. Another program allows members of the intelligence community to communicate via instant messaging, he said.

Category 11.2 *Unauthorized disclosure*

2004-10-19 **Google Desktop Search sensitive information disclosure share computer risk cybercafés security risk no update issued**

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml?artic
leID=50500707

October 19, Associated Press — New Google search tool poses security risk.

People who use public or workplace computers for e-mail, instant messaging and Web searching have a new security risk to worry about: Google's free new tool that indexes a PC's contents for quickly locating data. If it's installed on computers at libraries and Internet cafes, users could unwittingly allow people who follow them on the PCs, for example, to see sensitive information in e-mails they've exchanged. That could mean revealed passwords, conversations with doctors, or viewed Web pages detailing online purchases. Marissa Mayer, director of consumer Web products at Google Inc. said managers of shared computers should think twice about installing the software until Google develops advanced features like password protection and multi-user support.

Category 11.2 *Unauthorized disclosure*

2004-12-02 **government agencies lock down desktop security sensitive data disclosure prevention**

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml;jsess
ionid=TCYMTS5YRH1B0QSNDBGCKHSCJUMEKJVN?articleID=54202021

December 02, InformationWeek — Government agencies lock down desktops.

The Defense and Energy departments are leveraging desktop technologies to shore up security and better protect sensitive U.S. government data. The U.S. Department of Defense is leveraging PC blades to address a longtime concern that electromagnetic waves and stray currents or voltages containing key characteristics of classified data could be intercepted by enemies of the United States and used to reconstruct that classified data and compromise national security. The Energy Department has been shoring up security since it learned that as many as several hundred of its computers were stolen, lost, or improperly inventoried at Los Alamos National Laboratory between 1999 and 2002. For these two departments, security starts at the desktop, where new configurations are being deployed to keep data safely stored away on back-end servers.

Category 11.2 *Unauthorized disclosure*

2005-01-10 **hackers George Mason University personal information faculty students names photos Social Security numbers campus ID numbers identity theft**

EDUPAGE; http://news.com.com/2100-7349_3-5519592.html

HACKERS HIT GEORGE MASON

George Mason University has become the latest institution of higher education to be the victim of hackers' accessing personal information of faculty and students. University officials said that hackers gained access to information including names, photos, Social Security numbers, and campus ID numbers for "all members of the Mason community who have identification cards." An e-mail sent by the university's vice president for information technology indicated that the intruders appeared to be seeking "access to other campus systems rather than specific data," but the message warned that the information the hackers obtained could be used for identity theft. George Mason had ended its practice of putting Social Security numbers on ID cards, replacing them with university-generated numbers, in response to a Virginia state law that required such a change. The university maintains a database, however, that includes Social Security numbers. University officials discovered the intrusion on January 3 and said the hackers gained access to records of more than 30,000 faculty, staff, and students.

Category 11.2 *Unauthorized disclosure*

2005-01-14 **Apple Harvard student information products**

EDUPAGE; http://online.wsj.com/article/0,,SB110566157500825906,00.html

APPLE SUES HARVARD STUDENT

Apple Computer has filed a lawsuit against the operator of a Web site that revealed information about upcoming products before the company publicly unveiled them. The ThinkSecret Web site posted rumors of a sub-$500 Macintosh computer and an iPod that uses flash memory just days before those products were announced at the Macworld show. Apple has a reputation for being one of the most secretive high-tech companies concerning new products, and it alleges that the information posted by ThinkSecret was obtained illegally. The operator of the site, however, which many industry analysts regard as one of the premier rumor sites about Apple, turned out to be 19-year-old Nick Ciarelli, a freshman at Harvard. Ciarelli, who started the site six years ago, said he has done nothing wrong in collecting material to post. "My reporting practices are the same that any journalists use," he said. "I talk to sources, I confirm details, I follow up on tips and leads that I get." Intellectual-property attorney Robert E. Camors said it will be difficult for Apple to prove harm in the case because the information revealed does not constitute trade secrets as traditionally defined and because the information was not revealed sufficiently ahead of company announcements for competitors to benefit from it.

Category 11.2 *Unauthorized disclosure*

2005-01-23 **UNC hard drive personal information employees beneficiaries names Social Security numbers bank**

EDUPAGE; http://www.thedenverchannel.com/news/4121643/detail.html

UNC HARD DRIVE WITH PERSONAL INFORMATION DISAPPEARS

News of a missing hard drive at the University of Northern Colorado (UNC) in Greeley went from bad to worse when university officials revealed that the device included personal information not only for employees but also for their beneficiaries. The hard drive contained data including names, Social Security numbers, and bank account numbers for nearly 16,000 current and past employees of the university, as well as for beneficiaries, bringing the total to perhaps more than 30,000. At a meeting of about 200 university employees, UNC President Kay Norton said that although the school does not know whether the drive was stolen or was simply misplaced, the odds of theft increase as the days pass without locating the drive. Norton said, "We have to assume the worst," and UNC has launched a criminal investigation. UNC will not reimburse individuals for the costs of changing accounts to protect themselves, according to Norton, but some banks will change accounts without a charge.

Category 11.2 *Unauthorized disclosure*

2005-01-26 **data leakage unauthorized disclosure medical information Web site university FERPA legal liability pharmaceutical usage drug history**

RISKS 23 68

HARVARD UNIVERSITY DATA LEAKAGE OCCASIONS HORRIBLE PUN

RISKS moderator Peter G. Neumann reported on a case of potential data leakage:

An investigation by *The Harvard Crimson* was reported in that newspaper on 21 Jan 2005, noting that a Harvard University website, iCommons Poll Tool, for months had contained confidential information on the drug purchase history of students and employees that was easily accessible to outsiders. After *The Crimson* demonstrated this to university officials, the website was immediately shut down. Authentication information required for access was based on a Harvard ID and birthdate that were easily available on the Web. In addition, the Family Educational Rights Privacy Act (FERPA) requires that students may request a special security status for total privacy, and that status was not properly enforced. The university's drug insurer, PharmaCare, also had the same problems -- which still existed at the time of the article in *The Crimson*. This is seemingly a violation of the HIPAA legislation, which prohibits unauthorized disclosure of individual's medical records.

[I suppose if medicinal uses of marijuana were covered by insurance,
someone might have found the situation HIPAA-pot-amus-ing. PGN]

Category 11.2 *Unauthorized disclosure*

2005-01-27 **autocomplete e-mail addresses data leakage confidentiality**

RISKS 23 69

AUTOCOMPLETE… AUTOLYSIS… AUTOREPAIR… AW TO HELL WITH IT

Thom Kuhn points out the RISKS of allowing e-mail programs to autocomplete addresses:

A while ago I was listening to a public affairs program on NPR. One of the speakers was representing a trade association, and his comments really got to me. I Googled him and sent him a somewhat venomous e-mail. A few hours later I got an even more venomous reply. End of story? Not quite. My e-mail address was now in his shortcut list. A few weeks later I was copied on what was clearly meant to be an internal and confidential e-mail from this gentleman to this colleagues.

Category 11.2 *Unauthorized disclosure*

2005-02-02 **Acer Australia privacy breach confidentiality customer details shoppers Web site e-mail orders**

NewsScan; http://australianit.news.com.au/articles/0

PRIVACY BREACH AT ACER SITE

Acer's online customers suffered a major privacy breach after the computer maker's Australian shopping website exposed their personal details to other shoppers using the service. The online shopping portal www.shopacer.com.au revealed purchase order information including names, delivery addresses, e-mails and contact numbers of customers who had recently placed orders at the site. Customer credit card numbers were not disclosed. Customers who logged on to the site to check the status of their equipment orders via a bookmark stored in their web browser were freely able to access order details of other customers. (The Australian 2 Feb 2005)

Category 11.2 *Unauthorized disclosure*

2005-02-04 **data leakage Word comments document confidentiality**

RISKS; http://tinyurl.com/43dhg 23 71

ANOTHER MS-WORD INFO LEAK

Richard Akerman wrote about a case where a scientist made marginal comments about a press release from the McGill University Health Centre about health risks of Viox. The comments, made in MS-Word, were supposedly restricted but were actually visible to anyone using Windows XP and MS Word 2003.

Category 11.2 *Unauthorized disclosure*

2005-02-10 **Mailman flaw mail list software password information disclosure Apache vulnerable update issued**

DHS IAIP Daily; http://news.com.com/Flaw+in+mail−list+software+leaks+passwor ds/2100−1002_3−5571576.html?tag=nefd.top

FLAW IN MAIL-LIST SOFTWARE LEAKS PASSWORDS

A previously unknown vulnerability in Mailman, a popular open-source program for managing mailing lists, has led to the theft of the password file for a well-known security discussion group. The theft, discovered last week and reported in an announcement to the Full Disclosure security mailing list on Wednesday, February 9, casts uncertainty on the security of other discussion groups that use the open-source Mailman package. By specially crafting a Web address, an attacker can obtain the password for every member of a discussion group. Servers that run Apache 2.0 and Mailman are suspected to be immune to exploitation of the vulnerability, according to a security advisory on the Mailman Website. Vendor update is available: http://www.gnu.org/software/mailman/security.html

---

Category 11.2 *Unauthorized disclosure*

2005-02-18 **ChoicePoint data leakage consumer privacy Equifax credit bureau Social Security numbers SSN reports identity theft**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A33802-2005Feb18.html

CHOICEPOINT LEAKS CONSUMERS' DATA

ChoicePoint, a spinoff of credit reporting agency Equifax, has come under fire for a major security breach that exposed the personal data records of as many as 145,000 consumers to thieves posing as legitimate businesses. The information revealed included names, addresses, Social Security numbers and credit reports. "The irony appears to be that ChoicePoint has not done its own due diligence in verifying the identities of those 'businesses' that apply to be customers," says Beth Givens, director of the Privacy Rights Clearinghouse. "They're not doing the very thing they claim their service enables their customers to achieve." In its defense, ChoicePoint claims it scrutinizes all account applications, including business license verification and individuals' background checks, but in this case the fraudulent identities had not been reported stolen yet and everything seemed in order. ChoicePoint marketing director James Lee says they uncovered the deception by tracking the pattern of searches the suspects were conducting. (Washington Post 18 Feb 2005)

Category 11.2 *Unauthorized disclosure*

2005-02-26 **bank customer data loss encryption failure transportation security airline baggage magnetic backup tape identity theft**

RISKS; http://news.bbc.co.uk/1/hi/business/4300371.stm 23 76

BofA LOSES BACKUP TAPES IN TRANSIT WITH CUSTOMER DATA

Bank of America "lost computer tapes containing account details of more than one million customers who are US federal employees." The data were unencrypted. Nicolai E M Plum added, "There is another more general RISK, since the theft occurred on a commercial airline flight. There is a conflict between wishing to lock your luggage to prevent theft from luggage handlers (a group of people known to steal from luggage) and being told that if you lock your luggage the lock may be forced open and destroyed by the Transport Security Administration searching your bags - you can't win. The "TSA [master] key" lock idea will just mean the thieving baggage handler will acquire one of the master keys beforehand."

Category 11.2 *Unauthorized disclosure*

2005-03-03 **penetration hacking admissions Website ethics**

EDUPAGE; http://www.siliconvalley.com/mld/siliconvalley/11044063.htm

HACKER EXPOSES ADMISSIONS RECORDS

A hacker who was able to access admissions records for dozens of business schools posted instructions online for how applicants could access those records. Among the universities whose records were exposed were Harvard University, Stanford University, Duke University, Carnegie Mellon University, and Dartmouth College. All of the affected schools use an online application and notification system called ApplyYourself. The vulnerability that allowed the unauthorized access has been fixed, but during the nine hours in which the systems were exposed, several hundred students attempted to find out if they had been accepted to schools to which they applied. Final decisions and notifications of acceptance are not expected for several more weeks. School officials have been able to identify at least some of the applicants who gained access to the records systems, and officials from some schools said such activity would factor into the admission decision. Steve Nelson of Harvard's MBA program said, "Hacking into a system in this manner is unethical and also contrary to the behavior we expect of leaders we aspire to develop." Even if a student saw a decision, said Nelson, that decision isn't final until March 30. San Jose Mercury News, 3 March 2005

Category 11.2 *Unauthorized disclosure*

2005-03-08 **penetration hacking Harvard admissions Website reject applicants**

EDUPAGE; http://online.wsj.com/article/0,,SB111029921614173536,00.html

HARVARD REJECTS APPLICANTS WHO PEEKED

Officials from the Harvard Business School said they will reject 119 applicants who used a hacker's instructions to try to find out whether they had been accepted by the school. Calling the action "unethical" and saying that it cannot be rationalized, a statement from Harvard said, "Any applicant found to have done so will not be admitted to this school." Administrators at Carnegie Mellon University have also said they will reject candidates who attempted to gain unauthorized access to admissions records. Applicants to several other institutions affected--including Stanford University, Duke University, and Dartmouth College--will have to wait to find out how those schools decide to treat the situation. Using the instructions posted online by a hacker, applicants were able for a short period to use a name and password to access the admissions records. Institutions have been able to identify applicants who accessed admission records based on the name and password. For many who looked, there was no decision in the system, and school officials stressed that even if an applicant located an answer, those decisions were not necessarily final. Some have criticized Harvard officials for responding too harshly to the incident. Wall Street Journal, 8 March 2005 (sub. req'd)

Category 11.2 *Unauthorized disclosure*

2005-03-09 **hacker penetration publisher database Reed Elsevier personal information disclosure FBI US Secret Service**

EDUPAGE; http://news.com.com/2100-1029_3-5605736.html

HACKERS COMPROMISE PUBLISHER'S DATABASE

Hackers compromised a database owned by publisher Reed Elsevier, gaining access to names, addresses, Social Security numbers, and driver's license numbers of about 32,000 individuals. Other information, including credit history and financial data, was reportedly not involved. The breach happened at Seisint, a data-collection company that the publisher bought last year. Seisint is a competitor to ChoicePoint, which recently reported an incident in which hackers accessed records on 145,000 individuals. According to officials at Reed Elsevier, the fraud came to light when a billing complaint from a customer showed unauthorized activity with a user name and password. Reed Elsevier is contacting the individuals affected and working with the FBI and the Secret Service to locate the hackers. CNET, 9 March 2005

Category 11.2 Unauthorized disclosure

2005-03-11 **penetration hacking admissions Website reject applicants criticism**

EDUPAGE; http://chronicle.com/prm/daily/2005/03/2005031104n.htm

SCHOOLS CRITICIZED OVER REJECTION OF NOSY APPLICANTS

A number of business-school applicants who were rejected due to their looking at university admissions records online without authorization have spoken out against the universities' decision to exclude them. Carnegie Mellon University, Harvard University, and MIT have rejected the applications of 153 individuals who used a hacker's instructions to try to find out if they had been accepted. Although some applicants involved acknowledged that accessing the records was wrong, they contended that the actions do not constitute hacking and that the institutions have overreacted. One rejected applicant wrote a letter to Harvard, admitting a "lapse in judgment" but noting that he "wasn't trying to harm anyone and wasn't trying to get an advantage over anyone." Len Metheny, CEO and president of ApplyYourself, the software that all the affected schools used for applications, said the procedure to access the records was sufficiently complicated that anyone doing so would have to have known it was unauthorized. Chronicle of Higher Education, 11 March 2005 (sub. req'd)

Category 11.2 Unauthorized disclosure

2005-03-21 **personal data information disclosure California State University Chico**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=7964776

HACKERS HIT CSU CHICO

Joe Wills, spokesperson for California State University, Chico, said that hackers who broke into servers at the university may have accessed confidential records on 59,000 individuals associated with the institution. Wills said that early investigation of the attack, which happened three weeks ago, indicates that the perpetrators might have been trying to download files when they discovered the confidential information. Social Security numbers were part of the compromised records, which included students, former students, prospective students, and faculty. Reuters, 21 March 2005

Category 11.2 Unauthorized disclosure

2005-03-21 **personal data information disclosure University of Nevada at Las Vegas SEVIS database**

EDUPAGE; http://chronicle.com/prm/daily/2005/03/2005032102t.htm

UNLV SEVIS DATABASE COMPROMISED

The FBI and officials at the University of Nevada at Las Vegas (UNLV) are investigating an incident in which hackers gained access to the school's Student and Exchange Visitor Information System (SEVIS) database. SEVIS is the federal program that colleges and universities must use to track international students and faculty. According to a university spokesperson, the break-in was uncovered while it was happening, prompting optimism that the damage was thereby minimized.
The university said that the hackers had access to personal records, including birth dates, countries of origin, passport numbers, and Social Security numbers, on about 5,000 current and former students and faculty. Chronicle of Higher Education, 21 March 2005 (sub. req'd)

Category 11.2 Unauthorized disclosure

2005-04-01 **University of Georgia personal sensitive information disclosure e-portfolio system**

EDUPAGE; http://chronicle.com/prm/weekly/v51/i30/30a04102.htm

GEORGIA UNCOVERS MISUSE OF ONLINE PORTFOLIOS

After discovering files containing personal information on its e-portfolio system, officials at the University of Georgia are reviewing the institution's policies for online portfolios. A student in the university's New Media Institute--part of the school's journalism program--had used the e-portfolio system to store a list of names and credit card numbers on a university-owned server. Officials at the school are not sure how the student obtained the list, which came from a North Carolina company that sells pharmaceutical products online, or what the student intended to do with it. The server where the file resided was immediately taken down, and officials are now combing through the rest of the files before re-posting them, looking for any other inappropriate information. According to Scott Shamp, director of the New Media Institute, the incident has raised questions about how long and under what terms the university will offer online portfolio services to its students. Shamp, who expressed support for online portfolios, pointed to the possibility of third-party options to address concerns over liability for the institution. Chronicle of Higher Education, 1 April 2005 (sub. req'd)

Category 11.2 *Unauthorized disclosure*

2005-04-06 **personal data information disclosure University of Mississippi**

EDUPAGE; http://msnbc.msn.com/id/7407401/

U. OF MISSISSIPPI WEB PAGE SHOWED PERSONAL DATA

Officials at the University of Mississippi have removed files from their servers that included names and Social Security numbers for about 700 students after being notified that the files were available to anyone on the Web. The files were not linked from other pages, but they had been indexed by search engines. As a result, an individual identified only as Jay who was searching the Web for an old friend stumbled on the files. According to Jeff Alford, assistant vice chancellor for university relations, the files were posted by someone who no longer works for the university. That person likely posted them in late 2003, but university officials are not sure why he did so. "For some reason, he saved the information as a backup file on the university (Web) server," said Alford. "It is a clear violation of our privacy policy, and a serious violation." MSNBC, 6 April 2005

Category 11.2 *Unauthorized disclosure*

2005-04-12 **personal data information disclosure alumni Tufts University**

EDUPAGE; http://news.bostonherald.com/localRegional/view.bg?articleid=78100

TUFTS DISCLOSES DATA BREACH

Officials at Tufts University have begun notifying 106,000 alumni that their personal information stored on a university computer may have been compromised. The problem occurred last fall, when university officials noticed unusually large amounts of information passing through the computer, which stored names, addresses, phone numbers, Social Security numbers, and credit card numbers. The problem does not affect current students or employees. According to Betsey Jay, director of advancement communications, no evidence has surfaced about who is responsible or that any of the information was misused. At the time, officials at Tufts saw no reason to notify those affected, but a flurry of recent incidents in which personal information was compromised, including one at Tufts's neighbor, Boston College, prompted the university to inform alumni about the problem. Boston Herald, 12 April 2005

Category 11.2 *Unauthorized disclosure*

2005-04-12 **data leakage theft anomaly outlier bandwidth utilization file sharing investigation university**

Boston Globe
http://www.boston.com/business/technology/articles/2005/04/12/tufts_warns_al
umni_on_breach/

TUFTS WARNS OF POSSIBLE SECURITY BREACH

Tufts University in Boston had to send warning letters to 106,000 alumni warning of a possible breach of security on a computer that stores their names, addresses, and other personal information including (for some alumni) Social Security numbers and credit-card numbers. The possible breach was discovered by data center staff who noticed an unusually high use of high-bandwidth file transfers from that system. Investigators hypothesize that the system might have been commandeered for illegal file sharing.

Category 11.2 *Unauthorized disclosure*

2005-04-12 **LexisNexis data loss personal information disclosure identity ID thieves**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=8159934

LEXISNEXIS DISCLOSES MORE DATA LOSSES

LexisNexis this week revealed that much more personal information was exposed to identity thieves than reported in estimates released last month. Information including Social Security numbers for 310,000 U.S. Citizens was exposed--nearly 10 times the 32,000 previously announced by company officials. According to LexisNexis, the data were compromised in a total of 59 separate incidents over the past two years, most of them at subsidiary Seisint, which LexisNexis bought in July 2004. A spate of data breaches lately has prompted the U.S. Congress to hold hearings on problems affecting the data-brokerage industry and to propose regulations that would add strict controls on the collection and sale of personal information. Sen. Charles Schumer (D-N.Y.) said, "When a company like LexisNexis so badly underestimates its own ID theft breaches, it is clear that things are totally out of hand." Reuters, 12 April 2005

Category 11.2 *Unauthorized disclosure*

2005-04-21 **hacking penetration Carnegie Mellon University data breach personal information disclosure**

EDUPAGE; http://msnbc.msn.com/id/7590506/

CARNEGIE MELLON DISCLOSES POSSIBLE DATA BREACH

Officials from Carnegie Mellon University are notifying about 5,000 students, graduates, and staff that their personal information may have been compromised on the university's network. The exposed information concerns graduates of the Tepper School of Business from 1997 to 2004; current graduate students; applicants to the doctoral program from 2003 to 2005; applicants to the MBA program from 2002 to 2004; and administrative employees. Officials said information about faculty and undergraduate students was not affected. Mike Laffin, spokesperson for the university, said the problem was discovered on April 10 and that there is currently no evidence that any of the exposed personal information has been used for fraudulent purposes. MSNBC, 21 April 2005

Category 11.2 *Unauthorized disclosure*

2005-04-28 **data leakage privacy confidentiality drivers' licenses identity theft mail malfunction bug error government agency**

RISKS; http://tinyurl.com/9yfvb (reg'n req'd) 23 86

HUNDREDS OF TEXAS DRIVER'S LICENSES MAILED TO WRONG PEOPLE

An agency that warns Texans not to share personal information with strangers because of the risks of identity theft mistakenly mailed hundreds of driver's licenses to the wrong people. The Texas Department of Public Safety (DPS) blamed the mixup on a malfunctioning machine that was recently installed to sort licenses for mailing. Statewide, at least 500 to 600 people who applied for a license renewal or replacement in late March or early April instead received somebody else's card, said DPS spokesperson Tela Mange. A driver's license contains enough personal information for thieves to open up a line of credit or a bank account in that name, make long-distance phone calls or apply for a Social Security card, according to the Texas attorney general's office. Information on the license includes a full name, signature, birth date, height, eye color, address and a photograph. The driver's license number, assigned by DPS, is also used by many agencies to verify a person's identity. In the case of the mismailed licenses, no identity theft or other crime has been reported, Mange said. [Abstract by Peter Gregory]

Category 11.2 *Unauthorized disclosure*

2005-04-29 **hacking penetration personal sensitive informatioin disclosure Florida International Univerity identity ID theft**

EDUPAGE; http://www.theregister.com/2005/04/29/fiu_id_fraud_alert/

FIU SUFFERS COMPUTER HACK

Officials at Florida International University (FIU) are warning faculty and students about possible identity theft after it was discovered that a hacker had user names and passwords for 165 computers on campus. Although only a few of the computers contained personal information, and despite the fact that no evidence exists that anyone's information has been misused, school officials fear that the hacker may have had enough access to put the university's entire network in question. University staff have been instructed to inspect 3,000 computers on campus to determine if they have been compromised. FIU has recommended that faculty and students remove any personal information from their computers and that they monitor their credit cards for suspicious activity that could indicate fraud. The Register, 29 April 2005

Category 11.2 *Unauthorized disclosure*

2005-05-21 **hacking penetration Valdosta State University security breach personal information disclosure identity ID theft**

EDUPAGE; http://www.wsbtv.com/news/4515697/detail.html

VALDOSTA INVESTIGATES SECURITY BREACH

Officials at Valdosta State University (VSU) are investigating a security breach in which a computer hacker may have accessed personal information for as many as 40,000 students and employees. Last week, a hacker gained access to a campus server that contained information for the university's VSU 1Cards, which serve both as ID and debit cards for students and staff. The Georgia Bureau of Investigation is looking into the matter and has advised those affected to notify credit reporting agencies about the possible theft. The database that was accessed contained information on all VSU students since 1997, current employees of the institution, and employees who left between 1997 and 1999. A similar breach occurred last month at Georgia Southern University. Associated Press, 21 May 2005

Category 11.2 *Unauthorized disclosure*

2005-05-21 **university data leakage confidentiality privacy social security numbers SSN student faculty records**

http://www.indystar.com/apps/pbcs.dll/article?AID=/20050521/NEWS01/50521
0449/1006&template=printart

PURDUE WARNS OF ANOTHER SECURITY BREACH

For the third time in the past year, Purdue University in West Lafayette has experienced a computer security breach that may have allowed illegal access to confidential faculty or student records.

University officials said Friday they are alerting 11,360 current and former employees that their Social Security numbers and other information may have been accessed electronically from at least one of four campus computer workstations.

"It is critical that we all -- whether involved in this incident or not -- monitor our credit reports and financial statements," James R. Bottum, vice president for information technology, said in a prepared statement. "The problem we've experienced here is just one example of how vulnerable all organizations can be."

[Excerpt from a report by Barb Berggoetz, writing for the Indiana Star newspaper]

Category 11.2 *Unauthorized disclosure*

2005-06-24 **hacking penetration vandalism University of Connecticut security breach personal sensitive information disclosure Social Security Numbers**

EDUPAGE; http://www.nytimes.com/2005/06/25/technology/25conn.html

UNIVERSITY OF CONNECTICUT DISCOVERS SECURITY BREACH

Officials at the University of Connecticut have discovered a breach of one of the university's servers, which contained personal information for about 72,000 individuals. According to Michael Kerntke, a spokesperson for the school, the university found a program on the server that could have given a hacker access to the information on that computer, which included names, addresses, phone numbers, Social Security numbers, and dates of birth. Although the program has evidently been on the server since October 2003, officials said there was no evidence that any of the data had actually been taken. Kerntke noted that the program seems to have been part of a broad Internet attack rather than one specifically directed at the university. As a result, he said, "the attacker most likely had no knowledge of the kind of data stored on the server." New York Times, 24 June 2005 (registration req'd)

Category 11.2 *Unauthorized disclosure*

2005-06-24 **personal sensitive consumer information disclosure data broker ChoicePoint Social Security Numbers**

EDUPAGE; http://online.wsj.com/article/0,,SB111957007176668246,00.html

CHOICEPOINT CHANGES PRACTICES TO AVOID REPEAT DISCLOSURE

Following the high-profile loss of personal information on nearly 145,000 individuals, data broker ChoicePoint said it will make significant changes to its business procedures to prevent future security breaches. In its reports, the company will begin masking Social Security numbers, and it will limit the amount of business it conducts with certain customers, including private investigators, collection agencies, and small financial companies. ChoicePoint has also begun offering access to individuals--at no charge--to the information that the company keeps on them. Though not widely advertised, the new service provides one annual report of "personal public records" searches. ChoicePoint currently maintains a vast database of information culled from public and business records on nearly every adult in the United States. After the security breach that exposed so many individuals to identity theft, Congress held hearings on ChoicePoint and other data brokers and is considering tightening regulation of the data industry. Wall Street Journal, 24 June 2005 (sub. req'd)

Category 11.2 *Unauthorized disclosure*

2005-07-06 **student applicants university database privacy data leakage vulnerability accessibility control confidentiality Web**

RISKS; http://www.theregister.co.uk/2005/07/06/usc_site_cracked/ 23 93

UNIVERSITY OF SOUTHERN CALIFORNIA ONLINE APPLICATIONS SYSTEM FLAWED

A programming error in the University of Southern California's online system for accepting applications from prospective students left the personal information of ``hundreds of thousands of records'' publicly accessible. The flaw was discovered by a student in the process of applying.

[Abstract by Peter G. Neumann]

Category 11.2 *Unauthorized disclosure*

2005-07-06 **vulnerability flaw University of Southern California online application system Website applicant data exposure**

EDUPAGE; http://www.theregister.co.uk/2005/07/06/usc_site_cracked/

FLAW ALLOWS ACCESS TO USC ADMISSIONS SITE

Officials at the University of Southern California (USC) acknowledged that a flaw in the school's online application system left personal data on applicants to the university exposed to hackers. The vulnerability was discovered by a student, who found the problem when he was was using the system to apply to USC. He reported it to Internet security firm SecurityFocus, which then notified the university. The flaw reportedly exposed information including names, birth dates, and Social Security numbers on many thousands of applicants. After being notified of the problem, USC initially disabled only the log-in functionality but has since taken down the entire application. USC officials disclosed neither the number of individuals whose data was affected nor whether it would notify those affected. Under a recently enacted California law, consumers must be notified in the event that their personal information has been accessed without authorization. The Register, 6 July 2005

Category 11.2 *Unauthorized disclosure*

2005-08-03 **Cisco security breach passwords reset search engine vulnerability source code not exposed**

DHS IAIP Daily;
http://www.computerworld.com/developmenttopics/websitemgmt/s
tory/0,10801,103661,00.html

CISCO PASSWORDS RESET AFTER WEBSITE EXPOSURE

Cisco Systems Inc. is resetting passwords for all registered users of its Cisco.com Website after discovering a vulnerability in its search engine software that left user passwords exposed, the company said Wednesday, August 3. The passwords are used by Cisco customers, employees and partners who have registered on the Website to get access to special areas of the site or to receive e-mail alerts, said Cisco spokesperson John Noh. Cisco was made aware of the problem early Monday and corrected it immediately, Noh said. As a precaution, the company is now in the process of sending out new passwords to all registered users of Cisco.com, who will be unable to access password-protected areas until they receive their new passwords, Noh said. Noh could not say how long it will take to send out all of the new passwords. The vulnerability could not be exploited to gain access to sensitive information like Cisco's source code, he said. "We do not believe any sensitive data were compromised as a result of this."

Category 11.2 *Unauthorized disclosure*

2005-12-02 **information disclosure psychological records school Massachusetts**

RISKS; 24 11
http://www.boston.com/news/education/k_12/articles/2005/12/02/school_psychologists_student_records_accidentally_posted_online/

STUDENT PSYCHOLOGICAL INFORMATION DISCLOSURE

Peter Neumann summarizes an article in _Boston Globe_ article, a case of sensitive information being disclosed:

A school psychologist's records detailing students' confidential information and personal struggles were accidentally posted to the school system's Web site and were publicly available for at least four months. A reporter for *The Salem News* [Mass.] discovered the records last week and alerted school officials, the newspaper said in a story Friday. To protect students' privacy, the newspaper said it withheld publishing the story until the documents were removed from the Internet, which occurred Wednesday.

Category 11.2 *Unauthorized disclosure*

2005-12-08 **Meijer superstores employee personal sensitive information SSN disclosure accidental**

RISKS 24 12

MEIJER EMPLOYEE INFORMATION DISCLOSURE

RISKS contributor James Bauman received a letter about his daughter's health insurance benefit choices from her employer, Meijer Stores. However, the letter was not addressed to his daughter, and contained personal information about another Meijer employee. Mr. Bauman notes:

Because the other person had waived his benefits like my daughter had, there was little information. But, if the person had chosen a benefits package and had decided to cover their dependents, then the following information for the dependents would have been listed: names, relationship, birth date, sex, and social security number.

When Mr. Bauman telephoned Meijer about this information-disclosure problem, they said that they were aware of the issue: they asked employees who had received someone else's letter to destroy it.

Mr. Bauman concludes:

I hope their employees do the right and honorable thing, and do not use the identifying information for nefarious purposes, but we all know that the lamp of Diogenes would go out when within a mile of a few people…the ones we all worry about.

[Summary by Karthik Raman]

Category 11.2 *Unauthorized disclosure*

2006-01-05 **privacy confidentiality data leakage quality assurance QA error**

RISKS; http://tinyurl.com/oy2hz 24 14

GIFT LABEL VIOLATES PRIVACY

Some consumers may be dismayed to find their Social Security numbers printed on unsolicited packages from H&R Block, the result of a recent labeling blunder at the company.

The packages, which H&R Block mailed in December, contained free copies of the company's tax preparation software, TaxCut. By mistake, some of the packages also displayed recipients' Social Security numbers, which were embedded in 47-digit tracking codes above mailing labels.

[Contributed by Leigh Blankenship]

Category 11.2 *Unauthorized disclosure*

2006-02-20 **university school student records confidentiality integrity identity theft Web site availability**

RISKS; NZ Herald http://tinyurl.com/fpvrs 24 17

AUSTRALIAN CANTERBURY UNIVERSITY STUDENT RECORDS VULNERABLE

Thousands of [AU] Canterbury University students had their personal information exposed when online services were shut down leaving private records available to anyone with a user code and password last night. Information such as IRD numbers, transcripts, results, outstanding payments, medical conditions, and personal addresses could all be easily accessed online and could be changed by system users. The university's information technology department shut down the webfront. The university had installed a new online system late last year but there had not been any problems until now.

[Abstract by Peter G. Neumann]

11.3 Data theft

Category 11.3 *Data theft*

1997-07-10 **Web vandalism hackers credit card**

AP

In early July, 2397 customers of the ESPN Sportszone and nba.com received anonymous letters containing the last eight digits of their own credit cards. Both Web sites were sited on the Starwave hosting service. The message said, "You are the victim of a careless abuse of privacy and security. This is one of the worst implementations of security we've seen." The perpetrators claimed to be "an anonymous organization seeking to make the Internet a safe place for the consumer to do business." Although none of the credit card numbers seemed to have been used fraudulently, Starwave managers warned customers to get new credit card numbers as a precaution.

Category 11.3 *Data theft*

1998-01-06 **privacy bank data leakage confidentiality inside job QA**

RISKS 19 53

An employee of a Japanese bank offered to sell detailed customer records to a mailing-list company. Happily, that firm immediately contacted the bank and the scam was stopped.

Category 11.3 *Data theft*

1999-04-08 **criminal hacker investigation data diddling police penetration**

UPI

In East Lansing, MI a criminal hacker broke into a police computer through a faulty Web site and stole information with tips about rioters who trashed the town after "their" team lost a basketball game.

Category 11.3 *Data theft*

1999-10-05 **criminal hackers crackers theft fraud Web pages sites**

BBC MONITORING EUROPEAN - POLITICAL

In late September 1999, Czech police arrested a criminal hacker who was trying to sell stolen personal information about 2.5M users of Internet accounts. The 21-year-old was an employee of the Ceska Sporitelna savings bank and he confessed to the crime.

According to Czech criminal hackers interviewed on Czech radio in October, the state of security on most Czech Web sites is poor; however, the hackers tend to avoid police computers because of possible massive retaliation.

Category 11.3 *Data theft*

2000-03-17 **data theft credit card fraud**

NewsScan

In January 1999, a computer vandal stole information on 485,000 credit cards from an e-commerce site and then secretly stored them in a database on a U.S. government agency's Web site. Although the theft was discovered last March (1999) when a government administrator noticed that "a lot of the memory (on the Web site) was chewed up for no reason, so he checked and found the file (containing the stolen data)," many of the credit cards remain in use today because credit card companies and card-issuing credit unions decided that it would be too much trouble to shut down the accounts and issue new numbers, according to an unnamed source. There is no evidence that the any of the cards have been used to commit fraud, and Secret Service spokesman Jim Macken says investigations point to an Eastern European perpetrator. It's unclear why the data were deposited on a government Web site, although Macken suggests that it may be the online equivalent of thumbing one's nose at U.S. authorities. Later the same day, the Secret Service announced that it had tracked down a foreign criminal reponsible for the theft of the credit card information and the misuse of government computer resources. Negotiations were in progress for extradition of the suspect. MSNBC claimed that some of the cards had in fact been used for fraud.

Category 11.3 Data theft

2000-03-26 **criminal hacker penetration credit-card theft investigation arrest**

NewsScan, CNet http://cnet.com/news/0-1007-200-1590629.html, FedCIRC http://www.fedcirc.gov/news_2000.html

In March 2000, eighteen-year-old Raphael Gray was arrested in Wales on charges of Internet fraud following a joint investigation by the FBI and Welsh police. Gray and an unnamed accomplice had allegedly hacked into nine e-commerce sites, stealing credit card information on 26,000 accounts in the U.S., Canada, Thailand, Japan and Britain. Among the credit cards compromised was one belonging to Microsoft chairman Bill Gates. Gray, who calls himself the "Saint of E-Commerce," said, "I just wanted to prove how insecure these sites are. I have done the honest thing, but I have been ignored." Gray and his accomplice e-mailed the credit card details to NBCi, a subsidiary of the NBC broadcasting group.

Category 11.3 Data theft

2002-05-23 **penetration confidentiality data theft credit reports**

RISKS 22 09ff

According to a story excerpted in RISKS by Dave Hansen, >Officials still aren't sure who, or how, someone snatched 13,000 credit reports through Ford Motor Credit Co.'s Grand Rapids office." What they are sure about, however, is that no more credit reports will be stolen -- at least from this group. "We're not sure how this happened, to be honest," said Melinda Wilson, spokeswoman for Ford Motor Credit. "We thought we had a tight system. We're going to have an even tighter system now." The reports provided the intruders with a wealth of information, such as Social Security numbers, credit ratings, account numbers for bank accounts and credit cards, and creditors names and payment histories, Experian said.< Hansen commented, "Apparently, someone was able to steal credit reports from Experian by masquerading as Ford Motor Credit. They don't know how, but it won't happen again. Very confidence inspiring…."

Category 11.3 Data theft

2002-09-12 **penetration data theft employee spam**

NewsScan

LYRIS LISTS TARGETED FOR SPAM
Lyris Technologies, an e-mail list management company, says it's received reports that some of its customers' mailing lists may have been compromised. The company says it's looking into spam complaints that may involved hundreds of thousands of list subscribers, and has hired an outside consulting firm to sort through the evidence. It's also investigating whether a disgruntled employee might have stolen its lists. "In the envelope world of marketing, lists are routinely stolen by employees that are moving to another company," says Jason Catlett, president of Junkbusters, who notes that spammers especially covet lists of validated e-mail addresses belonging to a targeted group. "I don't have any evidence that that happened in this case, but it's happened in the offline world, and it wouldn't be implausible if it happened online." (CNet News.com 11 Sep 2002)
http://news.com.com/2100-1023-957567.html?tag=fd_top

Category 11.3 Data theft

2003-12-19 **hacker password cracking penetration database Acxiom Corporation**

RISKS; http://www.securityfocus.com/news/7697 23 8

Chats led to Acxiom hacker bust

Kevin Poulsen, SecurityFocus, 19 Dec 2003:

A Cincinnati man who plead guilty Thursday to cracking and cloning giant consumer databases was only caught because he helped out a friend in the hacker community. Daniel Baas, 25, plead guilty on 18 Dec 2003 to a single federal felony count of "exceeding authorized access" to a protected computer for using a cracked password to penetrate the systems of Arkansas-based Acxiom Corporation -- a company known among privacy advocates for its massive collection and sale of consumer data. The company also analyzes in-house consumer databases for a variety of companies. From October 2000 until June 2003, Baas worked as the system administrator at the Market Intelligence Group, a Cincinnati data mining company that was performing work for Acxiom. As part of his job, he had legitimate access to an Acxiom FTP server. At some point, while poking around on that server, he found an unprotected file containing encrypted passwords. Some of those passwords proved vulnerable to a run-of-the-mill password cracking program, and one of them, "packers," gave Baas access to all of the accounts used by Acxiom customers -- credit card companies, banks, phone companies, and other enterprises -- to access or manage consumer data stored by Acxiom. He began copying the databases in bulk, and burning them onto CDs. …

http://www.securityfocus.com/news/7697

Category 11.3 *Data theft*

2004-02-13 **ATM automated teller machines banks card number PIN theft reader radio**

RISKS; http://www.utexas.edu/admin/utpd/atm.html 23 19

INTERESTING DEVICE TO STEAL ATM ACCOUNTS

A team of organized criminals is installing equipment on legitimate bank ATMs in at least 2 regions to steal both the ATM card number and the PIN. The team sits nearby in a car receiving the information transmitted wirelessly over weekends and evenings from equipment they install on the front of the ATM (see photos). If you see an attachment like this, do not use the ATM and report it immediately to the bank using the 800 number or phone on the front of the ATM.

The equipment used to capture your ATM card number and PIN is cleverly disguised to look like normal ATM equipment. A "skimmer" is mounted to the front of the normal ATM card slot that reads the ATM card number and transmits it to the criminals sitting in a nearby car. At the same time, a wireless camera is disguised to look like a leaflet holder and is mounted in a position to view ATM PIN entries.

The thieves copy the cards and use the PIN numbers to withdraw thousands from many accounts in a very short time directly from the bank ATM.

Category 11.3 *Data theft*

2004-05-06 **skimming fraud identity theft**

DHS IAIP Daily;
http://www.epaynews.com/index.cgi?survey=&ref=browse&f=view&
id=108384268562221521 2&block=

May 06, ABC News — Skimming devices implanted in Florida gas pumps.

Credit and debit cardholders in Collier County, FL, have been defrauded out of almost $500,000 since last October, by criminals who are using card skimmers inside gas pumps to make counterfeit cards for fraudulent purchases. Gas pumps are susceptible to fraud in that they can be opened with a generic key, or a screwdriver, and a skimming device can quickly be attached to the payment hardware inside the pump. By this means, the thieves obtain all the details for counterfeiting cards, namely card numbers and PINs, which can be sold over the Internet for $20 to $100 per card. Debit cards, which link directly to consumers' bank accounts, are particularly vulnerable to cloning, as the bank account can be drained while the card is still in the cardholder's possession, and banks may need convincing that the fraud actually happened. South Florida's transient population makes it a target for card thieves, and to this end, some gas stations are asking card-paying customers to provide their zip code as an additional means of verification.

Category 11.3 *Data theft*

2004-05-17 **Cisco networking source code leak data theft**

DHS IAIP Daily; http://news.com.com/2100−7349−5213724.html

May 17, CNET News.com — Cisco investigates source code leak.

An unspecified amount of the proprietary source code that drives Cisco Systems' networking hardware has appeared on the Internet, the technology giant acknowledged early Monday, May 17. News of the latest source code leak appeared on a Russian security site, SecurityLab.ru, on Saturday, May 15, two days after its administrators received the leaked source code. According to SecurityLab.ru, online vandals had compromised Cisco's corporate network and stolen about 800MB of source code. A person with the alias "Franz" bragged about the intrusion and posted about 2.5MB of code on the Internet relay chat (IRC) system not long after the alleged break-in. "Cisco is aware that a potential compromise of its proprietary information occurred and was reported on a public Web site just prior to the weekend," said Jim Brady, a spokesman for the company. "The Cisco information security team is looking into this matter and investigating what happened." Brady could give no further details on the matter. This is the second time this year that a major technology company's product source code has been made public without authorization. It's uncertain to what degree the leaked code will affect Cisco security.

Category 11.3 *Data theft*

2004-05-18 **source code theft Cisco Terry Albertstein IOS 12.3 internet main backbone**

NewsScan

CISCO INVESTIGATING SOURCE CODE THEFT

Cisco has launched an investigation into "a potential compromise" of its intellectual property, a company official says, following reports that some versions of its IOS had been stolen by an individual who broke into the company's corporate network. Terry Alberstein, director of corporate affairs for the Asia-Pacific, said the alleged break-in was not due to any vulnerabilities in Cisco equipment, software or services. He said the company had been made aware of the issue before the weekend, after a report appeared on the Russian security news portal, securitylab.ru. The report said an individual had broken into Cisco's corporate network and stolen the source code for IOS 12.3 and 12.3t. Version 12.3 is used across the Internet's main backbone. The individual who claimed to have accessed Cisco System's corporate network, boasted about it on an underground Internet relay chat channel, claiming that the total amount of data in the archives was around 800 megabytes. Two snippets of code were provided as proof of the claims. (The Age 18 May 2004) rec'd from John Lamp, Deakin U.

Category 11.3 *Data theft*

2004-09-01 **portable handheld digital assistant PDA computer security theft loss encryption confidential data**

DHS IAIP Daily; http://www.theregister.co.uk/2004/09/01/pda_sec/

September 01, The Register — PDA security still dismal.

Worker apathy about PDA security is putting corporate data in jeopardy. The storage of the names and addresses of corporate customers on PDAs is now common - but security practices are struggling to keep up with technology usage. Two thirds of users do not use any kind of encryption to protect confidential data on mobile devices, according to a survey commissioned by Pointsec Mobile Technologies and Infosecurity Europe. The Mobile Vulnerability Survey 2004 found that a third of users do not even use password protection on their devices, leaving the information vulnerable to opportunists, hackers or competitors. The survey findings show that one of the fastest and easiest ways to access corporate data is through unprotected PDAs that are lost or stolen, as they contain business names and addresses, spreadsheets and other corporate documents. One in eight (13 percent) of respondents to the survey have lost their mobile device.

Category 11.3 *Data theft*

2005-01-11 **data theft university records SSN identity theft server crackers**

RISKS; http://www.gmu.edu/prod/alerts/supportcenter/index.jsp?ID=1157 23 66

GEORGE MASON UNIVERSITY LOSES CONTROL OF ID DATA

James Bauman wrote in RISKS:

The server at George Mason University in Virginia was compromised by crackers who stole personal information ("names, photos, Social Security numbers and (campus ID) numbers of all members of the Mason community who have identification cards") on 30,000 students, faculty, and staff.

The mega-risk here is obvious -- tens of thousands of people who may become victims of identity theft, one of the fastest growing crimes in America.

Category 11.3 *Data theft*

2005-03-08 **data theft credit card customer retail store database delayed discovery credit card**

RISKS; nce.lycos.com/home/news/story.asp?story=47512557 23 78

CREDIT INFORMATION STOLEN FROM DSW STORES

Credit card information from customers of more than 100 DSW Shoe Warehouse stores was stolen from a company computer's database over the last three months, a lawyer for the national chain said Tuesday. The company discovered the theft of credit card and personal shopping information on Friday and reported it to federal authorities, said Julie Davis, general counsel for the chain's parent, Retail Ventures Inc. The Secret Service is investigating, she said. DSW was alerted by a credit card company that noticed suspicious activity, she said.

Category 11.3 *Data theft*

2005-04-14 **data theft compromise personal information social security numbers SSN drivers' license unauthorized access identity theft database**

RISKS; http://tinyurl.com/89ql3 23 84

310,000 LEXIS-NEXIS RECORDS ACCESSED BY IDENTITY THIEVES

Peter G. Neumann summarized a major data-theft case:

The saga of hacked personal information continued with a report as we go to press that Lexis-Nexis admitted to having been victimized by the theft of personal records of 310,000 people (10 times more than originally reported), including SSNs and drivers' license numbers. 59 cases were discovered of access by unauthorized persons using legitimate IDs and passwords. 64,145 of those lost records involved California residents.

Monty Solomon added:

A computer security breach at Polo Ralph Lauren Corp. that has recently roiled two major credit card companies actually occurred last fall. But Polo only made the problem public on 14 Apr 2005.

Category 11.3 *Data theft*

2005-04-15 **data theft compromise personal information credit card information identity theft retail store**

RISKS; http://tinyurl.com/4upt7 23 84

POLO RALPH LAUREN CUSTOMER DATABASE ATTACKED

Peter G. Neumann summarized yet another data-theft case:

The scope of a computer system breach at a national retailer widened on 13 Apr 2005 to involve the customers of a second major credit card firm, but those companies refused to divulge the name of the retailer. The existence of the security breach first surfaced this week when HSBC North America began notifying 180,000 of its GM MasterCard customers that their credit card information had potentially been compromised. HSBC, which issues the GM cards, urged each customer to replace their card as quickly as possible.

Category 11.3 *Data theft*

2005-04-15 **data theft compromise personal information credit card information identity theft Social Security Number SSN university alumni association**

RISKS 23 84

TUFTS ALUMNI DATA COMPROMISED

Tufts University began sending letters to 106,000 alumni, warning of "abnormal activity" on their fund-raising computer system that contained names, addresses, phone numbers, and, in some cases, Social Security and credit card numbers. [Abstracted by Peter G. Neumann]

Category 11.3 *Data theft*

2005-05-20 **data theft gang collection agencies banks**

SANS NewsBites

WACHOVIA & BOA ALERT CUSTOMERS TO DATA THEFT

Wachovia Corp. and Bank of America are notifying certain active and inactive customers that the security of their personal data may have been breached. Police in New Jersey seized computer equipment, including disks that contained account information for some of the banks' customers. The account information was stolen as part of a scheme to sell the information to collection agencies.
Http://www.siliconvalley.com/mld/siliconvalley/rss/11642196.htm?template=ntentModules/printstory.jsp

Bank Data Theft Grows To 676,000 Customers (20 May 2005)

Police report that bank employees at four banks were involved in a New Jersey crime ring that used screen captures to record data about more than 676,000 customers. The criminals, nine of whom have been charged with crimes, sold the data to 40 collection agencies. The men charged are listed in the article
http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,101903,00.html

---

Category 11.3 *Data theft*

2005-05-23 **data theft financial records insider crime debt collection charges**

RISKS; http://tinyurl.com/b5khe 23 88

A BANK YOU MIGHT NOT WANT TO HAVE WACHOVIA

More than 48,000 customers of Wachovia Corp. And 600,000 of Bank of America Corp have been notified that their financial records may have been stolen by bank employees and sold to collection agencies. Nearly 700,000 customers of four banks may be affected, according to police in Hackensack, N.J. Nine people have been charged, including seven bank workers. Also affected were Commerce Bank and PNC Bank of Pittsburgh. Collection agent Orazio Lembo Jr., 35, of Hackensack made millions of dollars through the scheme. Lembo received lists of people sought for debt collection and turned that information over to the seven bank workers, who would compare those names to their client lists. The bank workers were paid $10 for each account they turned over to Lembo, Zisa said.

In a separate case with the potential for identity theft, a laptop containing the names and Social Security numbers of 16,500 current and former MCI Inc. Employees was stolen last month from the car of an MCI financial analyst in Colorado.

[Abstracts and pun by Peter G. Neumann]

Category 11.3 *Data theft*

2005-06-20 **data theft penetration criminal hackers credit card banking financial systems archiving permission policy violation virus identity theft fraud costs**

RISKS 23 91

CARDSYSTEMS KEEPS OLD DATA, GETS THEM STOLEN

CardSystems (a Tucson AZ company that handles credit card transactions for smaller banks and merchants) turns out to have been the source what was reported as the potential compromise of 40,000,000 credit cards (Visa, MasterCard, and American Express). In violation of established procedures, CardSystems was keeping old transactions online -- for research purposes -- with the intent of analyzing incompletely processed transactions. Something on the order of of 200,000 cards may be particularly at risk, and 70,000 bogus charges have already been reported. The CardSystems systems were hit with a virus that resulted in the capture of the information.

[Abtstract by Peter G. Neumann]

Category 11.3 *Data theft*

2005-08-17 **former AOL employee data theft conviction New York**

EDUPAGE;
http://today.reuters.com/business/newsarticle.aspx?storyID=nN1725168

FORMER AOL EMPLOYEE SENTENCED FOR DATA THEFT

A judge in New York has sentenced a former employee of America Online to 15 months in prison for stealing 92 million screen names from AOL and selling them to a spammer. Jason Smathers, who pleaded guilty earlier this year and cooperated with prosecutors, expressed remorse for his actions and asked the judge for leniency. Indeed, the judge could have given Smathers 24 months in prison for his crimes, which included conspiracy and interstate trafficking of stolen property. AOL has said it suffered monetary losses of $300,000 as a result of Smathers's actions. The judge in the case has given the company 10 days to prove those losses, after which he said he will impose a fine, hinting that he is leaning toward a fine of $84,000. Reuters, 17 August 2005

Category 11.3 *Data theft*

2005-08-22 **criminal hackers penetration security breach data theft personal information**

RISKS; http://www.fcw.com/article90229-08-19-05-Web 24 02

USAF PERSONNEL DATABASE COMPROMISED

Using an airman's log-in information to access the online Assignment Management System (AMS) and download data from it, someone gained access into an Air Force personnel system and accessed individual information on about half of its officers and "a handful" of its noncommissioned officers. The Air Force has started notifying more than 33,000 service personnel of the security breach, according to a statement. … Air Force officers can log in at www.afpc.randolph.af.mil/vs to see if their information was compromised. The service will call the enlisted members whose information the hackers viewed.

[Abstract by Ross Stapleton-Gray]

Category 11.3 *Data theft*

2005-09-15 **Verizon wireless lawsuit litigation data theft subscriber information accounts**

DHS IAIP Daily; http://www.mobilepipeline.com/showArticle.jhtml?articleID=17
0703409

VERIZON WIRELESS WINS INJUNCTION AGAINST DATA THIEVES

Verizon Wireless has received a court order preventing a Tennessee company from stealing subscriber information. The injunction prevents Source Resources from acquiring, possessing or selling customer account information without either a court order or the subscriber's permission. The Verizon court filing claimed that Source Resources used "deceit, trickery and dishonesty" to obtain customer records. Specifically, the wireless operator claimed that Source Resources "is engaged in wrongfully obtaining confidential customer information (such as the customer's calling records) … by posing as a customer of Verizon Wireless seeking information about his or her own account."

Category 11.3 *Data theft*

2005-09-16 **laptop data theft University of California Berkeley South Carolina recovery sensitive student information**

EDUPAGE; http://www.pcworld.com/news/article/0,aid,122576,00.asp

LOST UC BERKELEY LAPTOP RECOVERED

A laptop stolen in March from the University of California at Berkeley has been recovered, after being bought and sold several times, ultimately landing in South Carolina. When stolen, the computer contained sensitive data on more than 98,000 UC Berkeley graduate students, but by the time it was recovered, all of its files and operating system had been cleared, making it impossible to determine if the personal information was accessed after the theft. Following the theft, the university worked to contact those whose data was contained on the computer, as required by California law, and also hired an outside consultant to audit the institution's practices of handling such data, according to spokesperson Janet Gilmore. The university is currently assessing the recommendations of that audit and how to implement them. PCWorld, 16 September 2005

Category 11.3 Data theft

2006-01-10 **Bahamas data theft resort guests personal information hotel computer system**

EDUPAGE; http://news.com.com/2100-7348_3-6025591.html 23

DATA STOLEN ON RESORT GUESTS

The owners of a luxury hotel in the Bahamas announced that personal information on more than 50,000 guests was stolen from the hotel's computer system. The data stolen from the Atlantis resort on Paradise Island include names, addresses, Social Security numbers, bank account information, credit card numbers, and driver's license numbers. Representatives of the resort said they do not know whether the breach was the work of an insider or of an outside hacker. They said they have no reports so far that any of the information has been used fraudulently, but the resort is notifying all affected guests. Those affected can take advantage of a year-long credit monitoring service paid for by the hotel.

11.4 Covert channels

Category 11.4 *Covert channels*

2001-05-04 **covert channel confidentiality e-mail appropriate use spreadsheet ignorance novice user awareness education training Powerpoint presentation**

RISKS 21 39

Christopher Auger contributed an interesting scenario to RISKS about unintended disclosures. Seems that a sales director created a new organization chart on a worksheet in one of her existing Excel files. She told her secretary to forward the new chart to the entire company. Unfortunately, the secretary sent the entire Excel file, including two other worksheets. One worksheet contained highly sensitive Personnel Department information including employee salaries and sometimes disparaging remarks about specific employees. The other worksheet included a detailed plan for firing a specific, veteran salesman. The unintended disclosures caused an uproar and provided fuel for a lawsuit by the intended victim of her machinations.

Category 11.4 *Covert channels*

2001-05-11 **proprietary document formats hidden information concealed data confidentiality**

RISKS 21 40

According to Clive Page, writing in RISKS, MS-Word can generate two completely disparate texts if one uses UNIX utilities to read the files. In one case, he found a quote for equipment when he read the file using MS-Word but a quote for different equipment addressed to a different client when he used his non-Windows utilities.

Category 11.4 *Covert channels*

2001-10-08 **covert channel confidentiality e-mail appropriate use spreadsheet ignorance novice user awareness education training Excel spreadsheet paste unformatted**

RISKS 21 69

Will Middelaer noted another risk from Excel and Outlook that creates a covert channel for inadvertent data disclosure. Writing in RISK, he recounted how he and a colleague were puzzled at the size and lengthy opening of a simple e-mail message "composed of one short sentence of plain text followed by (what I thought was) a two column by ten row grid of excel cells. I put the cells into the e-mail by highlighting them in Excel, then copying and pasting them into an e-mail. What I did not know was that the e-mail message actually contained the entire 12,000 plus cells of the spreadsheet including formatting and formulas. Though it appears to contain only the 20 cells that I intended to send him, double clicking the cells in the e-mail launched Excel, which opened with a complete version of the spreadsheet from which I had selected the cells to send him. The only piece of information missing seems to be the name of the file, as it opens with a generic name."

A later posting indicated that this is a feature, not a bug: it's in the Microsoft Knowledge Base, where the text reads, "This is by design. . . ."

[MORAL: use PASTE UNFORMATTED or PASTE PICTURE when trying to send only an excerpt from an Excel spreadsheet.]

Category 11.4 *Covert channels*

2002-03-07 **covert channel eavedropping interception surveilliance privacy information warfare confidentiality**

NewsScan, RISKS 21 95FF

LED LIGHTS CAN REVEAL COMPUTER DATA
Scientists in the U.S. and the U.K. have found a way to remotely eavesdrop on a computer by monitoring the flashes of LED lights on electronic devices. Optical signals from the light-emitting diode lights found in computer modems and keyboards can be captured with a telescope and processed to reveal all the data passing through the device, says Joe Loughry, a computer programmer at Lockheed Martin. "It requires little apparatus, can be done at a considerable distance, and is completely undetectable. In effect, LED indicators act as little free-space optical data transmitters, like fiber optics without the fiber." Loughry says the most vulnerable devices are equipment used in low-speed, long-distance networks, such as ATMs (automatic teller machines). Corporate LANs and home Internet connections are generally not susceptible to the spying technique. Loughry says his interest in LEDs dates back to his days in graduate school: "I was working very late one night and waiting for a long file transfer to complete and I was just staring at these lights on the front of the modem and started to wonder if there was anything there." Loughry recommends locating equipment away from windows, putting black tape over the LEDs or deactivating when not in use. (Reuters 7 Mar 2002)
http://story.news.yahoo.com/news?tmpl=story&cid=581&u=/nm/20020307/tc_nm/tech_snooping_dc_1

* * *

A vigorous discussion in RISKS poured scorn on the notion that data could be read at any but very slow transfer rates from LEDs; correspondents noted that LEDs have a long persistence phase that would grossly swamp the fluctuations of any but glacially slow transfers. Commentators relegated the claims to the FUD (fear, uncertainty and doubt) bin and recalled seeing similar discussions in the alt.folklore.computers USENET group. on the other hand, some correspondents did recount personal involvement in successful data transfer experiments using diodes and light pens that were used for debugging systems.

Category 11.4 *Covert channels*

2002-03-18 **photocopier memory confidentiality data leakage**

RISKS 22 01

Alistair McDonald noted in RISKS that some modern photocopiers scan documents into memory and hold the image until paper is available. The next time someone replaces the paper, the stored image(s) get printed -- even if the person who wanted them copied has gone away. Such situations could compromise confidentiality. MORAL #1: don't assume that you know how unfamiliar machines work -- find out the details if you care about the possible consequences. MORAL #2: when designing systems, provide alerts to inform users of threats to their security. An indicator labeled "IMAGE CURRENTLY IN MEMORY" would have been nice.

Category 11.4 *Covert channels*

2003-11-14 **meta data dodgy-dosier syndrome Workshare hidden history histories information**

NewsScan

DODGING THE 'DODGY-DOSSIER SYNDROME' PROBLEM
Ninety percent of business documents are adapted from other documents, but 68% of the people doing the adapting don't know that the revised versions often contain metadata that identify the source documents, according to a study by UK software firm Workshare. The phenomenon has been dubbed "the dodgy-dossier syndrome" after the infamous UK government report on Iraq's alleged weapons of mass destruction program, a significant portion of which was found to have been copied from a 12-year-old thesis written by a PhD candidate. "There are inherent dangers due to document metadata, which identifies the historical changes within a document, author histories and document origins," says Workshare in its report. "Awareness of the term 'metadata' is low and fewer still know of its dangers." Exacerbating the problem of document adaptation is "document anarchy" — which describes the lack of standard practice in the workplace for contributing to or giving feedback on a document. "More business users are contributing to shared documents than ever before," says Workshare European VP Andrew Pearson, "and companies are losing control of what happens inside the process. Changes in the way organizations work have made this problem more acute in recent years with restructuring and flattening of the organization (bringing) these problems to the fore." (ZDNet UK 14 Nov 2003)

Category 11.4 *Covert channels*

2005-03-01 **data leakage device recognition clock skews**

RISKS; http://www.cse.ucsd.edu/users/tkohno/papers/PDF/ 23 77

COMPUTER CLOCK CHARACTERISTICS ALLOW TCP/IP DEVICE IDENTIFICATION

Tadayoshi Kohno wrote:

Together with Andre Broido and kc claffy from CAIDA, I have been working on methods for remote physical device fingerprinting, or remotely fingerprinting a physical device without any modification to or known cooperation from the fingerprintee. At a high level, our fingerprinting techniques exploit microscopic deviations in device hardware: clock skews. At a low level, our preferred technique exploits the fact that most modern TCP stacks implement the TCP Timestamps Option (RFC 1323). When this option is enabled, outgoing TCPs packets leak information about the sender's clock. This work further supports the following well-known observation: there can be security relevant information in what one might traditionally consider to be noise.

In a follow-up posting by Markus Roth in RISKS 23.80, he clarifies the precision of this kind of identification; the following is an excerpt from a much longer text:

>The authors claim that their method will allow you to learn 6 bits of information about a device. Well, 2^6 is only 64 different devices. If there are 200 million computers on the Internet, their method would divide the world into 64 groups of 3 million computers each. Your computer would look identical to 3 million other computers!

This technique would be useful to show negative but not positive results. If a laptop in Berlin gives a skew value of 26 microseconds, you can conclude that it is a different laptop than the one in New York. But if an arbitrary laptop in Berlin shows a 45 microsecond skew, you can only say that there are 3 million other computers like it. You cannot conclude that it is the same laptop that was once in New York.<

Our paper and abstract available here:
< http://www.cse.ucsd.edu/users/tkohno/papers/PDF/ >
< http://www.caida.org/outreach/papers/2005/fingerprinting/ >

Category 11.4 *Covert channels*

2005-05-01 **data leakage covert channel PDF classified report accessibility**

RISKS; http://it.slashdot.org/it/05/05/01/1314216.shtml?tid=172&tid=103 23 86

ACROBAT PDF FILES WITH "BLACKED-OUT" TEXT ARE READABLE

Bob Blakely III pointed out that using PDF files with blacked-out areas as a medium for preventing restricted information from being read does not work. In the case "of the classified report on the Nicola Calipari/Giuliana Sgrena incident[,] Italian newspaper (Corriere Della Sera) recovered and posted the classified text by performing a 'copy and paste' operation on the blacked-out sections."

Category 11.4 *Covert channels*

2005-09-22 **eavesdropping surveillance inference artificial intelligence data leakage covert channel**

Nature < http://www.nature.com/news/2005/050919/pf/050919-9_pf.html >

KEYBOARD NOISE ALLOWS INFERENCE ABOUT WHAT'S BEING TYPED

Using sophisticated artificial intelligence programs, scientists from UC Berkeley have been able to deduce what people are typing simply from the sounds of the different keys. Doug Tygar and colleagues say that they don't need to study the individual keyboard -- the programs use the differences in sounds of keys on the outer side of the keyboard vs the sounds of the inside keys. The microphones can be outside the room being monitored. Over time, the software gets better, and "Once our algorithm has ten minutes' worth of typed English, it can recover arbitrary text, such as passwords," says Tygar.

Category 11.4 *Covert channels*

2005-11-03 **breach confidentiality data leakage covert channel e-mail accidental release consequences stock exchange user ignorance training**

RISKS; http://tinyurl.com/bu6so 24 10

DATA LEAKAGE VIA SPREADSHEET SENT BY E-MAIL

Westpac…, a large Australian bank, was forced to halt trading on its shares and deliver its annual profit briefing a day early after it accidentally sent its results by email to research analysts.

A template containing past results was sent to analysts. It was soon discovered that the new figures were embedded in the spreadsheet and were accessible with via "a minor manipulation". Analysts telephoned the bank to report the error and the template was recalled.

But the damage was done. The Australian Stock Exchange was notified and trading was suspended as it appeared that some people had access to information not generally available to the market. The bank then brought forward its results announcement.

[Summary contributed by David Shaw]

Patrick O'Beirne reported that it appears that the critical data were "obscured" by using black shading on the cells involved (!).

Westpac Chief Financial Officer, Philip Chronican, said there was no evidence that the figures had been circulated and there were no signs of disorderly trading in Westpac shares. He added: "It is not just one error, it is a compounding of two or three errors ... We will obviously be conducting a full inquiry to make sure it doesn't happen again."

Category 11.4 *Covert channels*

2006-01-04 **data leakage confidentiality covert channel**

RISKS 24 14

PDF FILES MAY CARRY HIDDEN IMAGES

A colleague recently provided me with a PDF of a presentation he created using Keynote on a Macintosh. I needed to use some photographs from that document in a presentation of my own, so I used pdfimages, a public-domain tool, to extract them. Imagine my surprise when I discovered several images that were not apparent in the original, including logos for Yahoo and MSN, a snapshot of a commercial Web page, and a photograph of some former students.

I have not experimented with random files from the Web, so I don't know what tool is responsible for inserting the inadvertent images in the file, although it seems to be a classic case of using an existing document as a template for a new one. Clearly, however, PDF documents are capable of carrying images that are not visible to the casual user, and thus risk leaking information in the same way as Microsoft Word and Powerpoint.

[Abstract and commentary by Geoff Kuenning]

12.1 Wiretapping

Category 12.1 Wiretapping

1997-01-16 **wiretaps law enforcement rules proposal**

EDUPAGE

EDUPAGE reports: >The Federal Bureau of Investigation has released for public comment a new proposal for facilitating tapping of digital phone calls by law enforcement officials armed with court orders. Under the new proposal, which is significantly more modest than what the Bureau had asked for in a earlier plan, law enforcement officials would operate under a formula in which (for example) 523 phone lines could be monitored simultaneously in a place such as Manhattan. Privacy advocates oppose the FBI's plan as an unacceptable expansion of electronic surveillance. (New York Times 15 Jan 97 A8)<

Category 12.1 Wiretapping

1997-02-18 **wiretapping infowar court investigation**

Reuters

In France, the equivalent of the supreme court examined the legality of an inquiry into illegal wiretapping allegedly carried out by a government anti-terrorism unit. The unit was active in the administration of the late François Mitterand.

Category 12.1 Wiretapping

1997-05-29 **wiretapping eavesdropping privacy telephones government investigation**

Reuters

Government officials in Lebanon acknowledged for the first time that cellular phones and land lines were being systematically y tapped and the findings being distributed within the government. A parliamentary committee was formed to investigate the situation.

Category 12.1 Wiretapping

1997-07-17 **wiretap eavesdropping**

EDUPAGE

In July 1997, the telephone industry protested against FBI plans to allow continued wiretapping of conference calls even after the target leaves the conference call. The EDUPAGE editors wrote, "Arguing that the FBI's requests for expanded wiretap capabilities go beyond that agency's authority, telephone industry officials are asking the Federal Communications Commission to help them resist the FBI's proposed digital phone design, which would allow law enforcement officials to continue the wiretapping of a conference call even after the person targeted by a court-authorized wiretap drops out of the call. The phone industry claims the request would cost billions of dollars to implement and would expose it to lawsuits by civil liberties groups fighting against privacy invasions."

Category 12.1 Wiretapping

1997-08-08 **FBI wiretap warrant surveillance Internet phone**

Inter@ctive Week Online

Law enforcement agencies have long been able to obtain a tap-and-trace authorization from any local U.S. attorney. However, to be able to install a wiretap that would allow monitoring of conversations requires police to obtain authorization from a judge. As phone companies move towards sending speech over the Internet, tap-and-trace orders can actually provide full access to conversations being sent over the Net. Civil libertarians are concerned about a possible abuse of privacy; the Center for Democracy and Technology (CDT) and the Electronic Frontier Foundation (EFF) have both expressed concerns to the Federal Communications Commission. The ACLU is also concerned about the FBI's new wiretap policy.

Category 12.1 Wiretapping

1997-08-16 **wiretap bug phone eavesdropping**

UPI

A Dallas Schools Superintendant, Yvonne Gonzalez, caused anger among some employees by pursuing an investigation of corruption in the system. In mid-August, she was shocked to find possible evidence of a temporary bug on her phone — a couple of soldered wires. No other evidence of wire-tapping was found.

Category 12.1 Wiretapping

2002-06-11 **surveillance bugging eavedropping countermeasure detection wireless bugsweepers**

NewsScan

DETECTING CELL PHONES USED AS BUGGING DEVICES
An Israeli company has developed a device that can detect when a room is being bugged by a modified cell phone, which an intruder could call from anywhere in the world without it emitting a ringing tone. The phone's screen remains blank and it appears to be turned off. A co-designer of the device says, "The beauty of the cell phone as a bug is that it's an innocent looking and ubiquitous object. People trust cell phones, but modified and left in idle mode the cell phone can be used as a transmitter for up to a week. If it's connected to a power supply it can provide endless intelligence. Professional bugsweepers will ignore the cell phone frequency since the phones are so common and not suspicious." (Reuters 11 Jun 2002)
http://story.news.yahoo.com/news?tmpl=story&cid=581&ncid=581&e=4&u=/nm/20020611/tc_nm/tech_israel_netline_dc_1

Category 12.1 Wiretapping

2005-02-18 **espionage wire tapping optical cable undersea submarine military**

http://www.cnn.com/2005/US/02/18/submarine.secrets.ap/index.html

NUCLEAR SUBMARINE WOULD TAP UNDERSEA CABLES?

Intelligence analysts claimed that the new USS Jimmy Carter nuclear submarine would include equipment for tapping undersea cables, including fiber-optic cables, in addition to the usual complement of SIGINT equipment for radio communications interception.

Category 12.1 Wiretapping

2005-11-30 **wiretapping unreliable study law enforcement warrants implications Matt Blaze**

RISKS; http://www.iht.com/articles/2005/11/30/business/taps.php 24 11

STUDY: WIRETAPPING NOT RELIABLE

A _New York Times_ article discussed a study about the flaws of wiretapping done by Matt Blaze, a professor at the University of Pennsylvania. The study found that, using off-the-shelf equipment, it was possible to subvert law enforcement and other wiretapping by stopping the recorder remotely and falsifying the numbers dialed. Prof. Blaze noted, "This has implications not only for the accuracy of the intelligence that can be obtained from these taps, but also for the acceptability and weight of legal evidence derived from it".

The original article includes the following interesting detail (quoted):

* According to the Justice Department's most recent wiretap report, state and U.S. Courts authorized 1,710 "interceptions" of communications in 2004.

* To defeat wiretapping systems, the target need only send the same "idle signal" that the tapping equipment itself sends to the recorder when the telephone is not in use. The target could continue to have a conversation while sending the forged signal.

* The tone, also known as a C-tone, sounds like a low buzzing and is "slightly annoying," Blaze said, "but would not affect the voice quality" of the call."

[Abstract by Karthik Raman and MK]

12.2 Interception

Category 12.2 Interception

1997-02-06 **cellular eavesdropping scanners**

AP

Rep. Billy Tauzin, a Congressman from Louisiana, demonstrated to the House Commerce Telecommunications Subcommittee that an off-the-shelf police-frequency scanner can be modified to capture cellular phone calls in two minutes using a soldering iron and a two-inch wire. He then showed on the spot that the modified scanner could pick up a conversation between a cell-phone user and a regular telephone. The subcommittee is studying proposals to toughen enforcement of the law sponsored in 1992 by Rep. Edward Markey of Massachusetts that makes interception of cellular phone calls illegal and bans importation of foreign-made scanners capable of picking up these calls. The law also makes it illegal to sell scanners that can be altered easily to intercept cell- phone calls. Representatives of the Personal Communications Industry Association and the Cellular Telecommunications Industry Association argued that current laws, as written, are unenforceable and urged new approaches to protect privacy of wireless communications and that would include emerging technologies.

Category 12.2 Interception

1997-04-23 **Eavesdropping cellular phone mobile ECPA criminal prosecution interception**

RISKS; UPI, AP 18 75

Newt Gingrich's cell phone calls were overheard in December 1996 by a Florida couple using a radio scanner in their car. Gingrich was overheard "plotting strategy on how to deal with his ethics problems and possible attacks from opponents. This despite his promise, made the same day to the ethics subcommittee by his laywer, that he would not use his office or his allies to orchestrate a counter-attack to the charges." The snoopers brought their tape to the senior Democrat on the Congressional ethics committee; somehow a copy of the tape came into the possession of the New York Times, which published a report that caused much annoyance to all concerned. Republicans called foul, pointing out that such eavesdropping is explicitly illegal according to federal wiretapping statutes. In federal court in April 1997, John and Alice Martin were charged with wiretapping and faced fines of $5,000 each.

Category 12.2 Interception

1997-05-22 **eavesdropping packet sniffer hoax**

EDUPAGE

AT&T's WorldNet ISP was shown not to use the SSL to encrypt communications involving its account management. An engineer reported that he was able to capture other users' packets and list IDs and passwords. AT&T fielded someone who declared that the hole did not matter "because only WorldNet subscribers have access to those pages." [I guess only honest people bother to get WorldNet user accounts, eh?] However, be that as it may, it turned out the accusation was a hoax: the packet sniffers were placed on an internal LAN, not on the Internet, by system administrators gone bad.

Category 12.2 Interception

1997-09-19 **pager wireless interception eavesdropping**

RISKS 19 39, 40

The White House pager system was wide open to listeners in September; a hacker posted extensive transcripts of Secret Service and other communications from and about the First Family. Opponents of the Administration's policies on weak cryptography crowed that the case illustrated the importance of cryptography for security. The Secret Service denied that the breach was a security problem at all.

Category 12.2 Interception

1997-11-21 **pager interception eavedropping wiretapping**

AP, Washington Post, UPI, RISKS 19 35

Steve Bellovin summarized a case of digital eavedropping in NJ in August: "A New Jersey company has been charged with illegally intercepting and selling messages sent via a paging service. The messages — the content of which was sold to news organizations — were intended for delivery to the offices of various senior New York City officials, including the mayor's office and various top police and fire department officers." He added that the reason the authorities used pagers was their mistaken belief that the devices are more secure than phones. Where is PGP for pagers, wondered Dr Bellovin. In November, Steven Gessman, Vinnie Martin and Robert Gessman admitted illegally snatching the alphanumeric pager messages and divulging their contents to their paying subscribers. They were scheduled for sentencing on March 3, 1998.

Category 12.2 *Interception*

1998-01-06 **backup system management data destruction operations opsec**

RISKS 19 53

Sun Valley, ID uses a computer-based identification and authorization system using a computer-generated pass with a bar code, radio-linked scanners and computers, and so on. The system works very well. Unfortunately, after a hard disk crash in mid-December 1997, the operators found that — surprise — they had no backups for the data they lost. Thousands of users were asked to re-register with the area.

Category 12.2 Interception

1998-02-13 **RFI EMI radio-frequency interference TEMPEST eavesdropping**

RISKS 19 59

In February 1998, Martin Kuhn and Ross Anderson described a new method of using software to prevent eavesdropping via radio-frequency emissions. Ross Anderson explained in a posting to the UKCRYPTO mailing list,

>The story is as follows. Bill G gave our department $20m for a new building, and his people said that what they really wanted from our group was a better way to control software copying. So it would have been rather churlish of us not to at least look at their `problem'.

Now the `final solution' being peddled by the smartcard industry (and others) is to make software copying physically impossible, by tying program execution to a unique tamper-resistant hardware token. We wouldn't like to see this happen, and we have already done a lot to undermine confidence in the claims of tamper-proofness made by smartcard salesmen.

So Markus and I sat down and tried to figure out what we could do for the Evil Empire. We concluded that

(1) large companies generally pay for their software;
(2) if you try to coerce private individuals, the political backlash would be too much; so
(3) if the Evil Empire is to increase its revenue by cracking down on piracy, the people to go after are medium-sized companies.

So the design goal we set ourselves was a technology that would enable software vendors to catch the medium-sized offender - the dodgy freight company that runs 70 copies of Office 97 but only paid for one - while being ineffective against private individuals.

We succeeded.

In the process we have made some fundamental discoveries about Tempest. Army signals officers, defence contractors and spooks have been visibly flabberghasted to hear our ideas or see our demo.

In the old days, Tempest was about expensive hardware — custom equipment to monitor the enemy's emissions and very tricky shielding to stop him doing the same to you. It was all classified and strictly off-limits to the open research community.

We have ended that era. You can now use software to cause the eavesdropper in the van outside your house to see a completely different image from the one that you see on your screen. In its simplest form, our technique uses specially designed `Tempest fonts' to make the text on your screen invisible to the spooks. Our paper tells you how to design and code your own.

There are many opportunities for camouflage, deception and misconduct. For example, you could write a Tempest virus to snarf your enemy's PGP private key and radiate it without his knowledge by manipulating the dither patterns in his screen saver. You could even pick up the signal on a $100 short wave radio. The implications for people trying to build secure computer systems are non-trivial.

Anyway, we offered Bill G the prospect that instead of Word radiating the text you're working on to every spook on the block, it would only radiate a one-way function of its licence serial number. This would let an observer tell whether two machines were simultaneously running the same copy of Word, but nothing more. Surely a win-win situation, for Bill and for privacy.

But Microsoft turned down our offer. I won't breach confidences, but the high order bit is that their hearts are set on the kind of technology the smartcard people are promising - one that will definitively prevent all copying, even by private individuals. We don't plan to help them on that, and I expect that if they field anything that works, the net result will be to get Microsoft dismembered by the Department of Justice.

Meantime we want our Soft Tempest technology to be incorporated in as many products as possible - and not just security products!

So to Rainier Fahs, who asked: "If these rumors are true, I guess we will face a similar discussion on
free availability in the area of TEMPEST equipment. Does privacy protection also include the free choice of protection mechanism?"

I say this: our discovery, that Tempest protection can be done in software as well as hardware, puts it beyond the reach of effective export control. So yes, you now have a choice. You didn't before.<

See <http://www.cl.cam.ac.uk/~mgk25/ih98-tempest.pdf> for full details.

Category 12.2 *Interception*

1998-06-10 **cordless wireless phone interception eavesdropping**

RISKS 19 80

In Saratoga County, NY (near Albany), an unidentified woman reported to police that she had overhead a conversation placed with at least one cordless phone in which two men plotted an attack on an elderly woman. With the first names of the men in hand, the police were able to deduce the identity of one of the suspects and followed him as he drove around the intended victim's home. Police arrested three men and charged them with conspiracy. The woman refused to reveal her identity to police, probably because it is illegal to intercept wireless communications and also illegal to communicate the content of illegally-overheard wireless communications.

Category 12.2 *Interception*

1999-04-21 **surveillance microphone camera Internet**

The Times (London)

According to an article in _The Times_ of London on 1999-04-21, Philip Loranger of the US Army Information Assurance Office demonstrated that unprotected networks with workstations that have microphones or cameras are vulnerable to surveillance. "[I]ndeed, actions spoke louder than
words at a symposium last week in Virginia. He dialled into a military network and revealed that he could capture conversations or see what people were doing. The network had no intrusion-detection system attached."

Category 12.2 *Interception*

2001-01-08 **man-in-the-middle attack pager interception malicious teenager adolescent criminal hacker phreak medical information**

RISKS 21 19

Terry Carroll reported to RISKS as follows on a case of a teenager-in-the middle-attack:

AP reports that a Virginia teenager obtained a pager used by the Inova Fairfax Hospital, in Fairfax Virginia. According to the article, he then "gained access to the hospital's paging system" (the article is not clear on whether this was a hack, or what) and forwarded a physician's number to his pager.

When the physician was paged, the boy allegedly returned the calls and gave the nurses medical orders, including authorizing prescriptions and minor medical procedures (such as blood tests and oxygen administration). According to the Washington Post, he is believed to have issued "about a dozen orders."
. . . .
< http://news.findlaw.com/ap/o/1110/1-4-2001/20010104042024690.html>; also,
< http://www.washingtonpost.com/wp-dyn/articles/A14467-2001Jan3.html>.

An earlier report by the Post notes that:

The court papers and hospital say that on the overnight shift of Dec. 7-8, the youth ordered 12 treatments for six patients. His orders allegedly included prescribing the blood thinner heparin and asking for blood tests and oxygen for patients.

In each case, the orders were medically "appropriate under the circumstances," said Russell Seneca, chief of surgery at the hospital.

< http://www.washingtonpost.com/wp-dyn/articles/A13455-2000Dec15.html>

Category 12.2 *Interception*

2001-02-06 **e-mail interception privacy confidentiality bug vulnerability**

NewsScan

E-MAIL WIRETAPS
The University of Denver-based Privacy Foundation has begun calling attention to a new method of privacy invasion that allows someone to listen in on e-mail discussions. It can be defeated by disabling the Java programming language in Microsoft Outlook, Outlook Express, or Netscape 6 mail, and it doesn't affect people who use Eudora, America Online e-mail, or Web-based e-mail programs such as Hotmail or Yahoo Mail. Microsoft says the latest version of Outlook Express is not affected and Netscape says it will soon release a software patch that will eliminate the problem. (Atlanta Journal-Constitution 6 Feb 2001)

Category 12.2 *Interception*

2001-03-28 **potential interception hospital medical information privacy**

NewsScan

DIGITAL HOSPITAL
Each bed in HealthSouth's new $100-125 million hospital in Birmingham, Alabama, will have an Internet connection that doctors and nurses can use to access and update patient records. The hospital will open in 2003, and HealthSouth is considering building similar facilities in ten other U.S. cities. The company's chief executive says HealthSouth is "making reality out of something that many people have talked about but no one has attempted." (AP/USA Today 27 Mar 2001)
http://www.usatoday.com/life/cyber/tech/2001-03-27-hospital.htm

---

Category 12.2 *Interception*

2001-06-04 **cellular phone security encryption mobile interception**

NewsScan

CELL PHONE SECURITY
Rohde & Schwarz, based in Munich, Germany, is offering wireless customers in that country a cell phone that features military-grade privacy. The TopSec cell phone is being marketed to corporate executives and government officials who want to discuss sensitive issues without worrying about electronic eavesdroppers. "They're especially aimed at companies who want to be sure they're not being spied on by their competitors," says a Rohde & Schwartz spokesman, who adds that they've sold "a few hundred" TopSec models so far. He estimates the world market at 20,000 to 30,000 customers. The $3,000 device, which is a modified Siemens S35i phone with security features added, is believed to be the first mass-marketed mobile phone that offers high-quality service with a high level of encryption. The company has no immediate plans to market the phone in the U.S., but experts believe it's only a matter of time until such phones will be available in North America and elsewhere. (AP 4 Jun 2001)
http://news.excite.com/news/ap/010604/17/crypto-cell-phone

Category 12.2 *Interception*

2002-01-24 **ISP Internet service provider credit-card fraud snooping e-mail interception accusation trial prosecution**

RISKS 21 89

In Brisbane, Australia (reports Peter Deighan in RISKS), the Australian Competition and Consumer Commission began legal proceedings against the owners of an Internet service provider called Dataline.net.au for allegedly intercepting e-mails, collecting credit-card numbers, and debiting customers' credit cards without authorization.
http://203.6.251.7/accc.internet/digest/view_media.cfm?RecordID=574

Category 12.2 *Interception*

2002-02-11 **hotel Internet access proxy rerouting undocumented cache snooping interception confidentiality profiling SMTP server e-mail**

RISKS 21 91

Christian Holz discovered that the "STSN Internet Access, common at hotels. . . . re-route packets based on the service used(!)." Specifically, when he tried to reach his own SMTP server, he found that in fact his traffic was being rerouted -- without notification or permission -- to STSN's SMTP server. He concluded, "The risk: Obvious, if they can re-direct based on the service used, they could possibly see a lot of passwords by providing proxy-services for common services. In addition with the hotel-guest information, this could give an interesting profile of hotel guests. I wonder what information they can get their hands on if they have this services in Capitol-Hill hotels."

Category 12.2 *Interception*

2002-02-20 **eavesdropping interception spying confidentiality government law privacy surveillance politics information warfare**

RISKS 21 92

According to RISKS correspondent Geoffrey Bent, the government of Australia has admitted that there were violations of the Australian rules forbidding the Defence Signals Directorate from intercepting Australian communications during the notorious "Tampa" affair in which refugees picked up by that ship were the subect of intense political debate which was thought to have altered the political fortunes of the government.

Category 12.2 Interception

2002-03-12 **data leakage covert channel physical access telephoto lens**

Boston Globe http://digitalmass.boston.com/news/2002/03/12/data_leak.html

Two computer scientists were able to intercept data being transmitted via modems, routers and other electronic equipment with light-emitting diodes (LEDs) that blink as a function of data flow. Joe Loughry works at Lokheed Martin Space Systems in Denver, CO; David Umphress is Assoc. Prof. Computer Science at Auburn University in Alabama. Using a 100 mm focal-length lens coupled to a sensitive light detector, they were able to decode transmitted data at a distance of up to 100 feet (~33 m). In a related piece of research, it appears that Markus Kuhn at Canbridge University has worked out how to read daa from computer screens by analyzing the light reflected from the surrounding walls. Recommendations: move flashing lights away from windows; use duct tape to mask the lights.

Category 12.2 Interception

2002-06-27 **satellite confidential cleartext Internet**

RISKS, http://www.guardian.co.uk/international/story/0,3604,736462,00.html 22 13

Duncan Campbell, writing in _The Guardian_ (June 13, 2002):

European satellite TV viewers can watch live broadcasts of peacekeeping and anti-terrorist operations being conducted by US spyplanes over the Balkans. Normally secret video links from the American spies-in-the-sky have a serious security problem - a problem that makes it easier for terrorists to tune in to live video of US intelligence activity than to get Disney cartoons or new-release movies. For more than six months live pictures from manned spy aircraft and drones have been broadcast through a satellite over Brazil. The satellite, Telstar 11, is a commercial TV relay. The US spyplane broadcasts are not encrypted, meaning that anyone in the region with a normal satellite TV receiver can watch surveillance operations as they happen. The satellite feeds have also been connected to the Internet, potentially allowing the missions to be watched from around the globe.

Category 12.2 Interception

2003-10-19 **intercepting e-mail crime punishment privacy**

NewsScan

INTERCEPTING E-MAIL IS A CRIME

An Arizona woman was sentenced to 60 days of home detention for intercepting at least 215 e-mail messages directed to her husband's ex-wife. Law enforcement officials said Angel Lee fraudulently obtained the ex-wife's user name and password, allowing her to log in and read mail. Ex-wife Duongladde Ramsey said Lee's actions were comparable to breaking into her house and reading her diary, and the judge agreed, saying Lee's penalty is a warning to others who might be tempted to spy on others' e-mail accounts. "Privacy is still a cherished value," said U.S. District Judge Richard P. Matsch. (AP 19 Oct 2003)

Category 12.2 Interception

2004-08-24 **wiretapping prosecution trial**

NYT http://www.nytimes.com/2004/08/24/national/24tape.html?th

Back in 1996, Alice and John Martin illegally intercepted and recorded a cellular phone call involving Newt Gingrich (at that time Speaker of the House). The couple were fined $500 each for their ctrime. They gave their tape to Rep. Jim McDermott (D-WA), who cheerfully handed it over to the New York Times and the Atlanta Journal-Constitution. In August 2004, a judge finally ruled in a civil suit brought against Rep. McDermott by Rep. John Boehner (R-OH), who had been involved in the call. The judge ruled that Rep. McDermott has violated federal wiretap laws by passing on the tape.

Adam Liptak, writing in the New York Times, wrote an analysis of the legal issues involved:

"The wiretap law makes the knowing disclosure of an illegally intercepted communication both a crime and the basis for a civil lawsuit.

In 2001, however, the Supreme Court ruled that the law was unconstitutional, at least when used to punish disclosure of information about matters of public concern by people who did not themselves participate in obtaining it unlawfully.

`A stranger's illegal conduct does not suffice to remove the First Amendment shield from speech about a matter of public concern,' Justice John Paul Stevens wrote for the majority.

Judge Hogan said that decision did not protect Mr. McDermott because `he knew of the illegality of the Martins' disclosure at the time he voluntarily accepted it.'

That distinction, experts in First Amendment law said, is novel and at odds with the conventional understanding of the Supreme Court's decisions in this area."

Category 12.2 Interception

2004-08-30 **privacy e-mail law civil liberty Australia warrant SMS law enforcement access**

NewsScan

PRIVACY CONCERN OVER AUSTRALIAN E-MAIL LAW

Civil libertarians say that a proposed Australian law could allow authorities easy access to private, stored e-mails without a warrant, giving many new government bodies to access private e-mails, voicemail messages and SMS messages. Under current laws, unopened e-mails can only be accessed if they involve serious crime and only with a telecommunications intercept warrant. If the bill is passed authorities would need only a search warrant, or in some cases no warrant at all, according to online civil liberties group Electronic Frontiers Australia (EFA). (The Australian 30 Aug 2004) Rec'd from J. Lamp

---

12.3 Injection

Category 12.3 *Injection*

2005-08-09 **bluetooth wireless communications insertion attack automobile car radio fraud fake message alerts**

RISKS; http://trifinite.org/trifinite_stuff_carwhisperer.html 24 01

INJECTION ATTACKS ON CAR AUDIO

Martin Herfurt of the Car Whisperer project created a proof-of-concept device called "Car Whisperer" that allows hackers to inject audio into Bluetooth-equipped vehicles. Part of the summary is as follows:

>The carwhisperer project intends to sensibilise manufacturers of carkits and other Bluetooth appliances without display and keyboard for the possible security threat evolving from the use of standard passkeys.

A Bluetooth passkey is used within the pairing process that takes place, when two Bluetooth enabled devices connect for the first time. Besides other public data, the passkey is a secret parameter used in the process that generates and exchanges the so-called link key. In Bluetooth communication scenarios the link key is used for authentication and encryption of the information that is exchanged between the counterparts of the communication.

The cw_scanner script is repeatedly performing a device inquiry for visible Bluetooth devices of which the class matches the one of Bluetooth Headsets and Hands-Free Units. Once a visible Bluetooth device with the appropriate device class is found, the cw_scanner script executes the carwhisperer binary that connects to the found device (on RFCOMM channel 1) and opens a control connection and connects the SCO links.

The carwhiperer binary connects to the device found by the cw_scanner. The passkey that is required for the initial connection to the device is provided by the cw_pin.pl script that replaces the official Bluez PIN helper (graphical application that usually prompts for the passkey). The cw_pin.pl script provides the passkey depending on the Bluetooth address that requests it. Depending on the first three bytes of the address, which references the manufacturer, different passkeys are returned by the cw_pin.sh script. In quite a few cases the preset standard passkey on headsets and handsfree units is '0000' or '1234'.

Once the connection has been successfully established, the carwhisperer binary starts sending audio to, and recording audio from the headset. This allows attackers to inject audio data into the car. This could be fake traffic announcements or nice words. Attackers are also able to eavesdrop conversations among people sitting in the car.<

Herfurt adds, "In order to avoid getting attacked by carwhisperer, manufacturers should not use standard passkeys in their Bluetooth appliances. Moreover, there should be some kind of direct interaction with the device that allows a device to connect. Another recommendation would be to switch the handsfree unit to invisible mode, when no authorized device connects to it within a certain time."

13.1 Data diddling

Category 13.1 *Data diddling*

1997-01-11 **salami diddling fraud programming Trojan audit**

RISKS 18 75

Peter G. Neumann wrote in RISKS: "Willis Robinson, 22, of Libertytown, Maryland, was sentenced to 10 years in prison (6 of which were suspended) for having reprogrammed his Taco Bell drive-up-window cash register — causing it to ring up each $2.99 item internally as a 1-cent item, so that he could pocket $2.98 each time. He amassed $3600 before he was caught." Another correspondent adds that management assumed the error was hardware or software and only caught the perpetrator when he bragged about his crime to co-workers."

Category 13.1 *Data diddling*

1997-02-12 **data diddling intrusion**

AP

In Round Rock City, TX, the mayor's pager number started answering the phone with a rap song full of obscenities instead of the usual "Leave a message please." The mayor promised to change his pager security code more often. "I'm just glad my mother or my wife didn't try to page me," said the embarrassed official.

Category 13.1 *Data diddling*

1997-05-31 **phreaking answering machine diddling**

RISKS 19 20

After MI5 placed ads for recruits in Britain, 20,000 hopeful security agents called in only to hear a bizarre message on the answering machine: "Hello my name is Colonel Blotch. I am calling on behalf of the KGB. We have taken over MI5 because they are not secret any more and they are a very [useless] organisation."

Category 13.1 *Data diddling*

1997-06-26 **fraud identification authentication diddling sabotage**

AP

An employee of the San Mateo County District Attorney's office was accused of conspiring to have his boss, Ralph Minow, fired from his job. Paul Schmidt is accused of planting a logic bomb in his boss' computer using a fake time-stamp to make it look as if Minow had caused his own computer to crash on 97.03.26. Minow was unable to exculpate himself because the backup tapes he looked for were gone. Minow was fired and told he would be prosecuted for sabotage. However, computer security specialists noticed that one of the printouts presented as incriminating evidence of Minow's depredations had a logoff message of "Good evening" even though Schmidt claimed to have printed them in the morning. Close investigation revealed audit trails on the computer showing that someone had set the clock back to the 25th and then back. Schmidt was fired and filed a wrongful dismissal lawsuit, claiming that he was an innocent whistle-blower being persecuted for his efforts.

Category 13.1 *Data diddling*

1997-07-23 **data diddling**

PA News

In January, 30 million people called British Airways in a contest to win tickets on the Concorde aircraft. Two British Telecom employees from the same office won two of the 190 tickets — a coincidence that statisticians estimate had odds of 25 million to 1. Upon investigation, BT concluded that its employees "could have used technical knowledge to circumvent the filter system designed to let only a specified number of calls reach the ticket allocating office." The two men were fired and promptly sued for wrongful dismissal.

Category 13.1 *Data diddling*

1997-09-11 **SSN impersonation social engineering authentication verification QA quality assurance**

RISKS; AP 19 39

It is so easy for the Social Security Administration to accept death reports that someone has died that mischief-makers can easily ruin someone life if they haven't died. In Overland Park, KS Ms Kirsten Phillips was reported dead to the SSA by a non-existent brother-in-law. One week later, she was electronically revived, but by then the damage was done: government payments stopped, direct withdrawals by the government from her bank accounts, cancelled credit cards — a real mess. [SSA regulations ought to require at least one independent verification of reported death — by calling the purportedly deceased person, for instance, or requiring official documentation from a government source.]

Category 13.1 *Data diddling*

1997-10-01 **hacker vandalism**

SANS

The widely-respected SANS Security Digest was hacked in October 1997, with satirical, vulgar nonsense replacing the usual sedate text. The hacked issue began inauspiciously as follows: "Your October Network Security Digest is below. The Digest comes out eight times per year so slap mah fro. You'll also get a couple mre messages this week, and if you're lucky, uuencoded porn of my wife.

y0urs tr00ly in smut, Alan Paller and Michele Crabb

And now, what you've been dr00ling for!@#
. . .
CONTENTS:
1) pr0n (a GIF uuencoded)
2) VULNERABILITY THAT SOMEONE ELSE FOUND (exploit for SAMBA bug)
3) pr0n (a JPEG uuencoded)
4) 3l33t wAr3z (a URL)
5) H0w t0 subscr1be t0 BuGTRaQ!@#
6) m0r3 pr0n (another JPEG)
7) QUICK TIDBITS"

Category 13.1 *Data diddling*

1997-10-02 **hacking QA bank**

AAP

In Brisbane, Australia, three men charged with hacking A$1.76M by transferring the funds from the Commonwealth Bank to accounts at the Metway Bank in mid-September 1997 claimed that they were the victims of a quality assurance error. Their solicitor alleged that the Commonwealth Bank placed A$50M into a practice account that was supposed to be used for learning how to use the online system for direct payments.

Category 13.1 *Data diddling*

1997-10-24 **data diddling theft debit card bank e-commerce**

RISKS 19 42

Benoit Lavigne, writing in RISKS, reported on a curious case of data diddling. It seems that thieves broke into a picture-framing business at three in the morning on the night of Friday to Saturday. Using ten bank debit cards, the thieves instituted ten debit corrections to "refund" a total of $240,000 into their accounts from the business. The theft was bad enough, but the bank took over two weeks to reinstate the merchant's account's. One of the key vulnerabilities at the merchant's site was that the staff left a special card required to initiate transactions in the cash register. In addition, Lavigne commented, there ought to have been some mechanism on the bank side to identify the thoroughly unusual pattern of transactions and either queried them or stopped them while awaiting confirmation.

Category 13.1 *Data diddling*

1997-12-05 **data diddling taxes**

RISKS 19 48

Some Quebec restaurateurs have been using a U.S.-made computer program (a "zapper") that skimmed off up to 30% of the receipts, thereby evading Revenue Canada and provincial government tax payments to the tune of millions of dollars per year. A related story in the *Montreal Gazette* added that *Le Point* journalists succeeded in getting technical support on the zapper programs from POS equipment vendors; there seemed to be nothing unusual about the programs, judging from the matter-of-fact way the vendors responded to requests.

Category 13.1 *Data diddling*

1998-10-01 **data diddling corruption insider privacy**

RISKS 20 1

A Social Security Administration employee who become angry with a woman with whom he argued in an Internet chat room used a fellow-employee's terminal to fill in a death date for the woman in her SSA records. She applied for a loan at her bank and discovered that she was "cyberdead." Jorge Yong admitted culpability, resigned and paid $800 in fines and damages.

Category 13.1 *Data diddling*

1998-10-13 **fraud data diddling cheat chip programming inspectors salami**

RISKS 20 3

In Los Angeles, the district attorneys charged four men with fraud for allegedly installing computer chips in gasoline pumps that cheated consumers by overstating the amounts pumped. The problem came to light when an increasing number of consumers charged that they had been sold more gasoline than the capacity of their gas tanks. However, the fraud was difficult to prove initially because the perpetrators programmed the chips to deliver exactly the right amount of gasoline when asked for five- and ten-gallon amounts — precisely the amounts typically used by inspectors.

Category 13.1 *Data diddling*

2000-01-28 **quality assurance financial systems data diddling Web**

NewsScan, ZDNet
http://205.181.112.101/zdnn/stories/bursts/0,7407,2429909,00.html

As financial institutions continue to develop online innovations, . . . electronic banking got some bad news when it was discovered that the software used by the online X.Com Bank allowed customers to transfer funds from the account of any person at any U.S. bank. All they had to know was the person's account number and bank routing information. According to the company, the dollar amounts involved in fraudulent transfer were "not significant," and the security flaw has now been corrected. But security expert Elias Levy says, "Anyone with half a clue could perform these unauthorized transfers for over a month via their Web site and create some real financial problems for other people." The company's Web site boasts that its use of technology "makes accessing and moving your money easy." (New York Times 28 Jan 2000)

Category 13.1 *Data diddling*

2000-02-10 **data diddling embezzlement insider employee indictment**

New York Times

Tony Xiaotong Yu, 36, of Stamford, CT, was indicted on 2000-02-10 in NY State Supreme Court in Manhattan on charges of unauthorized modifications to a computer system and grand larceny. Mr Yu worked for Deutsche Morgan Grenfell Inc. from 1996 as a programmer. By the end of 1996, he became a securities trader. The indictment charges that he inserted a programmatic time bomb into a risk model on which he worked as a programmer; the trigger date was July 2000. The unauthorized code was discovered by other programmers, who apparently had to spend months repairing the program because of the unauthorized changes Mr Yu allegedly inserted.

Category 13.1 *Data diddling*

2000-06-15 **data diddling grade fixing scandal bribery access control logoff failure**

RISKS 20 91

Peter G. Neumann reported, "At least 20 Berkeley High School seniors (hopefully, graduating) are apparently involved in a grade altering episode. The grade program is accessible to only about 20 employees, who must use *two* passwords. (Wow, that is REAL security!) But one of the computers was most likely left logged in and unattended. One student admitted paying $10 for the change."

Category 13.1 *Data diddling*

2001-01-09 **employee background check vetting sabotage data diddling criminal hacker**

RISKS 21 19

Brian Randell noted in RISKS that some 18 months after an employee was caught in June 1999 attempting to hack sensitive data to sabotage a nuclear power station, strict new security measures were imposed on all such facilities. Apparently the perpetrator had two prior criminal convictions but no one bothered to check his background before hiring him.

Category 13.1 *Data diddling*

2001-11-26 **embezzlement stock fraud accountants data diddling theft trial guilty plea bargaining sentencing fines imprisonment**

RISKS; US Department of Justice 21 82
http://www.cybercrime.gov/Osowski_TangSent.htm

The <www.cybercrimes.gov> Web site of the US Department of Justice announced "Former Cisco Systems, Inc. Accountants Sentenced for Unauthorized Access to Computer Systems to Illegally Issue Almost $8 Million in Cisco Stock to Themselves." Highlights of the press release:

* ". . . [F]ormer Cisco Systems, Inc., accountants Geoffrey Osowski and Wilson Tang were each sentenced . . . [on 26 Nov 2001] to 34 months in prison for exceeding their authorized access to the computer systems of Cisco Systems in order to illegally issue almost $8 million in Cisco stock to themselves."

* ". . .[In] plea agreements with the government, Mr. Osowski and Mr. Tang each pled guilty to one count of computer fraud in violation of Title 18, United States Code, Section 1030(a)(4), agreed to the forfeiture of assets that the government had seized from the defendants (including stock already liquidated for $5,049,057, jewelry and an automobile), and agreed to pay restitution in the amount of the difference between $7,868,637 and the amount that the government will recover from the sale of the seized items."

* "In pleading guilty, Mr. Osowski and Mr. Tang admitted that between October 2000 and March 27, 2001, they participated together in a scheme to defraud Cisco Systems in order to obtain Cisco stock that they were not authorized to obtain. As part of the scheme, they exceeded their authorized access to computer systems at Cisco in order to access a computer system used by the company to manage stock option disbursals, used that access to identify control numbers to track authorized stock option disbursals, created forged forms purporting to authorize disbursals of stock, faxed the forged requests to the company responsible for controlling and issuing shares of Cisco Systems stock, and directed that stock be placed in their personal brokerage accounts. The two defendants admitted that the first time that they did this, in December 2000, they caused 97,750 shares of Cisco stock to be placed in two separate Merrill Lynch accounts, with 58,250 of the shares deposited in an account set up by Mr. Osowski and 39,500 shares deposited in an account set up by Mr. Tang. In February 2001, they caused two additional transfers of stock, in amounts of 67,500 shares and 65,300 shares, to be transferred to brokerage accounts in their names. The total value of the Cisco stock that they took on these three occasions (at the time that they transferred the stock) was approximately $7,868,637."

Category 13.1 *Data diddling*

2004-01-26 **Google hacking bomb manipulating search engine query results George W. Bush elections**

RISKS; http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2004/01/26/BUG3M4GVDS1.DTL 23 15

GOOGLE TARGETED BY PRANKSTERS

Monty Solomon refers us to a _San Francisco Chronicle_ article which reports that some Web site operators and bloggers were manipulating search results on Google. These pranksters exploit Google's method of ranking search results to get certain websites ranked better than others for specific queries. This way, the pranksters George W. Bush's biography appear as the top result on the queries "unelectable" and "miserable failure."

Category 13.1 *Data diddling*

2004-05-11 **hacker grade california high school student change grades data**

NewsScan

STUDENT HACKER 'MAKES THE GRADE'

A 17-year-old California high school student has been arrested and accused of a felony for allegedly hacking into his school's computer system and changing grades. The arrest came one week after school officials notified police of suspicious grade changes in the academic records of six juniors and one senior. Police Sgt. Steve Shulman says the investigation is continuing because "there may very well be other students involved." Administrators at Corona del Mar High School are examining the records of all 1,500 students to see if any other grades were altered. The charge against the student — "unauthorized alteration of computerized data" — carries a prison sentence of up to three years, but juvenile court officials and prosecutors have not yet decided whether to pursue charges in the case. A spokeswoman for the Newport-Mesa Unified School District says it appears that the records were accessed from a remote location — something that supposedly was not possible — and that the perpetrator was able to circumvent the password authorization feature: "We're upset that we were compromised and we're saddened that these students, who are obviously pretty smart, would use their intelligence for this. We're in a new age. We know that kids will find out what they can do, but we need to be clear that this is illegal — that it's not a game." (Los Angeles Times 11 May 2004)

Category 13.1 *Data diddling*

2005-04-10 **road construction message board criminal hacker joke prank speed limit**

RISKS; http://tinyurl.com/8xw8g 23 84

MICHIGAN ROADSIGN BOARD HACKED

Drivers on southbound Interstate 75 in Michigan saw a construction message board that previously had been alerting drivers in Genesee County near Clio that construction was soon to start. One morning it said "speed limit 100 mph go go go." (The speed limit in that area is 70 mph. The sign is controlled remotely by a subcontractor's computer.) [Abstract by Peter G. Neumann]

Category 13.1 *Data diddling*

2005-07-22 **Linux zlib buffer overflow data streams overflow execution**

DHS IAIP Daily; http://www.linuxsecurity.com/content/view/119860

ZLIB BUFFER OVERFLOW. ZLIB IMPROPERLY HANDLES INVALID DATA STREAMS WHICH COULD LEAD TO A BUFFER OVERFLOW

By creating a specially crafted compressed data stream, attackers can overwrite data structures for applications that use zlib, resulting in arbitrary code execution or a Denial of Service. There is no known workaround at this time.

Category 13.1 *Data diddling*

2006-05-10 **insider crime police chief database hacking data integrity alteration statistics fraud**

RISKS 24 28

NY CITY POLICY DEPUTY INSPECTOR HACKED POLIC DATABASE

According to the New York Post, a deputy inspector in the NY City Police Department (NYPD) hacked into the NYPD crime statistics database (called the CompStat program) to make his predecessor look bad by inflating old crime statistics and make himself look better by deflating current statistics. Ed Ravin commented in RISKS that "…[T]he Department …. Have stonewalled every outside investigation of this problem, especially the Mayor's Commission to Combat Police Corruption, whose chairman quietly resigned after the NYPD refused to cooperate with the Commission." He added, "The NYPD (and the many police departments worldwide who copy them) have become such slaves of their CompStat system that they spend their effort gaming it rather than doing their jobs and actually reducing crime."

13.2 Data corruption & destruction

Category 13.2 *Data corruption & destruction*

1997-02-07 **E&O errors omissions data loss destruction recovery**

RISKS 18 82

The National Association of Securities Dealers lost 20,000 records from its files because managers issued faulty guidelines which gave clerks the impression they were supposed to dispose of (too many) disciplinary records. It was estimated that recovery of the electronic records would take two months.

Category 13.2 *Data corruption & destruction*

1997-09-03 **data error QA quality assurance**

Knight-Ridder Newspapers

Lois Gates was surprised to discover in August 1997 that according to the Social Security Administration, she died in June 1997. The hale 65-year old was even more dismayed to find that the SSA had taken money out of her account in restitution for "erroneous" payments. Once the story hit the news media, the snafu was on its way to being fixed within days.

Category 13.2 *Data corruption & destruction*

1998-04-09 **data corruption disaster backups overwriting destroyed**

RISKS 19 66

At the Stanford University Graduate School of Business, system administrators installed additional disk capacity to their servers. They then reloaded files from a corrupt backup tape on 7 Mar. The faculty and student files were destroyed, leaving many faculty members and graduate students without their research files. [This incident again demonstrates the importance of VERIFYING THE READABILITY of backups. It also strengthens my belief in the wisdom of making TWO backups before attempting to reload a system.]

Category 13.2 *Data corruption & destruction*

2000-01-23 **backup failure operations quality control data loss**

RISKS 20 76

Someone responsible for the US National Archives' e-mail system did not understand the concept of a backup. In 1999, it seems that a system problem deleted about 43,000 messages. The contractor responsible for making backups had not, in fact, been doing any. Finally, someone turned off system logging because it slowed down the system. The Assistant Archivist had a brilliant, if pessimistic, view of backups, saying, "the safest way to save important messages is to print them out".

Category 13.2 *Data corruption & destruction*

2000-03-12 **QA quality assurance audit trail investigation grades**

RISKS 20 84 & 86

Mark Lutton reported in RISKS on a week-long gefuffle at MIT, when the grades of 22 students in a cell biology class were randomly altered. Initial suspicions focused on hacking, and the teacher, Harvey Lodish, told his class on 2 March 2000 that he had uncovered a cheating scandal. On March 10, the Boston Globe reported that in fact a teaching assistant had sorted the student-name column but not all the other ones, thus failing to carry all the data through the sort. Lutton suggested, "It seems to me that bound paper ledger books would be a much better tool for keeping grade records, at least for this teacher and his assistants." [Some other ideas: (1) Enable the audit-trail feature (can create large files but does record all changes); (2) keep daily backups with version numbers so that a good version of the data can be located and used quickly.]

In a later issue of the RISKS Forum Digest (20.86), correspondents Tony Lima and John Pearson both pointed out that the fundamental problem was that the teaching team was using a spreadsheet to do a database's job. Spreadsheets have no mechanism for ensuring record integrity, whereas even simple databases can protect against the kind of scrambling that occurred in this example.

Category 13.2 *Data corruption & destruction*

2000-07-10 **data corruption QA quality assurance testing**

RISKS, CNN 20 95
http://www.cnn.com/2000/TECH/computing/07/10/system.crash.idg/index.htm

Peter G. Neumann wrote, "Milan's stock exchange (Europe's fourth largest) opened 8 hours late on 5 Jul 2000, after corruption of the authorized-dealer database resulting from testing of a new covered-warrants market the previous evening — evidently a maintenance glitch. Brokers claimed losses of 20 billion lire (US$9.9M) from lost commissions. (The London exchange had an 8-hour blackout in April 2000.)"

Category 13.2 *Data corruption & destruction*

2001-06-10 **QA quality assurance incompatibility date formats platform operating system spreadsheet data corruption**

RISKS 21 47

MS-Excel on Macintosh computers uses a different date format ("1904 system") from Excel on Windows computers ("1900 system"). As a result, opening a Windows MS-Excel spreadsheet using Mac MS-Excel automatically converts all dates (and without notification). The resulting dates are exactly four years and a day earlier than the intended dates. RISKS correspondent Tom Walker noticed the well-known bug ("feature") during a legal proceeding where the error could have caused serious damage to the interests of several thousand employees. However, he wrote, "The fact that the data was presented in the course of an adversarial process was probably crucial to the error having been detected. I am wondering why there aren't more reports out there of encounters with this problem. Is this bug flying under the radar?"

Category 13.2 *Data corruption & destruction*

2001-06-19 **CD-ROM fungus destruction damage data loss corruption integrity destruction degradation**

RISKS 21 51

Scientists investigated a damaged CD in a tropical jungle in Belize and discovered a hitherto unknown fungus that "was steadily eating through the supposedly indestructible disc. The fungus had burrowed into the CD from the outer edge, then devoured the thin aluminium layer and some of the data-storing polycarbonate resin."

Category 13.2 *Data corruption & destruction*

2001-07-11 **QA quality assurance nuclear materials database data loss corruption**

RISKS 21 50

Several correspondents to RISKS commented on news that the nuclear-material-tracking software supplied to Russia by Los Alamos National Laboratory has serious bugs that cause data losses. The same software is in use in the USA as well. Since the nuclear laboraties in the USA are claimed no longer toi keep paper trails of their nuclear supplies, the data losses have serious implications for nuclear safety and world peace.

Category 13.2 *Data corruption & destruction*

2001-07-12 **QA quality assurance government records accounting database data loss corruption**

RISKS 21 50

James Paul commented on a serious government systems failure in Fiji: "A programming error resulted in the deletion of all Fiji Government accounts for the year 2000 and the postponement of official audits. There is reportedly some speculation about a cover-up of "mismanagement or abuse of taxpayer funds", although the simple solution of a screw-up seems likely. The information system dates from the mid-1970s. Presumably the various 52 government ministries and departments can retransmit the relevant data. [Source: Computer error deletes all Fiji Government accounts, Agence France-Presse, 11 Jul 2001, from the *Fiji Times*, 12 Jul 2001] "

Category 13.2 *Data corruption & destruction*

2001-08-07 **data destruction downtime availability disaster disk format bank closure delay customer relations**

RISKS 21 58

Nicolai Langfeldt wrote from Norway to report on a massive failure of the Norwegian banking system. His report in RISKS includes the following summary:

EDB Fellesdata AS runs the computer services of about half of Norway's banks. On Thursday 2 Aug 2001, they apparently installed about 280 disks in their Hitachi storage. Then, instead of initializing the new disks, they initalized _all_ their disks -- thereby wiping out the entire warehouse. EDB Fellesdata itself declines to make any statements in the case pending further contact with their customers, the banks. They are considering lawsuits, but if one of their own employees made a "user error", they may have a hard time of it.

Talk about a lot of eggs in one basket, one can only imagine how many terrabytes of database this is, considering the number of disks, and how long it takes to restore from backup, and how many transactions were waiting to be processed from _other_ banks once the restore is done. Apparently the computers were running by Sunday, card services and ATMs were available on Monday, but Internet banking and automatic-phone-banking access is limited. They have announced that updated account balances will not be available until Wednesday, the 7th day after the mishap. The concerned banks' customers could pay their bills by visiting a local branch office the whole time, but apparently the transactions had not been processed because creditors have been warned that money may be late in arriving (but presumably retro-credited once the transaction is processed?).

Category 13.2 *Data corruption & destruction*

2002-01-15 **data destruction sabotage evidence recovery forensic analysis reconstruction e-mail files data investigation**

NewsScan

DATA-RECOVERY EXPERTS LOOKING FOR MISSING ENRON E-MAIL [15 Jan 2002]
Lotus Notes e-mail messages ordered destroyed by a auditor whom Andersen has fired are now being searched by data-recovery experts using the same techniques used to look for suspected spy transmission and for Clinton White House correspondence sent by e-mail. A representative of Ontrack Data International says, "The general practitioner doesn't know that once you hit delete and get it out of your inbox that it's not gone. That is why this is a very fertile area for key evidence in litigation." Agencies such as the NSA, CIA and FBI go one extra step to keep deleted material from being recovered; they accomplish this through the use of software that repeatedly overwrites free space on hard drives. (AP/San Jose Mercury News 16 Jan 2002) http://www.siliconvalley.com/docs/news/svfront/085710.htm

---

Category 13.2 *Data corruption & destruction*

2002-03-11 **quality assurance QA design data integrity user interface documentation**

RISKS 21 94ff

A couple of correspondents wrote in to RISKS with yet another litany of complaints about Microsoft Office products that change input data unexpectedly. Both found that grades they were entering were being modified; one found that incorrect spellings were being forced, including into e-mail addresses. One complained about mysterious lines and bullets appearing in his text.

[MK comments: Everything the correspondents described is controlled through options available through the Tools menu item in Office products. Both correspondents illustrate the dangers resulting from the combination of bloatware (programs with enormous lists of functions and features) coupled with poor user interface design and inadequate training. Office products typically do not provide a visual indicator of the status of various "helpful" features such as the "AutoCorrect" and "Enable Autocomplete for Cell Values" functions. A user unaware of the existence of these functions has no clue where to look for the mysterious source of inexplicable data transformations, let alone any idea of how to turn them off.

MORAL: system administrators should set all autocorrection and autoformatting features OFF by default when delivering systems to novice users and should provide training to allow controlled reactivation of those features that the users feel will be helpful and controllable.]

Category 13.2 *Data corruption & destruction*

2002-03-12 **speech recognition default documentation data integrity corruption feature awareness**

RISKS 21 95

Hawkins Dale reported on another case of data corruption by default in RISKS:
>Slashdot (slashdot.org) and others are reporting that "some Windows XP users are finding random words inserted into their text as they write. The problem is caused by XP's speech recognition system, which is turned on by default by some manufacturers. It's listening to the random noise you get even when the mic is turned off."

Microsoft is blaming the problem on some computer manufacturers who enable this feature by default in their installation of the operating system.

Draw your own conclusions regarding the risks of adding powerful features that users are unaware of.<

Category 13.2 *Data corruption & destruction*

2002-03-19 **archives dynamic content technology change**

NewsScan

FOR LONG-TERM DOCUMENT PRESERVATION, YOU NEED TO EMULATE
RAND Corporation researcher Jeff Rothenberg says that for long-term document preservation you need to use emulation. "If you think about anything in digital form, the article itself is a program. Not the way we usually think about it, but even a string of ASCII codes is a program, a sequence of little commands, each of which is interpreted by some simple interpreter that knows how to draw those characters on the screen and knows how to do what the command says. If you don't have the right interpreter, the one that knows what each of these commands means, then you don't have the document. You might have some aspect of it, but you've lost the original's behavior. And just looking at Web pages, fewer sites consist of static HTML. There's lots of stuff that gets generated on the fly, Javascript, server-side Java, Active Server pages. If all you save is the text of those pages, you haven't got it, and that kind of convinces me that digital documents must be executable in the future to really preserve them." (IEEE Software Mar/Apr 2002)
http://computer.org/software/so2002/s2toc.htm /(sub req'd)

Category 13.2 *Data corruption & destruction*

2002-05-22 **backup disk failure data loss law enforcement police**

RISKS 22 08

Thomas Insel wrote in RISKS:

On 11 May 2002, *The New York Times* (page A13 of the National Edition) reported that the Macomb County, Michigan, sheriff's department lost over 50,000 photographs of criminals on a crashed hard drive. Not particularly exciting, except that they had wisely made hardcopy backups of some of the photos. The issue of electronic backups was never even raised. Perhaps many computer users no longer realize such a thing is possible?
http://www.nytimes.com/2002/05/11/national/11BRFS.html

Category 13.2 *Data corruption & destruction*

2002-07-22 **wrong number incorrect data QA quality assurance lawsuit penalties payment costs**

NewsScan

WRONG NUMBER COSTS GATEWAY $3.6 MILLION
A federal court has awarded a Pensacola business $3.6 million in damages from Gateway, which had accidentally distributed the wrong phone number for customer complaints to more than 275 Gateway stores. The error dated back to 1999, when someone at Gateway erred by using the 800 prefix instead of the correct 888 prefix for the company's toll-free customer complaint line. The wrong number was also posted on Gateway's Web site, listed on Internet billings and included on a form distributed to more than 100,000 Gateway customers. Mo' Money, which manufactures and distributes promotional items, said it contacted Gateway six days after the calls began, but that it took the computer company more than two years to fix the problem. "It was a nightmare," says Mo' Money president Cliff Mowe. "We had as many as 8,000 extra calls a month, and these were all angry people You couldn't get them off the line because the only number they had was ours. You'd have to explain it and go through it, and a lot of times they'd call you right back anyway." (AP 19 Jul 2002)

Category 13.2 *Data corruption & destruction*

2002-07-26 **e-mail archives storage policy removal destruction data loss**

NewsScan

HOTMAIL CLEAN-UP POLICY ANGERS USERS
Microsoft's Hotmail system has instituted a new storage policy that limits the time span for saved mail to 30 days. After that, it's automatically deleted from a user's Sent file -- an action that has left many users steaming. Desperate users who've pleaded for their mail back have been told it's irretrievable, and company officials say they warned users in mid-June of the change in policy. MSN product manager Parul Shah said users could avoid the problem by creating special folders and moving important messages out of the Sent file. The company is hoping the change in policy will prompt people to sign up for a fee-based version of the service that costs $19.95 a month for an additional 8MB of storage on top of the 2MB they get for free. Microsoft says it has more than 110 million Hotmail users, but that so far fewer than 300,000 have signed up for the extra storage feature. (CNet News.com 25 Jul 2002)
http://news.com.com/2100-1023-946430.html?tag=fd_top

Category 13.2 *Data corruption & destruction*

2002-08-02 **e-mail archives regulations securities industry regulations standards fines penalties data destruction**

NewsScan

WALL STREET BANKS DISCARDED E-MAIL MESSAGES PREMATURELY
Six prominent firms (Citigroup, Morgan Stanley, Merrill Lynch, Deutsche Bank, and U.S. Bancorp Piper jaffraye) may be fined for as much as $10 million for not keeping e-mail messages sent both within and outside the companies for three years. The penalties would come from the SEC, NASD, and the New Stock Exchange. (New York Times 2 Aug 2002)

Category 13.2 *Data corruption & destruction*

2004-11-10 **archives digital photography records storage management data corruption loss integrity**

NYT
http://www.nytimes.com/2004/11/10/technology/10archive.html?th=&pagewante
d=print&position=

Katie Hafner reported on a growing problem in November in a New York Times article: digital photographs and other records are much less stable than traditional paper documents. Amateurs lack the awareness and knowledge of the effects of technological obsolescence and are storing their precious data (home movies, photographs of loved ones, personal diaries) on media that are already unreadable because the technology is no longer available: 5" diskettes, old ZIP drives and the like. Worse still, even CD-ROMs are losing data integrity over a period of five years or so if their storage conditions are poor -- and often a single error in a critical area of a file will make the whole photo unreadable. Unlike fuzzy or scratched photos, a scratched CD-ROM may be completely unususable, with the loss of thousands of pictures.

Category 13.2 *Data corruption & destruction*

2005-03-03 **GFI security firm accidental data loss customer e-mail deletion free upgrades compensation BitDefender MailSecurity**

DHS IAIP Daily; http://news.zdnet.co.uk/0,39020330,39189933,00.htm

SECURITY FIRM DELETED CUSTOMERS' E-MAILS

An e-mail security scanning company has accidentally deleted thousands of its customers' e-mails. GFI is now offering free upgrades to all its customers after it deleted their e-mails by sending out incorrect update information. According to GFI, the problem occurred because of a change in BitDefender's technology, one of the products that GFI uses for its e-mail scanning. When the GFI MailSecurity update mechanism tried to install BitDefender updates on customer networks, the service started to delete all e-mails by default. BitDefender and GFI then rolled back the updates. GFI has promised all customers a free upgrade to its MailSecurity 9 product, which is available in two months. The company has also released a tool that can tell customers which e-mails were deleted and when.

Category 13.2 *Data corruption & destruction*

2005-04-19 **software quality assurance Web sales supervision approval error glitch bug contractual obligation financial loss integrity**

RISKS; http://tinyurl.com/ahal9 23 85

US AIRWAYS HONORS 1,000 TICKETS AT $1.86 DUE TO COMPUTER GLITCH

A computer error forced the bankrupt airline US Airways to sell over 1,000 tickets on the Web to people who payed $1.86 for each of them in mid-April 2005. News got out fast on the Web and some buyers bought ore than a dozen tickets simply to be able to swell their frequent-flyer miles for later use. US Airways honored all its contractual obligations despite the enormous cost.

Category 13.2 *Data corruption & destruction*

2005-07-11 **medical database laboratory results data integrity corruption mixup confusion error tests treatments**

RISKS; http://www.canada.com/calgary/calgaryherald/index.html 23 94

MEDICAL LAB DATABASE CORRUPTION AFFECTS 2,000 PATIENTS

[A] web database used by the Calgary Health Region to track and distribute results of lab tests has suffered a "glitch". According to the article that appeared today, "The Calgary Health Region announced Sunday that an Internet database - which physicians use to view lab work such as blood and urine tests - mixed up results between patients and posted records under the wrong names. Officials are now contacting the offices of nearly 400 doctors and other health providers who saw the incorrect records, to ensure patients are receiving proper treatment." Doctors are concerned that the mix-up means some patients are now receiving incorrect treatments which can complicate their conditions, or that patients are receiving treatments they don't need. Additionally, some patients may be fretting needlessly over their lab results because of the mix-up while others may be in for some unpleasant surprises when they receive the correct results.

[Abstract (lightly edited by MK) by R. A. Tremonti]

Category 13.2 *Data corruption & destruction*

2005-08-09 **software quality assurance QA data loss corruption integrity version control regression testing**

RISKS; http://www.heise.de/newsticker/meldung/62595 (in German) 24 01

GERMAN SOCIAL SERVICES SOFTWARE DROPS CHANGES

The online computer news service heise.de reports that an error in the software system A2LL, which computes welfare and jobless subsidies as well as administering the system, has dropped over 100,000 changes that should have been reported to health insurance providers.

New registrants, people going off welfare, address changes and the like were registered with the system and then the changes were automatically rescinded. The error cropped up after a new version of the software was installed on the central servers. [Perhaps they installed a test system by mistake that just pretends to accept changes? -dww]

The missed changes will not affect the insurance status of the people involved, but staff at the insurance companies must take care of all of the changes by hand.

[Abstract of German original by Debora Weber-Wulff]

Category 13.2 *Data corruption & destruction*

2005-11-09 **software quality assurance testing accounting error financial report**

RISKS; http://tinyurl.com/djshs 24 09

ACCOUNTING SOFTWARE BUG CAUSES $220M ERROR

"Freddie Mac will reduce its profit for the first half of 2005 by $220 million because of an error caused by faulty accounting software, the mortgage finance company said yesterday. … The error stems from a flaw in the accounting program Freddie Mac has used since 2001. In a recent review of the company's accounting system, Freddie Mac employees realized the software was routinely overstating the amount of interest that the housing finance company earned from certain types of mortgage-backed securities that it bought for investment purposes, spokesman Michael Cosgrove said."

[Contributed by Jeremy Epstein]

Category 13.2 *Data corruption & destruction*

2006-06-04 **data loss erasure destruction government suppression**

RISKS 24 31

AZNAR GOVERNMENT WIPES COMPUTER RECORDS

Miguel Gallardo reported in RISKS that the Aznar government of Spain "deleted all the Spanish Government Presidency computer systems in "La Moncloa" Official Palace after the elections (3 days after the terrorism attacks in Madrid-Atocha train station). There is a 12 thousand Euros bill just for deleting everything, even data back-ups."

Gallardo's APEDANICA public-interest organization is suing the government for destruction of public records.

Category 13.2 *Data corruption & destruction*

2006-06-11 **quality assurance QA automatic spreadsheet format conversion correction errors percentages**

Network World Security Management Newsletter

EXCEL CAN DAMAGE PERCENTAGE DATA

Warn your users to _turn off_ automated format conversion functions in Excel (or other spreadsheets) when working with production spreadsheets where complex alphanumeric codes are to be entered. It would be better to note and correct an error than to have the software silently make assumptions and modify their input, resulting in data rejection or – worse – acceptance of faulty data.

Use the Tools | Options | Edit sequence and uncheck the "Enable automatic percent entry" because it has two different rules in effect. With that option enabled, input numbers _greater_ than 1 are _divided_ by 100; e.g., entering 10 stores the value 10% (i.e., 0.1) and entering 1 stores 1% (i.e., 0.01). However, numbers _smaller_ than 1 are _not_ converted; thus .1 is stored as 10% and .01 is stored as 1%. As you can see, there are two different numbers that can result in the same stored value (yecchhh). If the data contain numbers that cross the boundary between these (not particularly obvious) rules, the numbers stored in the spreadsheet will not be those intended by the operator.

[Based on an article published in Network World Security Management Newsletter by M. E. Kabay; in press]

13.3 Embezzlement

Category 13.3 *Embezzlement*

1997-01-17 **data diddling**

PA News

Jamie Griffin, a 21-year old clerk working for London and Manchester Assurance in Exmouth, England altered computer records to hide his theft of more than £44,000. He lost all on gambling and then claimed that he had been forced to steal the money by the IRA. He eventually pleaded guilty to five charges of theft and was sentenced to seven months in jail.

Category 13.3 *Embezzlement*

1997-02-03 **Data diddling**

RISKS 18 81

Commercial customers of a major bank in the Netherlands can withdraw money directly from any bank account without permission and can falsify the text that appears in the victim's bank statement. This flaw in the security design was discovered by a minister in Friesia, the northern province of the Netherlands, when he was granted access to the accounts of his magazine subscribers. It became obvious that he had complete control over all debits and all text on victims' bank statements regardless of his original intent. Confronted with this evidence, a bank official dismissed the flaw as insignificant.

Category 13.3 *Embezzlement*

1997-03-18 **data diddling fraud**

AP

Daniel Perez, a claims processor at Unisys Corp. in Florida was accused of embezzling $1.3M by changing records in a database so that he could process claims against the fraudulent accounts. Working with confederates, the accused may have been involved in fraud totaling about $20M. Tim Moore, Florida Department of Law Enforcement Commissioner, scoffed at claims by Unisys that the discovery of the fraud as a result of auditors' work showed that their security systems were OK. ""I think anybody would suggest that Unisys use tighter security measures," said Moore.

Category 13.3 *Embezzlement*

1997-07-26 **embezzlement data diddling**

RISKS 19 26

Peter G. Neumann writes, "While working as a civilian military pay supervisor in the Army finance and accounting office at Fort Myer from 1994 to 1997, Teasa Hutchins Jr. caused regular military paychecks to be deposited to a bank account in the name of a bogus officer, and accumulated $169,000 for himself. He has pleaded guilty and faces up to 10 years in prison and a $250,000 fine."

Category 13.3 *Embezzlement*

1999-01-03 **theft fraud hackers bank impersonation crime punishment**

RISKS 20 14

Two more Chinese criminal hackers were sentenced to death in China in December 1998. According to John Knight, writing in RISKS, "One of the brothers, Hao Jingwen, opened 16 accounts under false names in September, the report said. Then he entered a branch of the Trade and Industry Bank in Zhenjiang, in Jiangsu province, and installed a piece of equipment in the bank's computer system." The twin bothers stole 720,000 Yuan (~U$87K) from a bank in Zhenjiang and transferred the money to their own accounts.

Category 13.3 Embezzlement

2005-10-21 **bank fraud identification authentication I&A personal identification numbers PINs insider crime fraud theft embezzlement test accounts algorithms inference lawsuits**

RISKS; http://www.theregister.co.uk/2005/10/21/phantoms_and_rogues/ 24 08

CONVOLUTED TALE OF THE GHOST WITHDRAWALS

Charles Arthur reported in _The Register_ on a fascinating case of incompetence and criminality in the British banking system. In "How ATM fraud nearly brought down British banking" he tell of how junior barrister (lawyer) Alistair Kelman discovered in the early 1990s that

* Thousands of people were being charged for withdrawals from their bank accounts that they did not make ("ghost withdrawals").

* Banks denied the possibility of error or fraud until experts such as Prof Ross Anderson of Cambridge University convinced the courts that the claim of infallibility was nonsense.

* There were thousands of cards which delivered money without deducting it from the owner's account -- they were actually using dummy accounts created by the programmers.

* Rogue programmers at a particular bank altered the PIN-generator to create only 3 unique PINs for all bank cards -- allowing them to steal money from any account at will.

This last discovery was very serious indeed:

>This "gave me major concern," says Kelman. "The security of the entire ATM network upon which the UK banking system was based was predicated on nobody knowing your PIN." He could see that if this reached the media, people would begin comparing PINs, and on finding identical ones would tell others, and the security system used by the banks would collapse overnight. Then there would be a dramatic run on the banks … as everyone tried to take their money to a safer place, such as under the mattress.

And there wasn't time for the banks to fix the problem if anyone went public with it. Their MTBU was too short. MTBU? That' s "Maximum Time to Belly Up", as coined by the majestic Donn Parker of Stanford Research Institute. He found that businesses that relied on computers for the control of their cash flow fell into catastrophic collapse if those computers were unavailable or unusable for a period of time. How long? By the late 1980s it had fallen from a month to a few days. That's not a good thing; it meant that a collapse of the computers that any UK clearing bank relied on would destroy it in less than a week.<

Just as Kelman was about to reveal the fatal vulnerability in a secret meeting of bank security experts in June 1993, he was dismissed by his last clients, losing the legal right to intervene in the issue. He kept quiet for more than 10 years, hoping that no one else would discover this dreadful vulnerability.

>"Fortunately for the UK banking system and the British people, nobody else did discover what I found about the activities of the Rogue Bank," Kelvin notes. Two years later, though, he had corroboration of what he had learnt: "the computing staff at the [Rogue] bank were completely out of control and engaged in multiple frauds."<

[Pointer to article contributed to RISKS by Andrew King; summary by MK using extracts from original article.]

13.4 Obsolescence

Category 13.4 *Obsolescence*

1998-04-16 **archives deterioration data loss integrity CD-ROM**

EDUPAGE

The RAND Corporation reported that CD-ROMs can deteriorate within 5-10 years — much faster than the 50 years usually quoted. This instability is quite apart from the even more serious problem of incompatibility of medium, where a perfectly good storage device becomes unreadable because of changes in technology. Ever try to read an 8-inch floppy disk from the 1970s on your DVD player?

Category 13.4 *Obsolescence*

2001-07-28 **data loss archives format medium programs programmers documentation tape**

RISKS 21 56

Valuable data from the mid-1970s collected by the Viking probes to Mars were lost over the years because no one bothered to convert the data to the next generation of medium and application program. By the time University of Southern California neurobiologist Joseph Miller asked for some records in 1999, the tapes were unreadable and uninterpretable.

Category 13.4 *Obsolescence*

2001-08-10 **backward compatibility de facto standard archives data loss**

RISKS 21 59

PDF documents created with Adobe Acrobat in 1998 were not readable using Acrobat 5.0 in 2001.

Category 13.4 *Obsolescence*

2002-04-24 **research URL stability bibliography links evanescence disappearance automated verification education**

NewsScan

RESEARCHERS FOCUS ON 'LINK ROT'
Two researchers at the University of Nebraska are focusing their attention on so-called "link rot" -- broken hyperlinks -- which are becoming an increasing concern for professors and teachers who assign reading and research activities using the Web. The two professors monitored 515 hyperlinks over a period of 20 months and found that at the end of the time, 18.8% of the links had disappeared -- over 11% of the .org links, 18.4% of the .edu links, and 42.5% of the .com links were no longer active at the end of the study. Broken links included resources from the Mayo Clinic, an encyclopedia of plant biology, links on steroid use and links to courses with relevant lecture notes. The study also found that a few of the links had redirected to porn sites, which could be a real concern for teachers of younger students. The two professors are now working on a grant proposal to the National Science Foundation to develop software that would automatically check links for faculty and alert them by e-mail if the URL or content changes. (Wired.com 24 Apr 2002)
http://www.wired.com/news/school/0,1383,51700,00.html

Category 13.4 Obsolescence

2002-08-30 **archives obsolescense virtual computer emulation**

NewsScan

'UNIVERSAL VIRTUAL COMPUTER' BATTLES OBSOLESCENCE
A researcher at IBM's Almaden Research Center has proposed a system he hopes will eliminate the problem of digital document obsolescence, which threatens to undermine archivists' efforts to retain digital material for future generations. Dr. Raymond Lorie has developed a prototype for a "universal virtual computer," which features architecture and language designed to be so logical and accessible that computer developers of the future will be able to write instructions to emulate it on their machines. The software written for the universal virtual computer extracts all the data stored in a file, but does not try to include all the bells and whistles associated with that file. "I don't need to recreate Acrobat Reader with all its buttons and colors," says Lorie. "That would be overkill." Instead, the program uses tags to include extra semantic information that will indicate what the file is and how to read it. These semantic tags might say, for instance, "There is text in this document and it is organized like this," he explains. John Steenbakkers, director of information technology for the Dutch national library, says the universal virtual computer concept works. "We have seen a proof of concept. If the universal virtual computer became a standard for digital archiving, it would be a major step forward," offering a controlled, one-time migration to a specific preservation format. Meanwhile, Jeff Rothenberg of the RAND Corporation says Lorie's idea of data extraction is limited. "I would prefer to store documents in their original forms and formats -- with all of the software that created them and is typically required to view them." Data extraction "will give you the contents -- or rather, what someone thought were the meaningful core contents -- in some future form. But it won't preserve the original." (New York Times 29 Aug 2002)

14.1 Viruses

Category 14.1 Viruses

1997-02-04 **Macro virus**

RISKS 18 81 ff

The ISO/ANSI C++ Standards Committee was hit by the Word Concept virus, suspending a meeting of 60 top-level programming experts for 20 minutes. The contributor to RISKS, Nathan Myers, noted an additional risk: ". . . causing users who know better than to run the buggy software laughing themselves silly at those who don't, and then getting punched in the nose."

Category 14.1 Viruses

1997-02-06 **UNIX virus LINUX**

Business Wire

The Bliss virus infects LINUX systems and was described on the USENET in the autumn of 1996. In February 1997, it was again reported in Linux and Bugtraq mailing lists. Someone sent the virus to McAfee, which erroneously published a news release claiming discovery of the virus and development of the first LINUX scanner. However, Dave Kennedy, Group Leader of the NCSA's Research, Education and Consulting Group, wrote, "They have no legitimate claim of discovery. And one of the Linux guru's has an MD5 based Linux scanner, but tripwire works too. So they have no legitimate claim to the first scanner either."

Category 14.1 Viruses

1997-02-19 **Virus (Mac)**

RISKS 18 83

PhotoDisc Inc. distributed a CD-ROM containing a virus-infected copy of Acrobat 3.0 in mid-February. Letters sent to customers did not admit that the company had distributed a virus, but rather described the problem as a "corruption" which could be cleared up by a "utility" that turned out to be a well-known free anti-virus program.

Category 14.1 Viruses

1997-04-15 **viruses**

NCSA

The ICSA's annual virus prevalence survey showed that despite increasing use of anti-virus products, three times more infections were reported in 1996 than in 1995. Macro viruses caused more than half of all virus infections. E-mail attachments are now an important vector for infection.

Category 14.1 Viruses

1997-07-31 **virus data corruption delay report**

AP

UN plans to approve food shipments to Iraqi children were delayed when an Iraqi document arrived at UN HQ on a virus-infected diskette. The virus caused a delay of a few days.

Category 14.1 Viruses

1997-10-02 **virus QA quality assurance**

Reuters

Compaq Computer Corporation shot itself in the virtual foot in September when 10% of its new Presario computers produced in Taiwan and shipped to Japan contained a virus apparently introduced at the manfacturing plant.

Category 14.1 Viruses

1998-06-23 **macro virus e-mail confidentiality posting newsgroups USENET**

RISKS 19 83

Mikko Hypponen of DataFellows Group in Finland wrote: A Word macro virus called WM/PolyPoster was recently found. As the number of macro viruses is soon reaching 3000, there's nothing special about this. However, under the right conditions, this virus sends copies of a victim's Word documents to 23 different Usenet newsgroups under subject lines like "New Virus Alert!," "Important Princess Diana Info" and "How to find child pornography." The spamming and breach of confidentiality are bad enough, but the virus also infects readers who download the infected documents.

Category 14.1 Viruses

1998-09-04 **virus macro Word Excel**

Computerworld News Wire

The "W97/X97M Shiver" virus was discovered by Network Associates. It cross-infects documents of both Microsoft Word and Excel programs. Infected documents are difficult or impossible to open successfully. A free diagnostic routine was available at <http://beta.nai.com/public/datafiles/>.

Category 14.1 Viruses

1998-12-21 **macro virus e-mail attachment Word**

New York Times
http://www.nytimes.com/library/tech/98/12/biztech/articles/21virus.html

The virulent "MS Word 97 Macro Class Virus" increased its prevalence in the last months of 1998, becoming a major irritant for victims confronted with pop-up messages stating "<Victim's user-name> is a big stupid jerk." Some victims' servers had so many alerts that they crashed simply because of the volume of infected documents. Apparently written by notorious virus-writer "Vicodin," who distributed many new viruses through the Internet. There were over 40 variants of this macro virus by the end of 1998. In addition to the annoying pop-ups, the viruses also modified the system registry, altering the Windows entry for company name to "Dr. Diet Mountain Dew" and the user's name entry to "VicodinES/CB/TNN," references to the "Code Breakers" and "The Narcotic Network" groups of virus-writers. For more information on the Class macro viruses, see <http://www.geocities.com/SiliconValley/Heights/3652/CLASS.HTM>.

Category 14.1 Viruses

1999-01-21 **virus contamination sabotage disgruntled employee**

Los Angeles Times

Zhang Wenming, a disgruntled Beijing programmer, confessed in January 1999 to infecting 20,000 of copies of educational software with a dangerous virus whose payload included erasing a victim's hard disk. Apparently the 28-year-old self taught programmer was furious at being fired for "poor work habits" and wreaked his revenge on his employer in the last days of his employment.

Category 14.1 Viruses

1999-02-08 **virus confidentiality privacy encryption key**

RISKS 20 19

The Codebreakers, virus writers with more technical skill than good sense or ethical sensibilities, wrote the Caligula virus, which sends users' PGP secret key ring to their FTP site. [This large virus illustrates the dangers of data transfer from inside the firewall and also the stupidity of a legal system that cannot recognize that virus code is not speech and should not be constitutionally protected. Cryptographers recommended that secret-key rings either be stored off the hard disk entirely when not in use or that all data on the disk be encrypted.]

Category 14.1 Viruses

1999-04-26 **Chernobyl virus CIH perpetrator virus writer history**

News wires

According to news wire reports, the Chernobyl computer virus struck hundreds of thousands of computers in Asia and the Middle East, with Turkey and South Korea each reporting 300,000 computers damaged on 26 April. Singapore reported more than 100 cases of infection by the Chernobyl virus (AKA CIH or Space Filler) on that date, the anniversary of the nuclear plant meltdown in 1986. One source estimated that 10% of all the PCs in the Gulf Emirates were affected by the virus, which writes garbage into the BIOS and can erase hard drives.

Category 14.1 Viruses

1999-05-03 **virus creator law enforcement plaintiffs hacker**

Australian Financial Review

Although 24-year-old Taiwanese information technologist Chen Ing-hau admitted writing the Chernobyl virus (also called CIH, the authors initials), local prosecutors were unable to charge him with anything because no one local had complained about the virus. Mr Chen apologized for the damage caused to hundreds of thousands of computers in Bangladesh, China, India, South Korea, Turkey, and many other countries with poor anti-virus precautions in place.

Category 14.1 Viruses

1999-08-19 **virus payload latency trigger logic bomb Windows operating systems**

Wall Street Journal

The Command anti-virus company announced discovery of the Win32.Kriz.3862 virus, which runs successfully under Windows 95, 98 and NT. This logic bomb would detonate on Christmas day; its payload includes massive overwriting of data on all data storage units and also damage to the BIOS. However, the virus had not been found outside the lab and so would be a low to medium risk, according to the researchers.

Category 14.1 Viruses

1999-09-02 **Word 97 macro virus**

PC Week Online, Computerworld

In mid-August, Symantec announced discovery of a dangerous MS-Word 97 macro virus called "Thursday" with a trigger date of 13 Dec. The virus turns off macro warnings in MS-Word. This virus was seen in the wild on about 5,000 computers in Austria, France, Germany, Ireland, Latvia, Poland, Switzerland, the UK, and the US. The payload can erase all files on the C: drive. All major anti-virus companies issues updates to their signature files to catch this virus.

Category 14.1 Viruses

1999-09-09 **virus macro worm**

PC World Online

Computer Associates International discovered a dangerous new virus/worm called Cholera. This laboratory virus sent itself through e-mail attachments to all available e-mail addresses found on a MAPI-compliant system. The virus/worm sent a message with a smiley face symbol and an attachment called "setup.exe" which foolish users might execute. The virus portion would then load itself into memory and insert software keys into WIN.INI and the Windows 9x registry file.

Category 14.1 Viruses

1999-10-11 **virus WindowsNT TSR terminate-stay-resident**

Network World Online

The WinNT.Infis virus was the first NT-specific virus found in the wild (in Russia). The virus was described as having a novel stealth mechanism.

Category 14.1 Viruses

1999-11-01 **free antivirus software Microsoft Y2K preparations**

InfoWorld Electric, Microsoft www.microsoft.com/y2k

Microsoft contracted with nine anti-virus product vendors to distribute their software free on its Web site. The move was described as preparation for particularly heavy virus attacks during the Y2K transition. Participants included Central Command, Computer Associates, Data Fellows, Network Associates, Norman ASA, Panda Software, Sophos, Symantec and Trend Micro.

Category 14.1 Viruses

1999-11-12 **virus Windows NT patch security kernel**

Newsbytes

The W32.FunLove.4099 virus discovered by the Symantec AntiVirus Research Center (SARC) in November, attacks Windows NT in a new way: by patching the security kernel. The virus modifies file access so that all files are accessible to any user — a perfect setup to allow a criminal hacker to wreak havoc on an infected system.

Category 14.1 Viruses

1999-11-19 **virus damage cost production factory**

Reuters

Dell Computer's plant in Cork, Ireland suffered five days of downtime after the company discovered that 500 of its computers had been infected with the FunLove virus. Staff had to track down the source of the infection and eradicate the virus from all its systems. Paul Taylor (Reuters) wrote, "the attack is regarded as one of the most damaging seen in Europe." In addition to the lost production time, the incident damaged customer relations, with some customers complaining about the delay in delivery of their systems.

Category 14.1 Viruses

2000-01-18 **Microsoft Windows 2000 specific virus**

Telecomworldwire, ComputerWorld
http://www.computerworld.com/home/print.nsf/all/000113DD52

F-Secure announced discovery of the first Windows2000-specific virus. Win2K.Inta or Win2000.Install is a file infector. The company stated that it was not a major threat.

Category 14.1 Viruses

2001-01-05 **php Hypertext Preprocessor scripting language virus malware**

Central Command

From the Central press release:

Central Command, a leading provider of PC anti-virus software and computer security services, and its partners today announced the discovery of PHP.NewWorld, the first virus using the Hypertext Preprocessor (PHP) scripting language to infect computer systems.

PHP (www.php.net) is one of the most popular scripting languages used in the development of e-commerce and heavy content websites. It gained its popularity thanks to its user-friendly programming features, and the incorporation of cross platform compatibility between Windows, Linux, and UNIX environment features included within the language.

"Although PHP.NewWorld is currently not a major threat, it marks a new step toward new virus generation," said Steven Sundermeier, Product Manager at Central Command, Inc.

. . . .PHP.NewWorld is spread to a system when executing an infected script. . . . PHP.NewWorld looks for .php, .hm, .html or .htt files in the C:\Windows directory. All files found with these extensions will become infected. When a user executes a .php file, the virus body will be executed from an external file and will take full control. In the case that the string "NewWorld.PHP" is identified as already existing, the infection routine will not be launched again. Thus, a file will not get infected twice. PHP.NewWorld has no activation date. The virus is not able to spread out from the infected system.

. . . .

Category 14.1 Viruses

2001-04-09 **Logo programming language concept virus**

Central Command

Here is the text of Central Command's announcement about a new concept virus:

Central Command. . . announced the discovery of I-Worm.LogoLogic.A, the world's first virus written using the popular Logo programming language.

"This is a proof of concept virus that utilizes a new development platform to spread, the SuperLogo programming language by Logotron. This language is popular in educational institutions and is a tool used to first expose future programming students to application development," said Steve Sundermeier, Product Manager at Central Command Inc.

Technical details

I-Worm.LogoLogic.A works only with default installations of Microsoft Windows 95 or 98 and mIRC: it assumes that the folders "C:\Windows" and "C:\Program Files" and "C:\MIRC" (default) or "D:\MIRC" or "E:\MIRC" exist. The virus requires the SuperLogo interpreter to be installed.

When executed, the virus overwrites the C:\MIRC\SCRIPT.INI with a small mIRC script that helps the propagation of the virus body (logic.lgp). The script also joins the channel #gigavirii and announces the infection, displaying the following message in the channel (a verse from "Livin' a Lie" a song written by Milk Inc., a Belgian pop band):

"Livin' a lie, tell me why I run and hide. Livin' a lie, you'll never know me deep inside."

After the mIRC infection, the virus drops a file in the Windows startup folder (C:\Windows\Start Menu\Programs\Startup\startup.vbs) that will spread the virus by e-mail. The script sends the virus to the first 80 e-mail addresses in the Microsoft Outlook and Outlook Express address book, with the following content:

Subject: Hey friends! Message: Hello! Look at my new SuperLogo program! Isn't it cool? Attachment: logic.lgp

It also overwrites C:\Windows\WINSTART.BAT and displays the following message: "You think Logo worms don't exist? Think again!"

When the infection routine is finished, the virus displays the message in the SuperLogo window: Logic, the Logo worm (c) Gigabyte

"We have no infection reports of this virus and nor do we consider it to be spreading at this time. This seems to be another demonstration by virus writers on their abilities," said Marius Gheorghescu virus researcher at Central Command's Emergency Virus Response Team.

Category 14.1 Viruses

2001-05-02 **virus prevalence report wild frequency study top ten**

NIPC Daily Report

UK anti-virus vendor Sophos has compiled its monthly listing of the top ten virus reported for April 2001. The April virus chart from the Sophos shows that W32/Magistr-A (Magistr) was first with 27.4% percent, followed by VBS/Kakworm (Kakworm) with 14.0 percent and W32/Hybris-B (Hybris variant) with 12.6 percent, respectively. In fourth was W32/Apology-B (Apology variant) with 9.3 percent , followed by W32/FLCSS (FunLove) with 5.1 percent. The W95/CIH-10xx (CIH or Chernobyl virus was in sixth 2.8 percent, W32/Badtrans-A (Badtrans) was followed by 2.8 percent. The ninth virus was WM97/Marker-C (Marker variant) with 2.3 percent and tenth was W32/Bymer-A (Bymer) with 2.3 percent.(Source: M2 Presswire, 2 May)

Category 14.1 Viruses

2002-01-10 **macro virus .NET proof-of-concept demonstration**

NewsScan

NEW "PROOF-OF-CONCEPT" VIRUS [10 Jan 2002]
A Czech programmer has created a "proof-of-concept" virus called W32/Donut to alert security antivirus vendors and Microsoft managers of software vulnerabilities in executable files created for Microsoft's .NET Web services technology. A spokesman for Symantec, a major vendor of security software, says that the virus "does not have any significant chance to become widespread. However, it shows that virus writers are paying close attention to the new .NET architecture from Microsoft and are attempting to understand the framework that eventually will be available on most systems." (Reuters/USA Today 10 Jan 2002)
http://www.usatoday.com/life/cyber/tech/2002/01/10/microsoft-dot-net-virus.h tm

---

Category 14.1 Viruses

2002-03-27 **worm picture cartoon e-mail social engineering Trojan**

NewsScan

CLINTON CARTOON CARRIES VIRUS
McAfee, the anti-virus software company, says a new virus called MyLife.B., is being circulated as an e-mail attachment featuring a cartoon about former president Bill Clinton. A McAfee executive says, "If this one does reach large proportions, it will be a very costly virus because most consumers don't have good backup methods for their operating system or important files on the C drive." The virus e-mails itself to everyone in a user's Microsoft Outlook address book or MSN Messenger contact list. The virus will cause damage only if you open the attachment - so don't open it! (USA Today 26 Mar 2002)
http://www.usatoday.com/life/cyber/tech/2002/03/26/viruses.htm

---

Category 14.1 Viruses

2002-04-22 **virus proof-of-concept programming language Vx virus exchange**

Security Wire Digest 4 31

*FIRST SAP VIRUS, NO WORRIES
Virus writers targeted another exotic programming language last week, but McAfee.com and Symantec report that the proof-of-concept ABAP.Rivpas.A virus doesn't work. It was written in the Advanced Business Application Programming language used by many large corporations to infect programs and reports used by the SAP R/3 business information system. The "intended virus" was first posted to a virus exchange Web site last year.
http://vil.nai.com/vil/content/v_99453.htm

Category 14.1 Viruses

2002-06-14 **malware virus picture proof-of-concept jpg steganography**

NewsScan

NEW VIRUS CAN INFECT PICTURE FILES
McAfee Security is reporting that a new virus called "Perrun" is the first ever to infect picture files, which, along with other data files, have long been considered safe from such threats. Researchers at McAfee received the virus from its creator and say it's what's called a proof-of-concept virus and does not cause any damage. Up until now, viruses infected and were spread through program files; data files might be deleted or damaged, but Perrun is the first to infect them by inserting portions of the virus code into the picture file. When a .JPG picture is viewed, the virus installs a file on the victim's hard drive that can infect other pictures. Because the original picture looks fine, the victim won't know that anything's amiss. (AP 13 Jun 2002)
http://apnews.excite.com/article/20020613/D7K4F4EG1.html

Category 14.1 Viruses

2002-08-13 **virus malware worm incidence growth**

NewsScan

ALL QUIET ON THE VIRUS FRONT
It's been a slow year for computer virus experts, with the Klez e-mail worm the only notable annoyance now making the rounds. "Klez is the biggest case of the year and that's it," says Mikko Hypponen, manager of antivirus research at Finland's F-Secure. "That's a big surprise to us and to everybody else in the antivirus community." Other monitoring firms report similar findings: Sophos Anti-Virus in the UK says it's detecting 600 to 700 new virus types per month -- about half as many as last year. Theories on why 2002 has seen a significant drop in viruses vary, ranging from the introduction of enhanced antivirus software to stiffer anti-hacker laws to more vigilant computer users. "For the antivirus industry in general, a slow-down would not be very good," says Hypponen. "But I'd love to see it happen. It would free up the resources for us to do something other than fight a problem that shouldn't even be there in the first place." (Reuters 13 Aug 2002)

Category 14.1 *Viruses*

2003-02-19 **spoof e-mail virus Pentagon Defense Technology Information Center DTIC thwarted**

NIPC/DHS

February 18, Federal Computer Week — Pentagon thwarts spoofed e-mail.

The Pentagon said today that an attempt to send a virus through its systems last week was thwarted before damage could be caused. On the morning of February 14, someone "spoofed" the Defense Technology Information Center (DTIC) header, camouflaging the sender's real address to make recipients think the message had come from the Defense Department. The message had a virus attached and was sent through Pentagon computers to two mailing lists. "Our computers caught the virus and stripped it out," said Terry Davis, manager of the Public Web Program in the Office of the Secretary of Defense. "So what went out was the original text message that was sent in the e-mail, but the virus and the attachment were both stripped." Davis said he and a few co-workers then went into the system to put safeguards in place to prevent someone else from spoofing a DTIC header.

Category 14.1 *Viruses*

2003-04-30 **anti virus monthly subscription AOL America Online McAfee**

NewsScan

AOL TO OFFER ANTIVIRUS PROTECTION FOR MONTHLY FEE
AOL has begun offering its subscribers a $2.95-a-month antivirus service that will automatically update a customer's computer as new viruses occur. Jupiter research analyst Michael Gartenberg explains, "It takes antivirus stuff from a more technology-aware audience to a more novice audience." The new AOL service uses McAfee antivirus software and will be seamlessly integrated into the AOL customer experience. (USA Today 30 Apr 2003)

Category 14.1 *Viruses*

2003-05-06 **mobile virus PDA smartphone backdoor Rob Bamforth Bloor Research problems exploit**

NIPC/DHS

May 06, vnunet — The danger of mobile viruses.

PDAs and smartphones create backdoors into corporate infrastructures that can be exploited by viruses and malicious code to spread infections. Rob Bamforth of Bloor Research, a British IT analyst company, said that one of the principal security problems with mobile devices is that they are typically brought into organizations by individuals who have purchased them independently, rather than being issued as part of a co-ordinated IT department rollout. This makes them very difficult to control and manage when they are connected to corporate networks. Bamforth added that, while viruses currently present little danger to the actual mobile handsets themselves, the greatest problem comes from the devices being used as a transmission medium through which viruses could infect company infrastructures.

Category 14.1 *Viruses*

2003-08-02 **DHS W32*Mimail virus attachment message.zip malicious code mass mailer MS03-014 microsoft outlook express**

NIPC/DHS

August 02, U.S. Department of Homeland Security — Department of Homeland Security Advisory "W32/Mimail Virus".

First reported on on Friday, August 1, the W32/Mimail virus is a malicious file attachment containing a specially crafted HTML file named 'message.html'. This file is delivered inside of a .ZIP archive file named 'message.zip'. Viewing the 'message.html' file on a vulnerable system will cause the malicious code, which is a mass-mailer, to be installed and executed. The vulnerability, which was identified in April 2003 and described in Microsoft Security Bulletin MS03-014, makes it possible for W32/Mimail to execute automatically once the .ZIP archive is opened. DHS/IAIP encourages sites to review Microsoft Security Bulletin MS03-014 and apply the Cumulative Patch for Outlook Express available on the Microsoft Website: http://www.microsoft.com/technet/treeview/default.asp?url=/t echnet/security/bulletin/MS03-014.asp.

Category 14.1 *Viruses*

2003-08-12 **Virus Maryland Motor Vehicle Administration MVA Cheron Wicker**

NIPC/DHS

August 12, — Virus forces Maryland Motor Vehicles Administration to close.

A computer virus forced the Maryland Motor Vehicle Administration to shut all of its offices at noon Tuesday, August 12. The department expected to reopen its offices Wednesday, officials said. "We have closed all of our offices and facilities statewide. So there's no telephone service right now. There's no online service right now. There's no kiosk or express office service," MVA spokeswoman Cheron Wicker said. Drivers who had business with Tuesday deadlines at the MVA were told not to worry. People who needed to renew registrations were told to wait for Wednesday. Wicker said it was too early to tell what damage may have been done.

Category 14.1 *Viruses*

2003-08-19 **Navy Marine Corps Intranet down virus NMCI e-mail secure network**

NIPC/DHS

August 19, Federal Computer Week — Navy Marine Corps Intranet goes down.

A virus took the Navy Marine Corps Intranet (NMCI) off-line Tuesday, August 19. A phone recording on the NMCI Strike Force hotline stated: "We are currently experiencing connectivity issues enterprise wide to include e-mail, Web and shared drive access due to a virus." NMCI is an enterprisewide network designed to connect everyone in the Navy and Marine Corps on a single, secure network. Since users started being moved to the system in 2001, almost 97,000 seats have been shifted from legacy systems.

Category 14.1 *Viruses*

2003-08-20 **Sobig virus e-mail systems MessageLabs Inc. hacker bacdoor trojan horse**

NIPC/DHS

August 20, Dow Jones Newswire — Sobig virus spread is fastest ever.

The "Sobig.F" computer virus that began attacking e-mail systems globally Tuesday, August 19, has been declared the fastest-spreading e-mail virus of all time. E-mail filtering company MessageLabs Inc. said it intercepted more than one million copies of Sobig.F Tuesday, the most ever in a single day. The interception rate was one in every 17 e-mail messages the firm scanned. Sobig.F continued to spread aggressively Wednesday. Sobig.F, which is the sixth and latest strain of a virus that first emerged in January, spreads through Windows personal computers via e-mail and network file-share systems. Besides clogging e-mail systems full of messages with subjects like "Re: Details" and "Re: Wicked screensaver," the virus also deposits a Trojan horse, or hacker back door, that can be used to turn victims' PCs into spam machines. The worm is programmed to stop spreading on September 10.

Category 14.1 *Viruses*

2003-09-17 **windows flaw Blaster exploit Ken Dunham Trojan horses MSBlast worm unpatched computers root access underground source code**

NIPC/DHS

September 17, CNET News.com — Flaws set to spawn another Blaster.

Tools exploiting a new Windows flaw have started to appear, prompting warnings of imminent virus attacks. Ken Dunham, an analyst at a private security firm, said on Tuesday, September 16, that it is "highly likely" that new worms or Trojan horses will emerge in the next few days. These bugs are expected to prey on computers that have not been updated with the latest security patch for Microsoft's operating system. "A new Blaster-like worm family could be created in a matter of hours or days, now that exploit source code has been posted in the underground," Dunham wrote in an email. "The new attack tool makes it trivial for any malicious actor to gain unauthorized root access to an unpatched computer." Experts advised people last week that a new virus was reasonably likely, given the fact that the recently discovered Windows vulnerabilities are similar to those that paved the way for the MSBlast worm.

Category 14.1 Viruses

2004-01-07 **malware malicious code bogus FBI warning social engineering**

The Register
http://www.theregister.co.uk/2004/01/07/bogus_fbi_warning_file_contains/

BOGUS FBI WARNING FILE CONTAINS MALWARE.

John Leyden of The Register wrote, "Virus writers are attempting to trick music fans into opening malicious code with a message purporting to arise from an FBI investigation into illegal file trading. Recipients of the bogus warning are told they are under investigation. Infectious emails contain an attachment allegedly containing evidence against the 'accused' which actually contains Windows malware, the Melbourne Age reports. The message appears authentic but closer inspection reveals factual errors and spelling mistakes that give the game away. This is the sneakiest piece of social engineering by a virus writer that we can recall."

Link to original article by Sam Varghese in _The Age_ of Melbourne:
http://www.theage.com.au/articles/2004/01/06/1073268005348.html?oneclick=true

---

Category 14.1 Viruses

2004-01-14 **Network Associates Anti-Virus Handhelds ePO Microsoft Pocket PC**

NewsBits;
http://www.internetweek.com/breakingNews/showArticle.jhtml%3Bjsessionid=YKFLTHGCLCUBWQSNDBGCKHY?articleID=17300738

Network Associates Adds Anti-Virus Protection For Handhelds

Network Associates on Tuesday added a new anti-virus defense product to its security portfolio, one that targets enterprises with employees carrying Microsoft Pocket PC and Windows Mobile devices. Dubbed McAfee VirusScan PDA Enterprise, the new software installs a small anti-virus client on the mobile gear, but can be managed by the IT staff using Network Associates' McAfee ePolicy Orchestrator (ePO), an verseer's tool that sets and enforces security policies.

Category 14.1 Viruses

2004-02-03 **virus attack Microsoft escape bounty offer MyDoom worm SCO**

NewsScan

MICROSOFT DUCKS, EVADES ASSAULT BY VANDALS

Microsoft has rebuffed an attempted software virus attack aimed at shutting down some of the company's Web sites yesterday — two days after a different version of the same "Mydoom" virus shut down the Web site of The SCO Group in Utah. Microsoft says it will pay $250,000 to anyone who helps authorities find and prosecute the author of the virus. A similar offer has also been made by The SCO Group. (AP/Washington Post 3 Feb 2004)

Category 14.1 Viruses

2004-03-03 **virus worm network attack epidemic Netsky**

DHS IAIP Daily; http://www.esecurityplanet.com/trends/article.php/3320501

March 02, eSecurity Planet — Virus attacks reach 'epidemic' proportions.

ust as the industry was reeling Monday, March 1, from the weekend release of a new Netsky variant and five new Bagle variants, another two Bagle variants and one more Netsky variant have hit the Internet. Netsky-D, alone, has caused $58.5 million in damages worldwide, according to mi2g, a London-based security assessment company. And as that variant continues to wreak havoc across the Internet, Netsky-E has been discovered. The latest variant spreads via email and network shares, but so far is not causing as much trouble as its predecessors. "Whoever is behind the Netsky worms is hell bent on causing as much chaos as possible," says Graham Cluley, of Sophos, Inc., an anti-virus and anti-spam company. "They have deliberately released new versions of their virus, tweaked to try and avoid detection by anti-virus software." The Bagle family ushered in Bagle-H and Bagle-I Monday. Bagle-H is an e-mail worm which contains a password-protected Zip file which avoids anti-virus detection. When the attachment is opened, the worm opens up a backdoor on Port 2745 and waits for commands from the virus author. Bagle-I follows the same pattern but has been tweaked to avoid detection by anti-virus software programmed to stop Bagle-H.

Category 14.1 Viruses

2004-03-25 **virus worm writer trial Romania Blaster variant international cybercrime free speech**

DHS IAIP Daily;

March 23, Reuters — Accused virus writer faces trial in Romania.

A decisive test for what is called the "toughest cybercrime law in the world" began Tuesday, March 23, with the opening of a case against a Romanian man charged with spreading a computer virus that affected approximately 1,000 computers. Dan Dumitru Ciobanu is accused of making "Blaster.F," a mild copy of one of last summer's harshest Internet worms. If convicted, the 24-year-old faces between three and 15 years in prison. Romania has enacted tough laws to protect its emerging reputation as a hub of skilled programmers for Western companies and erase any connection with cybercrime syndicates that law enforcement officials say are being run out of Eastern Europe. The Ciobanu case has reignited an international debate on appropriate justice for cybercrimes. With public thirst for cybercrime justice growing, experts wonder what impact a potential stiff sentence on Ciobanu will have on deterring a growing underground of virus writers.

Category 14.1 Viruses

2004-07-03 **Internet Explorer flaw vulnerability hole weakness virus transmission Websites Secunia**

NewsScan

WHEN A FEATURE BECOMES A BUG

A report by Secunia, a computer security company, says that an Internet Explorer feature is being used by network vandals to convert Web sites into virus transmitters. (It's not a bug but a feature intended to make browsing more convenient.) Two other flaws in Microsoft products allowed hackers to direct Internet Explorer browsers to automatically run the virus when visiting an infected site. Microsoft says that updated code will be automatically installed on computers set to receive it. The update is also available at http://windowsupdate.microsoft.com. (AP/USA Today 3 Jul 2004)

Category 14.1 Viruses

2004-08-05 **portable digital assistant PDA malicious code virus PocketPC Kaspersky**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/26848−1.html

August 05, Government Computer News — Malicious code targeting PDAs identified.

The first backdoor code for personal digital assistants has emerged, raising concerns that handheld devices soon could be targeted by hackers. The code, called Backdoor.WinCE.Brador.a, was identified by Kaspersky Labs. It is 5,632 bytes and targets PDAs running PocketPC. The Moscow-based antivirus company called Brador a classic Trojan backdoor program, which could expose handheld devices to remote exploitation. Security experts said the threat from Brador is not imminent, but probably is inevitable. The sample seen by Kaspersky was attached to an e-mail from a Russian sender and with Russian text. It creates an executable file in the PDA's autorun folder so that it takes over whenever the device is turned on. It identifies the IP address, contacts the author and opens port 44299 for further commands. The author was offering to sell the client code. PDA users should protect their devices with anti-virus software.

Category 14.1 Viruses

2004-08-17 **e-mail viruses worms smarter MessageLabs writers spammers collaborations**

DHS IAIP Daily;
http://www.reuters.com/newsArticle.jhtml?type=topNews&storyI D=6001506

August 17, Reuters — E-mail viruses getting smarter, report says.

Computer security group MessageLabs, which scans client e-mails for viruses to block, said it picked apart some 5.6 billion e-mails from January to June this year and found 1-in-12 contained some sort of virus that penetrated firewalls meant to block them. MessageLabs said it believes the biggest e-mail security threat during the first half of 2004 was closer cooperation between virus writers and spammers, writers of unsolicited messages that often advertise products or get people to spend money. The reason the two groups are getting together is profit, MessageLabs has learned through monitoring chat rooms. With the recent proliferation of software blocking spam, the spammers are paying virus writers to create viruses that attach to their e-mails and circumvent the spam blockers.

Category 14.1 Viruses

2004-08-24 **Windows 64-bit processor proof-of-concept virus Symantec advisory**

DHS IAIP Daily; http://www.cbronline.com/article_news.asp?guid=3AF80B03−DE93
−4EBD−B37F−41BC1B124C4B

August 24, Computer Business Review Online — First 64-bit Windows virus intercepted.

Anti-virus experts have intercepted the first computer virus targeting 64-bit Windows workstations. According to an advisory issued by Symantec, W64.Shruggle.1318 is a fairly simple "proof-of-concept" virus programmed to attack 64-bit Windows executables on AMD64 systems. Alfred Huger, senior engineer at Symantec Security Response, said it looks like Shruggle has no malicious intent. The virus is not circulating in the wild; Symantec found it on a sample-sharing network used by antivirus firms. "This shows that viruses are being developed for 64-bit processors," Huger said. The worldwide move to 64-bit will not preclude the need for virus detection, he indicated. The virus does not infect 32-bit Portable Executable files and won't run natively on 32-bit Windows platforms. However, it can be run on a 32-bit computer that is using 64-bit simulation software. Original Advisory: http://securityresponse.symantec.com/avcenter/venc/data/w64. shruggle.1318.html

---

Category 14.1 Viruses

2004-08-26 **exam theft virus China black market question papers Microsoft Word Excel**

NewsScan

'EXAM THEFT' VIRUS HITS CHINA

A Beijing technology firm, Jiangmin Science Technology, is reporting the discovery of a computer virus specifically designed to steal files labeled "exam" or "test questions." The "exam theft" virus targets Microsoft Word and Excel files, and some observers speculate the virus creators may have been motivated by the thriving trade in black-market exam papers in that region. (The Register 26 Aug 2004)

Category 14.1 Viruses

2004-08-30 **cybercrime organized virus worm writing spam bot net sales**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/story/0,10801,95501,00.html?SKC=security−95501

August 30, Computerworld — Organized crime invades cyberspace.

Antivirus researchers have uncovered a startling increase in organized virus- and worm-writing activity that they say is powering an underground economy specializing in identity theft and spam. "The July 2004 outbreak of MyDoom.O was yet another reminder that spammers are now using sophisticated, blended threats that mix spam, viruses and denial-of-service attacks," according to Andrew Lochart, director of product marketing at Postini Inc. According to Mikko Hypponen, antivirus research director at F-Secure Corp., MyDoom.O was the beginning of a concerted, unabashed effort to turn virus and worm infections into cash. Underground bartering and selling is conducted on Websites such as a Russian site that, among other things, sells subscription services to compromised computers. Viruses and worms carrying Trojan horse code are also powering massive identity theft rings. "Whether or not this is traditional organized crime doesn't matter -- because they are organized, and what they are doing is criminal," says Hypponen.

Category 14.1 Viruses

2004-08-31 **Department of Defense DoD viral computer infection Army Space and Missile Defense Command SIPRNET**

DHS IAIP Daily; http://www.fcw.com/fcw/articles/2004/0830/web−siprnet−08−31− 04.asp

August 31, Federal Computer Week — DoD reveals viral infection.

Two computers in the Army Space and Missile Defense command connected to the Defense Department's classified Secret Internet Protocol Router Network (SIPRNET) were infected because they did not have any virus protection. William Congo, a spokesperson for the Huntsville, AL-based Space and Missile Defense Command said the two computers were located at a facility in Colorado Springs, CO. The viruses were detected quickly and the two computers were then isolated from the SIPRNET, Congo added. The incident occurred "within the past month" and officials are still investigating the matter to determine how the infection occurred and prevent future occurrences, he said.

Category 14.1 Viruses

2004-09-20 **virus growth volume attacks less successful Symantec Antivirus report zombies infected computers**

DHS IAIP Daily; http://news.com.com/Viruses+keep+on+growing/2100−7349_3 −5374 399.html?tag=nefd.top

September 20, CNET News.com — Viruses keep on growing.

The volume of worms and viruses is increasing, but the rate of successful attacks has dropped, according to a new report from Symantec. The antivirus company's biannual Internet Security Threat Report found that 4,496 new Windows viruses and worms were released between January and June, up more than 4.5 times from same period last year. But overall, Symantec, the daily volume of actual attacks decreased in the first six months of 2004. Alfred Huger, a senior director at Symantec's Security Response team said malicious code writers were increasingly going to spammers to sell them access to the computers that they hack, or break into. Spammers, after paying the hackers, then flood those hacked computers with unsolicited messages, or spam. Symantec also said it expects more viruses and worms in the future to be written to attack systems that run on the Linux operating system and hand-held devices as they become more widely used. The report also noted that the rate at which personal computers are being hijacked by hackers rocketed in the first half of 2004. An average of 30,000 computers per day were turned into enslaved "zombies," compared with just 2000 per day in 2003. Report: http://enterprisesecurity.symantec.com/content.cfm?articleid =1539

Category 14.1 Viruses

2004-11-05 **computer virus attack New Jersey Motor Vehicle Commission MVC**

DHS IAIP Daily; http://www.app.com/app/story/0,21625,1102760,00.html

November 05, Asbury Park Press (NJ) — Computer virus hits state offices.

Drivers and applicants endured sometimes long waits at the newly overhauled New Jersey Motor Vehicle Commission's (MVC) offices on three days last week after a hard-charging computer virus struck its statewide system. Agency spokesperson Gordon Deal said the computer bug zapped, to far lesser degrees, systems in the departments of Treasury, Transportation, and Law & Public Safety. Deal said systems experts do not know where the virus originated or if it had been targeting state computers.

Category 14.1 Viruses

2004-11-22 **virus trojan SANS MyDoom Trojan.Agent.EC Bofra Virtumonde adware**

NewsScan; http://www.internetnews.com/security/article.php/3439011

WHAT EVIL LURKS IN BANNER ADS?

Versions of the MyDoom virus are showing up on banner ads, spreading their misery via compromised ad servers. The SANS Institute Internet Storm Center reports that a "high profile UK Web site" was among those affected and on Sunday, and The Register confirmed that "early on Saturday morning some banner advertising served for The Register by third-party ad serving company Falk AG became infected with the Bofra/IFrame exploit." Falk AG serves ads to many popular sites, including NBC Universal, ATOM Shockwave, The Golf Channel and A&E Networks. In addition to Bofra/MyDoom, two additional viruses are working their way through compromised networks: the first, called Virtumonde Adware, hijacks a server and directs users to different pages and searches than those they had intended. The other, dubbed Trojan. Agent.EC, can take control of a PC through the back door and direct it to upload and execute whatever code the attacker wishes. (Internet News 22 Nov 2004)

Category 14.1 *Viruses*

2004-12-07 **computer virus infection Jefferson County public schools Kentucky precautions anti-virus software**

DHS IAIP Daily; http://www.courier−journal.com/localnews/2004/12/07ky/A1−vir us1207−5418.html

December 07, The Courier-Journal (KY) — Computer virus infects Jefferson County schools.

Jefferson County public schools in Kentucky are battling a virus that has infected at least 1,000 computers and wreaked havoc on everything from attendance reports to students' ability to finish term papers. Officials blame the same "w32gaobot" virus that hit tens of thousands of school computers statewide late last month, freezing school Websites and barring student access to the Internet. After getting into the state's education computer network, that virus bogged down computers partly by generating overloading traffic on the Internet — and in some cases reading computer passwords and dispersing them and other technical information onto the Internet. Potentially debilitating viruses "show up on a regular basis now," said Cary Petersen, director of technology in Jefferson County Public Schools. One problem controlling viruses in a school system like Jefferson County's, which has about 28,000 computers, is that there are many possible entry points, including spam e-mail attachments, Internet ads or infected floppy disks. Precautions, including anti-viral software and educating workers not to open an e-mail without certain knowledge of its origins, have helped limit the spread, Petersen said.

Category 14.1 *Viruses*

2005-01-06 **Microsoft enter antivirus market anti-spyware technology release Windows XP Update Automatic**

DHS IAIP Daily; http://www.pcworld.com/news/article/0,aid,119197,00.asp

MICROSOFT TO ENTER THE ANTIVIRUS MARKET

Microsoft announced Thursday, January 6, the release of anti-spyware technology and said it would begin giving away an improved tool to remove worms and viruses from its customers' computers. While the free antivirus and virus removal tools are not an immediate threat to the products from competing companies, the releases could signal tougher times ahead for desktop security vendors, as Microsoft uses its size and influence to expand into markets now dominated by those companies, industry experts say. A spokesperson for Microsoft's Security Business & Technology Unit, says that spyware is a major concern for Microsoft customers, who are looking to the company for help. Spyware accounts for more than one-third of software program crashes on Windows XP that are reported to the company. Microsoft also says that it is releasing a free malicious-software removal tool that consolidates earlier software tools for eradicating the Blaster, MyDoom, and Sasser worms, and that will be updated each month to detect and remove other threats as they appear. Windows customers will be able to receive the malicious-code removal tool through Windows Update and the Windows Automatic Update features.

Category 14.1 *Viruses*

2005-01-31 **new virus anti-virus antivirus attack technique bypass filter ZIP RAR .zip .rar file compression algorithm**

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1756636,00.asp

NEW VIRUS ATTACK TECHNIQUE BYPASSES FILTERS

Administrators and service providers have begun seeing virus-infected messages with a new type of attachment hitting their mail servers: an .rar archive. .Rar files are similar to .zip files in that they are containers used to hold one or more compressed files. The .rar format is not as widely known as .zip, but it is used for a number of tasks, including compressing very large files, such as music and video. Many of the messages in .rar virus e-mail are invitations to view pornographic content, which is part of the reason for the viruses' success, experts say. .Rar's compression algorithm is 30 percent more efficient than .zip technology. One recent .rar virus that appeared at the end of last week is disguised as a patch from Microsoft. Anti-virus vendors have acknowledged the presence of viruses delivered as .rar files and are working to develop tools to identify and eradicate the malware.

Category 14.1 Viruses

2005-02-22 **Federal Bureau Investigation FBI warning computer virus fbi.gov address Internet Fraud Complaint Center**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/articles/A45131−2005Feb 22.html

FBI OFFICIALS WARN ABOUT COMPUTER VIRUS

The FBI warned Tuesday, February 22, that a computer virus is being spread through unsolicited e-mails that purport to come from the FBI. The e-mails appear to come from an fbi.gov address. They tell recipients that they have accessed illegal Websites and that their Internet use has been monitored by the FBI's "Internet Fraud Complaint Center," the FBI said.

Category 14.1 Viruses

2005-02-24 **malware virus alert Web site government notification notice news users vulnerability social engineering exploit**

RISKS; http://news.bbc.co.uk/1/hi/technology/4291005.stm 23 75

UK GETS OFFICIAL VIRUS ALERT SITE

Chris Leeson relayed information from a BBC News report that "The UK government is setting up a Virus Alert site to warn users of viruses, vulnerabilities and so on. It is aimed at home and small business users. . . It is expected to issue between six and ten alerts a year, concentrating on the most major problems. It will not provide patches, but will point the user to where the patches can be downloaded. It is also made clear that the site is not a panacea or a substitute for proper AV and Firewall provision."

However, Leeson warned,

>Alas, there remains a number [of] problems:

1. This would be a great site for the Malware Brigade to spoof. I hope that it is more secure than most Web Sites.

2. They are concentrating on the most serious threats. Understandable, but even the "less serious" threats can be trouble.

3. Most PC users are simply not interested in PC Security and won't be convinced that they have to be. The new users may well not realise that they are exposed at all. (I am a little sore about this having just spent three days trying to salvage someone's XP system after the PC had spent two weeks on Broadband without Firewall or AV…)<

Category 14.1 Viruses

2005-05-18 **computer virus German election influence ring wing hacktivism Trojan Horse**

DHS IAIP Daily; http://www.iht.com/articles/2005/05/17/business/virus.php

COMPUTER VIRUS MAY BE AIMED AT GERMAN ELECTION

The creator of a computer Trojan horse that unleashed a torrent of far-right spam e-mail messages in Germany on Tuesday, May 17, may be trying to influence the outcome of the election Sunday, May 22, in North Rhine-Westphalia, a German software expert said. Computers infected with the so-called Sober.q Trojan horse unwittingly sent thousands of spam e-mails bearing links to the Website of the National Democratic Party (NPD), a party that espouses "Germany for Germans," the death penalty for some drug dealers and an end to asylum-seeker rights. "This is most likely connected to the election coming up on Sunday," said Christoph Hardy, a spokesperson for the German unit of Sophos, a British anti-virus software company. "It was probably generated by someone who is sympathetic to the far-right, trying to create anger and a protest vote in Sunday's election." Sober.q was reported to have spread widely around Europe and also to have infected computers in the United States and Asia. The originator of the Trojan horse was most likely German because the programming language used to create the Trojan horse was German, as was the language in the e-mail.

Category 14.1 Viruses

2005-06-03 **virus Osama bin Laden e-mail junk attachment Microsoft Windows solution upgrade Windows**

DHS IAIP Daily; http://news.bbc.co.uk/1/hi/technology/4607203.stm

FAKE OSAMA BIN LADEN E-MAILHIDES VIRUS

Users are being warned not to open junk e-mailmessages claiming Osama bin Laden has been captured. The messages claim to contain pictures of the al Qaeda leader's arrest but anyone opening the attachment will fall victim to a Microsoft Windows virus. Since June 1, anti-virus companies have been catching the junk mail messages in large numbers. Anyone opening the attachments or visiting the Website will get a version of the Psyme trojan installed on their PC. The vulnerability exploited by Psyme is found in Windows 2000, 95, 98, ME, NT, XP and Windows Server 2003. Users are urged to update their version of Windows to close the loophole.

Category 14.1 Viruses

2005-06-09 **new virus vulnerability scanner hacker methods botnets**

DHS IAIP Daily; http://www.newscientist.com/article.ns?id=dn7500

NEW TYPE OF VIRUS SCANS NETWORKS FOR VULNERABILITIES

An emerging breed of computer virus that keeps hackers informed about the latest weaknesses in computer networks has been discovered by security experts. The viruses infect a computer network, scan for security vulnerabilities and then report back to hackers through an Internet chatroom. Armies of computers infected with "bot" viruses are routinely controlled via a chatroom connection and are used to knock for denial of service attacks or as a conduit for sending out spam e-mail. However, the ability of some bots to scan their hosts for unpatched security holes and report their findings back to hackers has gone largely unnoticed until now. The emerging class of malware or malicious software - known as vulnerability assessment worms - "phone home" to allow hackers to fine-tune further attacks or perhaps even target an individual PC within a network. This pernicious form of program is just one of a growing number of new viruses identified each month, says computer security expert Bruce Schneier. "The virus trend doesn't look good," Schneier writes in the June 2005 edition of the Association for Computing Machinery journal, Queue. "More than a thousand new worms and viruses were discovered in the last six months alone."

Category 14.1 Viruses

2005-07-29 **virus writer targets anti-virus companies Sophos Symantec McAfee**

DHS IAIP Daily;
http://www.techweb.com/showArticle.jhtml?articleID=166403862

VIRUS WRITER TARGETS ANTI-VIRUS VENDORS

A virus writer apparently seeking notoriety instead of financial gain has released malicious code that ridicules anti-virus vendors and Sasser worm author Sven Jaschan, a security firm said Friday, July 29. The Lebreat-D virus, which is rated a low threat, creates in infected computers a JPEG image file of Jaschan, a German teenager recently convicted of authoring the widespread Sasser and Netsky worms, Sophos Plc said. The Lebreat worm, which is spread through email attachments and exploits a Microsoft security vulnerability, opens a backdoor to an infected Windows computer, enabling a hacker to gain control. The virus indicates that a denial of service attack could be planned against security vendors Symantec Corp. and McAfee Inc., but doesn't say when, Sophos said.

Category 14.1 Viruses

2005-09-22 **PC phone crossover virus Trojan Symbian 6o operating system OS Bluetooth propagation**

DHS IAIP Daily; http://www.vnunet.com/vnunet/news/2142665/first−pc−phone
−cro ssover−virus

FIRST PC/PHONE CROSSOVER VIRUS FOUND

The first mobile phone virus capable of infecting a computer has been found. Experts at have detected the Cardtrp worm that affects handsets running the Symbian 60 operating system. This work spreads via Bluetooh and MMS but could also spread through memory cards. Mikko Hyppönen, chief research officer at F-Secure, said: "The goal of this backdoor Trojan is most likely to cause the user to infect his PC when he is trying to disinfect his phone.

Category 14.1 Viruses

2005-10-04 **BBC News criminals victims spyware data viruses information MessageLabs**

DHS IAIP Daily; http://news.bbc.co.uk/2/hi/technology/4306048.stm

WEB HELPS CRIMINALS TRAP VICTIMS

Statistics have shows that criminals are using spyware to get hold of personal data they can sell or use themselves. This is a shift from e-mailed viruses that were sent to steal this valuable information. According to Mark Sunner, chief technology officer at MessageLabs, "More and more malicious code is appearing in web traffic as opposed to e-mail."

Category 14.1 Viruses

2005-11-01 **hacker virus e-mail computer hijacking botnets avian flu information social engineering**

DHS IAIP Daily;
http://news.yahoo.com/s/nm/20051101/od_uk_nm/oukoe_uk_crime_
birdflu_hackers;_ylt=AiSkjGPhKv3hc6uuQZYRAPes0NUE;_ylu=X3oDM
TA3NW1oMDRpBHNlYwM3NTc−

HACKERS USE BIRD FLU E-MAILS TO HIJACK COMPUTERS

Computer hackers are exploiting fears about avian flu by releasing a computer virus attached to an e-mail that appears to contain avian flu information. According to Panda Software, the virus Naiva.A masquerades as a word document with e-mail subject lines such as "Outbreak in North America" and "What is avian influenza (bird flu)?" When the file is opened, the virus modifies, creates, and delete files. The virus also installs a program that allows hackers to gain remote control of infected computers. The virus spreads through e-mails, Internet downloads, and file transfers.

Category 14.1 Viruses

2005-12-01 **biggest virus attack outbreak November 2005 Sober FBI CIA messages social engineering**

DHS IAIP Daily;
http://www.techweb.com/wire/security/174403317;jsessionid=0E
Z1TE0ZK20WWQSNDBGCKHSCJUMEKJVN

SOBER ATTACK BIGGEST VIRUS OUTBREAK EVER

Apparently, messages from the Federal Bureau of Investigation and Central Intelligence Agency are the way to spread worms, a security firm said Thursday, December 1, as it tallied up Sober's wildfire spread during November and concluded that the outbreak was the biggest ever. E-mail security provider Postini said that it had quarantined more than 218 million Sober-infected messages last week, more than four times the 50 million-message average that it blocks in a run-of-the-mill month. "This Sober generated close to a 1,500 percent increase in virus infected e-mail traffic in the past week," said Scott Petry, vice president of products and engineering at Postini, in a statement. Petry also said that Sober's attack was twice as large as the largest previous on Postini's records. Other security vendors took note of the recent Sober -- the variant is dubbed Sober.x, Sober.y, or Sober.z by most anti-virus firms -- and its impact during November. Both Sophos and Fortinet, for instance, had the new Sober at the top of their November charts as well.

Category 14.1 Viruses

2006-02-06 **Sophos report PC virus work month ever January malware release**

DHS IAIP Daily; http://www.scmagazine.com/uk/news/article/539732/sober− 23
domin ates−virusfilled−january/

SOPHOS: JANUARY 2006 IS THE WORST MONTH ON RECORD FOR PC VIRUSES

Sophos said that 2,312 new articles of malware appeared last month, an increase of more than one-third since December. The Sober worm, called W32/Sober-Z by Sophos, accounted for nearly 45 percent of all malware. However, its recent dominance as the most frequently seen type of malware is set to end, the firm warned, because it stopped spreading on January 6. Following Sober, the top five was rounded out by Netsky-P, Zafi-B, Nyxem and Mytob-BE in that order. Mytob-FO, Netsky-D, Mytob-EX, Mytob-C and Mytob-AS rounded out the top ten January viruses, according to Sophos.

Category 14.1 Viruses

2006-02-16 **virus writers Apple Mac OS X release iChat vector low threat McAfee rating**

EDUPAGE; http://news.zdnet.com/2100-1009_22-6040681.html 23

VIRUS WRITERS TURN TO APPLE

A new computer virus that targets the Apple OS X operating system has been identified. Although the malicious code is not sophisticated--it requires users to "download the application and execute the resulting file," according to Apple--and has been labeled a low-level threat by McAfee and Symantec, it may represent the first virus in circulation that attacks users of Apple's operating system. Ray Wagner of Gartner said that the virus is "not really news" except that it is "the first OS X malicious content in the wild that's been noted at this point." The bug spreads primarily by sending itself through Apple's iChat instant messaging program to those on an infected computer's buddy list. Several security firms have updated their threat profiles to include the new virus.

Category 14.1 Viruses

2006-02-27 **cross-infecting virus discovery PC Windows wireless pocket device proof-of-concept Trojan**

DHS IAIP Daily; http://www.scmagazine.com/uk/news/article/543503/crossinfect ing−virus−discovered/ 23

CROSS-INFECTING VIRUS DISCOVERED.

The first malware to cross-infect a PC and a Windows wireless pocket device has been discovered, the Mobile Antivirus Researchers Association (MARA) said. The proof-of-concept, file-destroying Trojan automatically spreads from a Win32 desktop to a Windows Mobile Pocket PC. "With the growing use of hand-held devices, this type of virus may become very prevalent in the future. This virus closes the gap between handhelds and desktops," the association said. Jonathan Read of MARA said that previous "crossover" viruses -- "required either Bluetooth on the device and the PC, or the user had to physically transfer the virus on a memory card." But this trojan is the first to use ActiveSync -- a program that synchronizes files and other data between a Windows PC and a Windows Mobile device -- to cross-infect a desktop and hand-held PC. It also is the first crossover malware to infect the PC before attacking the mobile device. Dave Cole, director of Symantec Security Response, said today that he expects hackers to continue to experiment with new platforms, such as mobile devices. He predicts such attacks gradually will become more financially motivated as users increase their reliance on hand-held computers in their daily lives.

Category 14.1 Viruses

2006-03-15 **RFID threat viruses security vulnerability proof-of-concept**

EDUPAGE; http://www.nytimes.com/2006/03/15/technology/15tag.html 23

RFID SUSCEPTIBLE TO VIRUSES

A group of researchers affiliated with Vrije Universiteit in Amsterdam has discovered a way to spread a computer virus through RFID tags, a scenario most security experts had previously dismissed. The researchers demonstrated that a virus can spread from an infected tag to the scanners and systems that register the tags and to other tags. In an airport, for example, an infected luggage RFID tag can infect airline systems, possibly allowing some luggage to avoid being screened, and can spread to other luggage and other airports. The group called RFID malware "a Pandora's box" of potential problems. Aware of the risks of disclosing a vulnerability, the researchers also offered advice to RFID developers about how to protect their systems. Peter Neumann, computer scientist at research firm SRI International, echoed the researchers' warnings about RFID technology. "It shouldn't surprise you that a system that is designed to be manufactured as cheaply as possible," he said, "is designed with no security constraints whatsoever." Daniel Mullen, president of the Association for Automatic Identification and Mobility, which represents the industry, said companies developing the technology are engaged in an "ongoing dialogue about protecting information on the tag and in the database."

Category 14.1 Viruses

2006-04-07 **cross-platform proof-of-concept Windows Linux virus warning Kaspersky Labs**

DHS IAIP Daily; http://www.computerworld.com/printthis/2006/0,4814,110330,00 .html 23

KASPERSKY WARNS OF CROSS-PLATFORM VIRUS PROOF-OF-CONCEPT.

Kaspersky Labs is reporting a new proof-of-concept virus capable of infecting both Windows and Linux systems. The cross-platform virus is relatively simple and appears to have a low impact, according to Kaspersky. Even so, it could be a sign that virus writers are beginning to research ways of writing new code capable of infecting multiple platforms, said Shane Coursen, senior technical consultant at Kaspersky. The new virus, which Kaspersky calls Virus.Linux.Bi.a/Virus.Win32.Bi.a, is written in assembler and infects only those files in the current directory. "However, it is interesting in that it is capable of infecting the different file formats used by Linux and Windows," Kaspersky said.

Category 14.1 Viruses

2006-05-02 **WOW virus online gamers targeted World of Warcraft Trojan Horse attack fraud theft**

DHS IAIP Daily; http://www.it− observer.com/news/6217/wow_virus_targets_onlin e_gamers/ 23

WOW VIRUS TARGETS ONLINE GAMERS.

Security analysts at MicroWorld Technologies report that a new variant of the password stealing Trojan, named "Trojan-PSW.Win32.WOW.x," is spreading fast, attacking account holders of the online game "World of Warcraft." World of Warcraft is a multi-million dollar entity in the world of cyber games where huge sums change hands every second. Once the hacker gets hold of a gamer's password, he can transfer victim's goods to his personal account, which is easily converted to liquid currency through Gaming Currency Exchange Websites. MicroWorld experts have found that this Trojan slips into user computers via pop-up ads being displayed on many dubious gaming Websites, through a vulnerability in Internet Explorer.

Category 14.1 Viruses

2006-05-08 **World Cup 2006 virus season start FIFA social engineering**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1959084,00.asp 23

WORLD CUP VIRUS SEASON KICKS OFF.

The FIFA World Cup 2006 tournament won't get underway in Germany until early June, but computer virus writers are already attempting to cash in on the planet's most popular sporting event with viruses aimed at deceiving eager soccer fans. Researchers at UK-based Sophos released notification of a new attack that infects Microsoft Excel files and has been disguised as a spreadsheet charting the national teams participating in the World Cup. Identified by the security company as XF97/Yagnuul-A, the virus lives in an Excel file that offers to help people set up fantasy sports competitions related to the international soccer championship, and also attempts to market itself specifically to fans of the English Premiership, one of the world's top professional leagues. Once the World Cup virus has infected a PC, it begins forwarding itself to other people using the corrupted machine and may also send itself to people listed in any e-mail client software on the device, Sophos said. The Excel virus marks the second World Cup-oriented attack identified by the company in the last week.

14.2 Worms

Category 14.2 *Worms*

1999-11-10 **virus worm e-mail attachment highlight automatic MS-Outlook prototype proof-of-concept**

AP, Dow Jones

In early November, a worrisome new worm appeared on the scene. The BubbleBoy proof-of-concept worm was sent to Network Associates, who immediately posted a free software patch and alerted the FBI of the danger. The problem with this worm was that it would infect a host if an MS-Outlook user merely highlighted the subject line of the carrier e-mail message — no double-clicking required. The worm's payload was mild — changes to the registry and a simple display screen — but experts warned that the same techniques could carry much more dangerous payloads in future variations. The worm spread by mailing itself to every e-mail address on the infected system's address list, thus posing an even greater potential danger than the Melissa worm. [This attack again demonstrates the foolishness of allowing automatic execution of code by e-mail and word-processing packages.]

Category 14.2 *Worms*

1999-12-10 **virus worm e-mail denial-of-service crash attachment police**

News wires, ZDNet
http://dailynews.yahoo.com/h/zd/19991210/tc/19991210060.html

The search for the originator of the Melissa e-mail computer virus/worm began immediately after the outbreak. Initial findings traced the virus to Access Orlando, a Florida ISP, whose servers were shut down by order of the FBI for forensic examination; the systems were then confiscated. That occurrence was then traced back to Source of Kaos, a free-speech Web site where the virus may have lain dormant for months in a closed but not deleted virus-distributor's pages. In an interesting wrinkle, the MS-Word serial number on the original infected documents were circulated on the Net to help track down the perpetrator. The next steps turned to AOL, where the virus was released to the public. The giant ISP's information named a possible suspect and by the 2nd of April, the FBI arrested David L. Smith (aged 30) of Aberdeen, NJ. Smith apparently panicked when he heard the FBI were on the trail of the Melissa spawner and he threw away his computer — stupidly, into the trash at his own apartment building. Smith was charged with second degree offenses of interruption of public communication, conspiracy to commit the offense and attempt to commit the offense, third degree theft of computer service, and third degree damage or wrongful access to computer systems. If convicted, Smith faced a maximum penalty of 480,000 dollars in fines and 40 years in prison. On 10 December, Smith pleaded guilty to all federal charges and agreed to every particular of the indictment, including the ICSA.net estimates of at least $80M of consequential damages due to the Melissa infections.

Category 14.2 *Worms*

2000-01-01 **script worm e-mail Outlook**

SecurityPortal, Computer Associates, SARC

The Wscript.Kak was identified in late December 1999 by Computer Associates. This worm spreads through e-mail using only Outlook Express 5.0 running on Windows 98. With Internet Explorer 5 settings at low or medium, the embedded script executes automatically, without user intervention. That is, the worm replicates even if the user does _not_ open or preview an infected attachment. Once loaded, the worm attaches a copy of itself to every outbound e-mail message. By April 2000, this worm was the top infectious code in Europe, the Asia Pacific region and the USA.

Category 14.2 *Worms*

2000-01-03 **worm IRC e-mail**

SecurityPortal.com (reprinted with permission),
http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=VBS_TUNE

Trend Micro Virus Alert: VBS_TUNE: This worm is fast spreading and uses email (Microsoft Outlook) and IRC servers (mIRC, and PIRCH). This worm is destructive and it spreads in the same way as the Melissa virus, but unlike Melissa, VBS_TUNE also uses IRC servers for propagation.

Category 14.2 Worms

2000-01-15 **e-mail-enabled dropper worm Trojan**

F-Secure http://www.f-secure.com/v-descs/haiku.htm

F-Secure (formerly Data Fellows) identified another e-mail enabled worm they called Haiku. Its carrier was a detailed e-mail message about a Haiku generator which actually works. However, the worm code spreads through appropriation of the victim's e-mail address list.

Category 14.2 Worms

2000-05-08 **worm e-mail malware**

NewsScan

The I LOVE YOU computer worm struck computers all over the world, starting in Asia, then Europe. The malicious software spread as an e-mail attachment, sending itself to all the recipients in standard e-mail address books.] Within days, there . . .[were] new variations of the destructive software program popularly known as the Love Bug because it's sent as an attachment with the words "I love you" in the subject line. In one variation, the subject line purports that the message you're receiving contains a joke, and in another you're told that the message is a confirmation notice for a Mother's Day gift order. To avoid being affected by the bug, do NOT open attachments to suspicious e-mail messages. (ZDNet 5 May 2000)

Philippine authorities . . . detained a 27-year-old man for questioning after searching the house of the suspected creator of the infamous "Love Bug" virus. The virus, called the most virulent ever created, was responsible for deleting files on computers worldwide, as it wormed its way from computer to computer using e-mail address books to target its next victims. The main suspect is said to be a 23-year-old woman living with the man who was detained, a young computer student from a middle-class family. Detectives have said it is possible that the suspect is not responsible, but her computer certainly is: "It was only [her] computer used to launch the virus that was traced but anybody could use that computer," said an official with the Philippine National Bureau of Investigation. "The user here is invisible, it could be anybody. The difference is that the person we have identified is the registered owner of that computer." (Reuters/TechWeb 8 May 2000)

[On 11 May,] Filipino computer science student Onel de Guzman of AMA Computer College in Manila . . . told authorities that he may accidentally have launched the destructive "Love Bug" virus out of "youthful exuberance." However, he would not admit that he had himself created it, saying in Tagalog: "It is one of the questions we would rather leave for the future." The name GRAMMERSoft, a computer group to which the 23-year-old man belongs, appears in the computer code of the virus, and reporters have learned that de Guzman's thesis project was rejected by AMA officials because it described a way of illegally obtaining passwords from other computer users. But investigators have not charged either de Guzman or his friend Michael Buen of any crime, nor identified them as suspects. Asked what he felt about the massive amount of damage caused around the world by the virus, de Guzman's reply was: "Nothing." (AP/San Jose Mercury News 11 May 2000)

Philippine authorities investigating the source of the "Love Bug" computer virus that originated in that country . . . [said] they have more than four principal suspects who may have been responsible for launching the virus, which destroys computer files, steals passwords, and replicates itself by sending copies of the virus to everyone in the infected computer's address book. Suspects include Onel de Guzman, a 24-year-old dropout of a computer school, and his friend Reonel Ramones, the only one of the group of suspects who will definitely be charged with criminal wrongdoing. The names of the other suspects were found on diskettes confiscated from the apartment Ramones shared with de Guzman and de Guzman's sister. (Reuters/San Jose Mercury News 12 May 2000)

Category 14.2 Worms

2000-05-19 **worm e-mail enabled malware Outlook**

NewsScan

A variation on the "Love Bug" computer [worm] . . . [started] going around [in May], destroying most of the files on computers it defects. Targeted at users of Microsoft's Outlook mail program, the . . . [worm] is contained in the attachment of a ".vbs" attachment arriving in an e-mail message with a subject line starting with "FW:" followed by a randomly selected name. If you receive such a message, do not open the attachment. (AP/Washington Post 19 May 2000)

Category 14.2 Worms

2000-06-06 **malware worm denial of service e-mail cell phone propaganda hactivism vandals**

NewsScan, MSNBC http://www.msnbc.com/news/417066.asp

The first-ever computer . . . [worm] targeting cell phones is causing anxiety in Spain, where about 100 infections have been reported so far. The "I-Worm.Timofonica" virus works in much the same way as the ILOVEYOU . . . [worm] that wreaked havoc on computer systems last month — it arrives as an e-mail attachment that, when opened, sends a copy of itself to everyone in the victim's Microsoft Outlook address book. For each one of those messages, it generates a random cell phone number from a block of numbers known to be used by Spanish telecom carrier Telefonica. A short message is then sent to each mobile phone, castigating Telefonica for alleged monopolistic tendencies and questionable corporate practices. As a final insult, it also attempts to delete all files on the victim's hard drive and performs several other operations that makes restoration difficult. "Two or three viruses down the road we might see these things taking out phones," warns one security specialist. (MSNBC 6 Jun 2000)

Category 14.2 Worms

2000-06-19 **worm Trojan e-mail scrap object file suffix masquerade**

NewsScan, San Jose Mercury News http://www.sjmercury.com/svtech/news/breaking/merc/docs/009074.htm, San Jose Mercury News http://www.sjmercury.com/svtech/news/breaking/merc/docs/021805.htm

A new computer . . . [worm] called "Stages," is going around and clogging the e-mail systems of some organizations. Like the recent "Love Bug" . . . [worm] it multiplies by sending a copy of itself to everyone listed in the infected computer's address book; however, unlike that other . . . [worm], it masquerades as a ".txt" file even though it's really a ".shs" file that can contain executable and malicious code. Beware of opening the attachment of any e-mail message containing the words "funny," "life stages," or "jokes" in the subject line. (AP/San Jose Mercury News 19 Jun 2000)

[By early August,] There . . .[were] more than 200 reported cases in Japan of a computer virus called "Stages" that invades address books in the Microsoft Outlook software of computer users who open an e-mail attachment labeled Life-Stages.txt.shs. The virus apparently originated in the U.S. If you receive an e-mail attachment of that kind, do not open it. (AP/San Jose Mercury News 3 Aug 2000)

Category 14.2 Worms

2000-08-21 **worm criminal hacker prosecution jurisdiction**

NewsScan

Deciding that new laws against computer crime could not be applied retroactively, the [U.S.] Justice Department . . . dropped charges against the former college student suspected of responsibility for unleashing the "Love Bug" computer . . . [worm] last May. Worldwide damages were estimated at up to $10 billion. (USA Today 21 Aug 2000)

Category 14.2 Worms

2000-11-01 **virus worm payload remote control e-mail Trojan dropper**

NASA Incident Response Center http://www-nasirc.nasa.gov/nasa/whats_new.html B-00-156

The SONIC worm was found in the wild on Oct 30. This nasty remote-control worm arrived by e-mail with subject "I'm your poison" and an attachment (either GIRLS.EXE or LOVERS.EXE). If the Trojan dropper is run, it installs a core process that then searches for payload instructions on a site in the GeoCities Web-hosting service. The current payload opens a backdoor to the infected system and also monitors activity, much like BackOrifice. There were already several variants in circulation by the time the worm was discovered by Kaspersky Labs. There was some hope that the original hard-coded GeoCities site could be shut down, but it was likely that other payload-supply sites would be encoded in new variants.

Category 14.2 Worms

2001-02-12 **encrypted Visual Basic worm infection malware**

Central Command

VBS.SST.A, aka Calamar, Kalamar.A and Anna Kournikova worm is a Visual Basic Script worm that spread rapidly worldwide starting in February 2001. Central Command described it as follows:

"The worm travels via an email message with the following text:

Subject line: Here you have, ;0)
Message body: Hi: Check This!
File attachment: AnnaKournikova.jpg.vbs

The worm attempts to trick users into executing the file attached to the e-mail message by pretending to be a jpeg graphic image of the Russian tennis player Anna Kournikova.

On January 26th the worm attempts to connect to a website www.dynabyte.nl

The worm modifies the systems registry by creating an entry named HKEY_CURRENT_USER\software\OnTheFly

When the worm is activated it emails itself to every address in the Outlook address book."

A week later, Trend Virus reported, "Several variants of the "Anna Kournikova" virus a.k.a. VBS_KALAMAR.A have emerged in the wild. These variants are similar to the previous virus and are detected by Trend antivirus, however, they differ in their subject header and message body. Like VBS_KALAMAR.A, these variants were also created using the VBSWG virus construction kit. Trend provided protection against Anna Kournikova before it began to spread, and Trend customers who had updated their pattern file and scan engine on a regular basis did not have to worry about this fast-spreading virus."

Category 14.2 Worms

2001-03-09 **Visual Basic VBS worm generator**

Viruslist.com

Viruslist.com issed the following warning: "As it became known on March 9, a computer hacker going by the pseudonym of [K]alamar--who belongs to a cyber-hooligans group from Argentina and is known to be the author of the script-virus generator "Vbs Worms Generator", which was used to create the infamous "Kournikova" virus--has released a new version of his program. Kaspersky Lab immediately responded to the discovered threat and already has integrated a new universal anti-virus module."

Category 14.2 Worms

2001-08-06 **worm patch vulnerability**

NewsScan

"CODE RED II" WORM TARGETS NT AND 2000
Web site administrators who are running Microsoft's Windows NT or 2000 operating systems are being urged to download a software patch from the Microsoft site to protect against a new "worm" called Code Red II. Individual users have little to worry about for now: there is no direct risk to people running the Windows 95, 98, or Me operating systems or those using Macintoshes. (AP/USA Today 6 Aug 2001)
http://www.usatoday.com/life/cyber/tech/2001-08-05-code-red2.htm

---

Category 14.2 Worms

2001-08-09 **e-mail enabled worm virus Web defacement**

NewsScan

FIGHTING THE "CODE RED" WORM [30 Jul 2001]
Representatives from the White, the FBI, Microsoft and others are engaging in a public information campaign to alert computer users of the dangers of the "Code Red" worm that exploits a flaw in Windows NT and 2000 operating systems and defaces Web sites with the words "hacked by Chinese." The vandals have left this message on hundreds of thousands of computers connected to the Internet, and the government-funded Computer Emergency Response Team predicts that the worm will start spreading again this week and "has the potential to disrupt business and personal use of the Internet." Microsoft has a patch for problem on its Web site. (AP/San Jose Mercury News 30 Jul 2001)
http://www.siliconvalley.com/docs/news/svfront/004342.htm

NO PERSONAL DATA COMPROMISED BY CODE RED'S HIT ON HOTMAIL [9 Aug 2001]
Microsoft says that the "Code Red" worm struck some of servers running its MSN Hotmail service, which provides e-mail access to 110 million people, but that no personal information was breached. Code Red attacks only Windows NT and Windows 2000 software used on Web servers, and does not affect Windows 95, 98, or Me. (CNet/New York Times 9 Aug 2001)
http://partners.nytimes.com/cnet/CNET_0-1003-200-6826572.html

---

Category 14.2 Worms

2001-11-27 **e-mail enabled worm keystroke capture logging audit confidentiality**

NewsScan

NEW "WORM" CAN CAPTURE KEYSTROKES [27 Nov 2001]
A malicious program called Badtrans is moving around the Internet and worming itself into vulnerable computers and using a keystroke logger to surreptitiously record passwords, credit data, and other information. A virus manager at the security firm McAfee says that the worm "does no damage to files but does drop a backdoor trojan on the machine which would allow a hacker to come back and access personal information." Badtrans spreads through Microsoft's Outlook or Outlook Express e-mail programs and arrives with an attachment that can be executed simply by reading or previewing it and doesn't need to be double-clicked or opened separately. (Reuters/San Jose Mercury News 27 Nov 2001)
http://www.siliconvalley.com/docs/news/svfront/034639.htm

Category 14.2 Worms

2002-05-05 **worm virus e-mail social engineering**

RISKS 22 05

In April 2002, a variant of the the KLEZ worm family known since November 2001 became a major threat to MS Outlook users worldwide. Peter G. Neumann summarized the situation:

A rogue computer program that is the online equivalent of a quick-change artist is infecting computers around the world via e-mail and clogging computer networks. The program, W32/KLEZ.H, is a "blended threat," combining elements of a virus, which infects machines, and a worm, which transports itself from machine to machine. It also tries to disable some antivirus programs. It makes itself hard for users to spot by changing its e-mail subject line, message and name of the attachment at random, drawing from a database that includes, for example, such subject lines as "Hello, honey," and "A very funny Web site." The program has grown increasingly common as users unknowingly activate it sometimes without even opening the e-mail attachment that carries the virus and allow it to send copies of itself to those in the victim's e-mail address file.

Category 14.2 Worms

2002-05-05 **worm virus e-mail social engineering**

RISKS 22 05ff

By early May 2002, the KLEZ.H worm/virus was spreading extremely fast on the Internet and was having secondary effects. For one thing, because of the habit of forging e-mail headers to make it look as if someone on a victim's address list was the originator, many non-infected people were receiving angry e-mail from victims claiming that they were spawning infected e-mail. Worse, some of the recipients complained to system administrators or ISPs, causing much confusion and wasted effort as everyone had to figure out that the supposed originator was nothing of the sort. For another, some of the anti-virus products were firing off automated warnings to the supposed originators of infected messages; when these recipients happened to have enabled autoreply messages (the dreaded "I am out of the office" script), there was a real risk of mailstorms as each additional message from the supposedly infected source prompted yet another warning. Bounce messages also contributed to the mayhem.

Category 14.2 *Worms*

2002-05-20 **worm vulnerability exploit browser**

Security Wire Digest 4 39

*NEW WORM ON THE PROWL
A new worm called W32.Yaha.c@mm is slowly making inroads on users' computers by capitalizing on unpatched Microsoft Windows systems. Exploiting the "Incorrect MIME Header Can Cause IE to Execute E-mail Attachment" vulnerability, it uses a two-part extension. The first is chosen from .doc, .mp3, .xls, .wav, .txt, .jpg, .gif, .dat, .bmp, .htm, .mpg, .mdb or .zip. The second is chosen from .pif, .bat or .scr. The worm searches an infected user's hard drive, address book and Instant Message programs for e-mail addresses and then mass mails itself. However, the worm is flawed and won't work unless MSN Messenger is installed on a system.

Category 14.2 *Worms*

2002-05-21 **P2P peer-to-peer networks file sharing worm attack sabotage information warfare infowar motivation pornography**

FindLaw Download This 86

ITS CREATOR SAYS KAZAA BENJAMIN WORM MEANS WELL
The creators of a new worm that targets users of the Kazaa file-trading network say they released the code to frustrate Internet users searching for pirated software and child pornography. Anti-virus software vendors have issued warnings that the so-called "Benjamin worm" is being unintentionally propagated among Kazaa users who download any of dozens of executable programs and screen savers that have been infected with the malicious code. According to one of its developers, Paul Komoszki, Benjamin is a "controlled test" of a program designed to disrupt the illegal exchange of copyrighted data and child porn over peer-to-peer networks.
http://www.newsbytes.com/news/02/176684.html

Category 14.2 *Worms*

2002-09-18 **malware worm Linux servers denial-of-service attack DoS**

NewsScan

'SLAPPER' WORM IS A DRONE-IN-WAITING
The computer security firm Network Associates is calling attention to "Slapper," an invasive network "worm" capable of insinuating its way into Linux server computer systems and waiting until it, and many others like it, are activated to produce denial-of-service attacks that can overwhelm targeted Web sites. Network Associates' researcher Jimmy Kuo says the worm is being closely monitored and currently presents no great risk, but says "it could turn on a dime and become a wide spreader if someone fed in a new version." (Reuters/USA Today 2002)

Category 14.2 *Worms*

2002-10-01 **worm back door keystroke logger bug flaw browser known vulnerability e-mail**

NewsScan

ANOTHER WORM ATTACKS INTERNET EXPLORER: THE BUGBEAR
Taking advantage of a known vulnerability in Microsoft's Internet Explorer software, the Bugbear worm now moving around the world opens up a back door in the computers and logs keystrokes. But a bug in the worm (this is beginning to sound silly) has prevented Bugbear from taking over the address list on a computer and sending itself to new people. Ranked now as only a "medium risk" nuisance, it appears under a large variety of names but the attachment typically has a double file extension, such as .doc.pif. (Forbes 30 Sep 2002)

Category 14.2 *Worms*

2003-01-10 **virus alert Internet anti-virus undetected mass mailing F-Secure**

NIPC/DHS

January 09, eSecurity Planet — Virus Alert: W32.Lirva.A and ExploreZip.

Two major viruses have struck the Internet at the same time. ExploreZip, an Internet worm first let loose in the wild back in 1999, has reemerged with just enough changes made to allow it to slip through anti-virus software undetected. And it has the added ability to override files on the infected computer, as well as on any other computer in the same network. Once ExploreZip infects a computer, it will automatically respond to any email received with a seemingly valid subject line and the user's name, along with an infected attachment. Another problematic virus is the mass-mailing worm that pays tribute to Canadian singer Avril Lavigne. The worm is going under a few different names, including Avril and Lirva (which is Avril spelled backwards). Although this virus is less destructive than ExploreZip, anti-virus software company F-Secure Corp. has rated both viruses as Level 2 Threats, the second-highest threat category. The Lirva worm got a Level 2 rating because of the speed with which it's spreading around the world. It reportedly originated, in middle Europe and has spread to Turkey, the United States and Southeast Asia in less than 48 hours. Once Lirva infects a computer, it opens the computer's Internet Explorer browser to official Avril Lavigne Web site on the 7th, 11th and 24th of the month. It then starts to display colored circles on

---

Category 14.2 *Worms*

2003-01-14 **virus Internet alert SMTP engine self-propagating**

NIPC/DHS

January 13, ZDNet — Virus alert: W32/Sobig-A.

Anti-virus experts are warning of a new virus, code-named W32/Sobig-A, which was discovered late last week and spread rapidly over the weekend. Sobig is a mass-mailing worm incorporating its own SMTP engine, according to antivirus companies. It arrives from the e-mail address "big@boss.com" and bears a subject line such as "Re: here is that sample", "Re: Movies", "Re: Document" or "Re: Sample". The e-mail contains an attachment called "Document003.pif", "Sample.pif", "Untitled1.pif" or "Movie_0074.pif". It affects the Windows 95, 98, Me, NT, 2000 and XP platforms. When the attachment is clicked on, it runs a program that searches for files containing e-mail addresses and uses these to send infected e-mails. It also connects to a Web site and downloads a text file containing another Web address, from which it attempts to download and run another program. MessageLabs speculated that this program was a backdoor trojan horse, which could allow a hacker to take control of the user's PC. If there is a local-area network connection, Sobig attempts to copy itself onto shared network folders. CERT/CC has received over one hundred reports of this worm. Anti-virus software companies Sophos, Symantec and McAfee have published instructions on their websites for blocking and removing the worm.

Category 14.2 *Worms*

2003-01-27 **worm damage Internet servers patches**

NewsScan

INTERNET WORM TOOK ONLY 10 MINUTES TO CAUSE GLOBAL HAVOC
The "SQL Slammer" worm that slowed Internet traffic significantly [in late January 2003] managed to infect computer servers worldwide in about 10 minutes, making it the fastest such virus seen, according to a University of California at San Diego team. "At its peak, achieved approximately three minutes after it was released, the worm scanned 55 million Internet hosts per second. It infect ed at least 750,000 victims, and probably considerably more," says one team member. The SQL Slammer worm was only the third of its type seen on the Net, and managed to spread nearly 100 times faster than the Code Red infection 18 months ago. (The Independent 4 Feb 2003)

THE WORM TURNED BACK: SLAMMER DAMAGE CONTAINED
[By the 27th of January, it was] unlikely that there [would] be much additional destruction from the so-called Slammer computer worm that wreaked damage on the Internet over the weekend, by infecting more than a quarter of a million computer servers and clogging networks throughout the world. The worm targeted a known [vulnerability] in Microsoft's 2000 SQL server database server; the company had issued software security patches in July but many network administrators had failed to install them. But now the worst appears to be over, says an executive at the security firm Symantec. (USA Today 27 Jan 2003)

MICROSOFT, HEAL THYSELF!
Microsoft has been embarrassed by having to acknowledge that the SQL Slammer virus, which infected computer servers all over the world, also contaminated some of Microsoft's own servers, because system administrators had failed to heed the company's own advice to install a software patch months ago to fix a known system vulnerability. A Microsoft executive had to admit: "We, like the rest of the industry, struggle to get 100% compliance with our patch management. We recognize — now more than ever — that this is something we need to work on. And, like the rest of the industry, we're working to fix it." (New York Times 28 Jan 2003)

Category 14.2 *Worms*

2003-02-03 **Slammer worm avoidable vulnerability detection tool available NSA NIPC FBI SANS**

NIPC/DHS

January 31, Computerworld — Free benchmark could have found Slammer vulnerability.

Industry experts and users said the Slammer worm should have been a non-issue for companies because the patches and a free tool capable of detecting the vulnerability exploited by the worm were available six months ago. In particular, they point to the issuance in July of the Consensus Minimum Security Benchmarks, also known as the Gold Standard. Developed jointly by five federal agencies, including the National Security Agency (NSA) and the FBI's National Infrastructure Protection Center, as well as the SANS Institute and the Center for Internet Security (CIS), the Gold Standard benchmark can be used to test Windows 2000 Professional systems running as workstations for proper configuration. Alan Paller, director of research at SANS, said an NSA study of the benchmark concluded that by running it on a network a company could eliminate more than 90% of known vulnerabilities. Claude Bailey, an IT security analyst at one of the nation's largest financial management firms, said that while the Gold Standard is a good starting point, his security administrators say the problem isn't in detecting the vulnerability but in deploying the patches and fixes across an organization of 50,000 employees — and guaranteeing that the patch won't cause more problems. "We tested the original patch [for the SQL vulnerability], and it had problems," said Bailey. Now, with the financial firm in the middle of tax season, there's too much to lose to deploy patches that break other parts of the network.

Category 14.2 *Worms*

2003-02-05 **study Slammer worm fastest ever SQL Server Microsoft vulnerability**

NIPC/DHS

February 03, IDG News Service — Study: Slammer was fastest-spreading worm yet.

A just-completed study into the Slammer worm, which hit the Internet a week ago, has concluded that Slammer was the fastest-spreading worm yet seen. The study was conducted by a group of experts representing the Cooperative Association for Internet Data Analysis (CAIDA); the International Computer Science Institute; security company Silicon Defense; the University of California, Berkeley's electrical engineering and computer sciences department; and the University of California, San Diego's computer science and engineering department. Slammer's spread was fast for several reasons. At just 376 bytes in size, the worm and required headers fit inside a 404-byte Universal Datagram Protocol packet. Code Red, which hit in mid-2001, was 4KB in size. The worm also worked differently from Code Red. Slammer generated random IP addresses and dispatched itself to those addresses without scanning to find out whether the target machine was running either of the two pieces of software that were vulnerable to attack: Microsoft Corp.'s SQL Server 2000 database and MSDE 2000 (Microsoft SQL Server 2000 Data Engine). Because of its random nature, given enough time, the worm would hit all vulnerable machines. Spread of the worm eventually began to slow because bandwidth from infected machines to the Internet couldn't support the exponential growth in IP packets being generated. Its signature, attacking a specific port on vulnerable systems, was also easy to detect, and network-level blocking of the ports in question was effective in slowing the worm. In the past, worms often targeted only software for which there was a large installed base of users. But given the speed with which Slammer-like worms can spread, less popular software now also presents a viable breeding ground for worms, the report said.

Category 14.2 *Worms*

2003-03-11 **worm network Windows passwords target F-Secure**

NIPC/DHS

March 10, IDG News Service — New worm targets weak Windows passwords.

A new worm, W32/Deloder-A (Deloder), appeared on Sunday and is considered a low risk for infection, according to an alert posted by anti-virus company F-Secure. The worm, which is believed to have originated in China, attempts to connect to other computers on a network through TCP (Transmission Control Protocol) port 445, randomly generating IP addresses to locate vulnerable machines. If the worm succeeds in breaking the Administrator account password, it places copies of a backdoor (trojan) program known as "inst.exe" in several locations on the infected machine. Machines running Windows 95, 98, NT, 2000, ME and XP are vulnerable to attack by Deloder, Symantec said. No infections from Deloder have been reported and most firewalls block access to port 445. Computer users are advised to contact their anti-virus company for further details.

Category 14.2 *Worms*

2003-03-11 **worm dictionary attack password administrator**

NewsScan

DELOADER WORM ATTACKS EASY-TO-GUESS PASSWORDS
A new software worm called W32/Deloader-A tries to guess passwords on machines running many of the Microsoft Windows operating systems: it attempts to log on to a machine's administrator account by trying likely passwords such as 'admin', 'password,' '12345', and 'administrator', and so forth. The worm is thought to have originated in China. Although Deloader is considered a low risk for infection, many home computers without firewalls may be vulnerable to its attacks.
(IDG/Computerworld 11 Mar 2003)

Category 14.2 *Worms*

2003-03-12 **worm network Code Red II variant discover Internet Information System IIS infect**

NIPC/DHS

March 11, eWEEK — New variant of Code Red II discovered.

Security experts are watching a new variant of the Code Red II worm that began appearing on some monitoring networks Tuesday. The worm is nearly identical to its ancestor, save for a modified drop-dead date that is now several thousand years in the future. Known as Code Red.F, the worm uses the same infection method as the previous versions, attacking Web servers running Microsoft Corp.'s IIS software. The worm so far has infected only a few machines, and because most administrators patched their servers after the initial Code Red outbreak in 2001, it is unlikely to spread extensively, experts say. All of the Code Red worms exploit an unchecked buffer in the Index Server in the IIS software. They then spread by infecting one machine and then scanning a list of random IP addresses and attempting to connect to port 80. The original Code Red, which struck in July 2001, infected several hundred thousand IIS servers and caused massive traffic disruptions on some portions of the Internet.

Category 14.2 *Worms*

2003-03-19 **worm network vulnerability lax security policy**

NIPC/DHS

March 17, eWEEK — Deloder, Lovgate worms mark perils of slack security policy.

Many computer users persist in using their names or children's birthdays as log-on credentials, and two recent worm outbreaks have shown why that's such a risky practice. Deloder, the latest worm to hit vulnerable Windows machines, as well as a recent version of Lovgate, both use a list of common passwords in an attempt to compromise computers. Lovgate began spreading late last month, while Deloder appeared last week. Although neither worm has spread as far or as fast as threats such as SQL Slammer or Code Red, both Deloder and Lovgate clearly illustrate the danger inherent in lax security policies. In Deloder's case, the worm tries to connect to random Windows NT, Windows 2000 and Windows XP machines on TCP port 445, normally used by Microsoft Corp.'s Active Directory. It then looks for network shares on the remote machine and, if it finds any, tries to copy itself to the shares by using easily guessed passwords to gain access. The worm also installs a Trojan horse and a utility for executing commands on remote machines. Lovgate behaves in a similar fashion. It spreads from an infected machine using the Messaging API Windows functions by answering recent mail with an infected reply. It then tries to copy itself to network shares and their sub-folders. If the folders are password- protected, Lovgate tries passwords such as "admin" and "123."

Category 14.2 *Worms*

2003-03-21 **Iraq war worm network social engineering spy satellite photos entice**

NIPC/DHS

March 18, Sophos — Swedish computer worm lures with Iraq spy satellite photos.

Sophos researchers report that they have discovered a new email-aware worm that feeds on public interest in the imminent war in Iraq in an apparent attempt to lure unsuspecting users. The W32/Ganda-A worm, which appears to have been written in Sweden, uses a variety of different email subject lines and message bodies in both English and Swedish to try and encourage computer users to run its viral attachment. Possible subjects are "Spy pics," "GO USA" and "Is USA always number one?" In a bizarre twist, the author of W32/Ganda-A claims to have a grievance with the Swedish educational system. Companies should consider blocking all Windows programs at their email gateway. Computer users should keep their anti-virus software updated.

Category 14.2 *Worms*

2003-05-19 **e-mail worm Palyh internet masking support@microsoft.com F-Secure registry windows address directories**

NIPC/DHS

May 19, IDG News Service — Palyh worm disguises itself as an email from Microsoft.

A mass-mailing e-mail worm known both as W32/Palyh and W32.HLLW.Mankx@mm is spreading on the Internet, masking itself as a message from support@microsoft.com. The worm arrives as an executable attachment to e-mail messages with a variety of subjects and messages. The virus can be released only when a user clicks on the attachment file, anti-virus company F-Secure Corp. said. Once released the virus code modifies the Windows registry so that the worm program is launched whenever Windows is run. It also searches an infected computer for files containing e-mail addresses that it can send itself to and looks for computers that are accessible through shared directories on a network and copies itself to those machines. Anti-virus vendors are advising customers to update their anti-virus software.

Category 14.2 *Worms*

2003-06-02 **e-mail virus bill gates Sobig-C forward addresses infected computers MessageLabs Please see the attached file screensaver.scr movie.pif documents.pif infect computers bill@microsoft.com**

NIPC/DHS

June 02, BBC News — E-mail virus uses Bill Gates.

A Windows virus, called Sobig-C, is spreading widely across the Internet. It does not harm a computer but forwards itself to any addresses found on the infected computer, using several faked addresses such as bill@microsoft.com. Anti-virus companies have rated Sobig-C as a high risk virus. According to e-mail filtering firm MessageLabs, it was first spotted on May 31 in the U.S. Users should watch for e-mails containing subject lines such as "Re: Movie", "Re: Approved", or "Re: Your application", with the message "Please see the attached file". The worm uses a number of different attachment names including "screensaver.scr", "movie.pif" and "documents.pif". Users are advised to delete any suspect e-mails and to update their anti-virus software.

Category 14.2 *Worms*

2003-06-05 **Bugbear virus internet logging keystrokes PCs confidential information**

NIPC/DHS

June 05, Reuters — Variant of Bugbear virus spreading on PCs.

A variant of the Bugbear worm, which spread around the Internet last October, opening back doors on computers and logging keystrokes, has started to infect users around the world, putting them at risk of losing confidential information. According to Mikael Albrecht of computer security company F-Secure, the worm includes a large list of domains belonging mostly to banks. "The list...includes banks from all over the world; Europe, US, Asia and Africa. Bugbear.B changes system settings if activated in one of these banks," he said. The worm variant is better at using addresses in a user's e-mail program than the original, sending itself to those addresses using the infected user's identity, said David Emm of anti-virus company Network Associates Inc. Once activated, Bugbear.B tries to disable some security programs and starts to snoop on an infected system. Bugbear.B takes advantage of a known vulnerability in Microsoft Corp.'s Internet Explorer and can be run automatically simply by reading the e-mail and not opening the attachment. Users are advised to keep their anti-virus software updated.

Category 14.2 *Worms*

2003-06-06 **University Stanford spam e-mail sensitive information computer system campus PCs salary bonus**

NIPC/DHS

June 06, Mercury News — Virus sends confidential Stanford information out in e-mail.

People at Stanford University got spam Thursday containing sensitive information including confidential details about employee salaries and bonuses. The Bugbear.B virus that infected the university's computer system Thursday sent out files at random from campus PCs. It's unclear if outsiders read the rogue e-mails, but some of the 35,000 computer users inside Stanford did — including the man in charge of Stanford's computer systems. The university Web site said Stanford's computer crew intercepted messages containing salary and bonus information.

Category 14.2 *Worms*

2003-06-18 **Sobig-D worm variant support@microsoft.com admin@support.com network shares e-mail randomized subject lines anti-virus**

NIPC/DHS

June 18, The Register — Fresh variant to Sobig worm.

A new variant in the Sobig series appeared Wednesday. Sobig-D is a little different from its predecessors the Sobig-B (support@microsoft.com) and Sobig-C (bill@microsoft.com) worms. Infectious emails sent out by Sobig.D appear to come from admin@support.com. The worm is spreading modestly and causing only a minimal amount of damage. Most vendors rate it as low risk. Although it normally spreads via email, Sobig-D can also spread through network shares. In its more common email form, Sobig-D appears as email with randomized subject lines (such as Re: Documents and Re: Movies) and carries infectious .scr and .pif attachments. Like its predecessors, Sobig-D has a built-in expiration date—in this case July 2. Users should keep their anti-virus software updated.

Category 14.2 *Worms*

2003-06-23 **Fortnight worm exploits Windows JavaScript worm VM ActiveX micorosft anti-virus registry keys**

NIPC/DHS

June 23, The Register — Fortnight worm exploits antique Windows vuln.

Windows users are being infected by a JavaScript worm - even though protection has been available for almost three years. The Fortnight JavaScript worm exploits a vulnerability in Microsoft VM ActiveX which makes it possible for malicious code to execute simply by reading an message in an HTML aware email client. Microsoft issued protection against the vulnerability in October 2000. Despite this, users are still becoming infected to a modest extent with recently released variants of JS/Fortnight-D and JS/Fortnight-F. The worm's actions include changing registry keys and adding links to various Web sites to a victim's favourites list. Users should keep their anti-virus software updated.

Category 14.2 *Worms*

2003-06-26 **Sobig.E worm computer networks CERT Carnegie Mellon web browser cache hard drives**

NIPC/DHS

June 26, Computerworld — Sobig.E worm spreading around globe.

The latest version of the Sobig worm, Sobig.E, has been making its way through computer networks around the world since Wednesday. The worm spreads by scouring an infected computer's hard drive for e-mail addresses in address books or even Web browser cache files, then sends itself out to the addresses it finds. It can spoof its sender's address, so the recipients believe they are receiving a message from someone they know. Graham Cluley of anti-virus software vendor Sophos says the new version of Sobig, which is set to expire on July 14, is being sent as a .zip file, perhaps to allow it to spread in corporate environments where .exe and other file types are automatically blocked in incoming e-mails. Marty Lindner of the CERT Coordination Center at Carnegie Mellon University in Pittsburgh, said the rapid spread of the worm since yesterday means recipients are still opening files in messages even when they have been warned countless times that it's unsafe to do so. Users should update their anti-virus software and should not open unsolicited attachments.

Category 14.2 *Worms*

2003-06-30 **computer virus data leakage Harvard university bugbear.b machine infection student records**

NIPC/DHS

June 30, U-Wire — Computer virus leaks files from Harvard.

The Bugbear.b virus hit the Harvard University campus June 6. When Bugbear.b infects a machine, it sends messages to recipients in an individuals' address book. In addition to a virus-laden attachment, such e-mails often contain text fragments from files on that machine, which may include documents and private correspondence. Harvard students reported receiving seemingly misaddressed messages bearing harmless communications. But at least one message received by at least three Harvard undergraduates contained a confidential memo concerning a case before the Administrative Board. Educational privacy law can penalize institutions who negligently or intentionally transmit their students' records. Director of Harvard Arts and Sciences Computer Services Frank Steen said that his department reacted quickly to the Bugbear virus and that the actual number of computers infected was minimal.

Category 14.2 *Worms*

2003-08-11 **W32/Blaster worm DCOM vulnerability RPC Remote Procedure Call msblast.exe denial of service**

NIPC/DHS

August 11, CERT/CC — CERT Advisory CA-2003-20: W32/Blaster worm.

The W32/Blaster worm exploits a vulnerability in Microsoft's DCOM RPC interface as described Microsoft Security Bulletin MS03-026. Upon successful execution, the worm attempts to retrieve a copy of the file msblast.exe from the compromising host. Once this file is retrieved, the compromised system then runs it and begins scanning for other vulnerable systems to compromise in the same manner. In the course of propagation, a TCP session to port 135 is used to execute the attack. However, access to TCP ports 139 and 445 may also provide attack. The worm includes the ability to launch a TCP SYN flood denial-of-service attack against windowsupdate.com. Unusual or unexpected traffic to windowsupdate.com may indicate a network infection, so system administrators may wish to monitor network traffic. Sites that do not use windowsupdate.com to manage patches may wish to block outbound traffic to windowsupdate.com. Users are encouraged to apply the patches available on the Microsoft Website:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS03-026.asp.

Category 14.2 *Worms*

2003-08-12 **MsBlast LoveSan Blaster microsoft update worms server target DHS copy cat attacks TCp UDP**

NIPC/DHS

August 12, U.S. Department of Homeland Security — Potential for Significant Impact on Internet Operations Due to Vulnerability in Microsoft Operating Systems (2nd UPDATE: Worm Spreading on the Internet).

The Department of Homeland Security (DHS) has issued a second update to the July 24, 2003 advisory on Microsoft operating systems. Today's update warns that malicious code dubbed "MSBlast," "Lovesan," or "Blaster" began circulating on the Internet on August 11th. This worm takes advantage of the vulnerability discussed in the July 24th advisory and contains code that will target Microsoft's update servers on August 16th. This additional attack could cause significant Internet-wide disruptions. It is possible that other worms based on this vulnerability will be released over the next few days as "copy cat" attacks. In this 2nd update, DHS recommends that the Microsoft update (available at http://microsoft.com/technet/treeview/default.asp?url=/techn et/security/bulletin/MS03-026.asp) be applied as soon as possible to the systems affected. In addition to blocking the TCP and UDP ports listed in the July 24th advisory, DHS further recommends that Ports 69 (TFTP) and 4444 be blocked when possible. Both of these ports are used to spread the worm.

Category 14.2 *Worms*

2003-08-13 **Blaster worm fix patch download site microsoft NT 2000 XP LoveSan Comcast Corp cable modem**

NIPC/DHS

August 13, eWEEK — Worm: long wait for fix.

Computer users were scrambling Wednesday, August 13, for alternate fixes for the havoc wreaked by the Blaster worm as many people were unable to reach Microsoft Corp.'s main patch download site. The Windows Update Web site was extremely sluggish Tuesday and Wednesday, and some users reported being unable to reach the site at all. The Blaster worm, also known as LoveSan, began infecting Windows NT, 2000 and XP machines Monday and continues to spread rapidly. The worm exploits a vulnerability in the Windows RPC (Remote Procedure Call) service and uses a lot of bandwidth scanning for other vulnerable machines once it has infected a PC. Microsoft made a patch available for the flaw in mid-July. Blaster is also causing service problems on Comcast Corp.'s cable modem network. Several Comcast customers said their service had been down for extended periods during the last couple of days and that Comcast officials said Blaster was to blame.

Category 14.2 *Worms*

2003-08-18 **MS-RPC DCOM worm infeting machines DoS Denial Service nacho welchia msblast.d ICMP**

NIPC/DHS

August 18, U.S. Department of Homeland Security — New version of the MS-RPC DCOM Worm infecting machines and creating Denial of Service Conditions.

A new worm that exploits the same security weakness as the Blaster worm (also known as "lovsan" or "msblast") has been released on the Internet. This new worm, dubbed "nachi", "welchia", or "msblast.d" does not infect systems that have been updated to counter the Blaster worm but will re-infect computers that are currently infected with Blaster or one of its variants. It deletes the original worm, patches the system by downloading the update from Microsoft, and replaces the original worm with itself. The variant then begins scanning or flooding the network with high volumes of ICMP (Internet Control Message Protocol) traffic causing network congestion which can result in denial of service conditions. Users should patch the MS-RPC DCOM vulnerability immediately using the instructions available on the Microsoft Website: http://www.microsoft.com/security/incident/blast.asp.

Category 14.2 *Worms*

2003-08-21 **virus network hacker Windows spread Sobig**

NewsScan

SOBIG IS FASTEST-SPREADING VIRUS EVER
The newest version of the Sobig virus is said to be the fastest-spreading network virus ever, and MessageLabs (a company that filters e-mail for corporate clients) intercepted more than a million copies of the "Sobig.F" virus in a single day — or one in every 17 e-mail messages the firm scanned. The virus spreads through Windows PCs via e-mail and corporate networks, and deposits a Trojan horse, or hacker back door, that can be used to turn victims' PCs into relayers of spam e-mail. Yesterday, a worm virus brought down the signaling systems of railroad company CSX Corp, causing delays and canceled trains through the Eastern states. (Dow Jones/AP/SJMN 21 Aug 2003)

Category 14.2 *Worms*

2003-09-03 **virus worm denial of service DoS availability patch operations interruption shutdown power plant**

NewsScan;http://www.usatoday.com/tech/news/computersecurity/2003-09-03-nuclear-plants-threat_x.htm

NRC ISSUES WARNING ABOUT VIRUS AND WORM ATTACKS
The Nuclear Regulatory Commission (NRC) is issuing a general warning to nuclear plant operators about computer failures that caused by network infections that caused a several-hour shut-down last January at the Davis-Besse nuclear power plant in Ohio. (The NRC emphasized that safety of that plant was not compromised by the computer failures or the shutdown.) The Davis-Besse plant operator, FirstEnergy Nuclear, determined that a contractor had established an unprotected computer connection to its corporate network, thereby allowing the Slammer worm to spread internally, since the utility had also failed to install a corrective software patch from Microsoft. (AP/USA Today 3 Sep 2003)

Category 14.2 *Worms*

2003-09-19 **internet explorer worm Anti-Virus companies Swen Gibe KaZaA Outlook Express shared networks e-mail Microsoft Corp. victim computer attachment patches Trojan Horse**

NIPC/DHS

September 19, Reuters — New worm targets Internet Explorer.

Anti-virus companies warned on Thursday, September 18, of a new computer worm circulating through e-mail that purports to be security software from Microsoft Corp. but actually tries to disable security programs that are already running. The worm, dubbed "Swen" or "Gibe," takes advantage of a two-year-old hole in Internet Explorer and affects systems that have not installed a patch for that security hole, according to an Internet security company. The malicious program arrives as an attachment to an e-mail pretending to contain a patch for holes in Internet Explorer, Outlook and Outlook Express and then mails itself off to addresses located on the victim's computer. The worm also can spread over Internet relay chat and the Kazaa peer-to-peer network, as well as copy itself over shared networks. Microsoft has cautioned customers in the past against e-mail software updates, saying it does not distribute patches as attachments, but rather directs them to its website.

Category 14.2 *Worms*

2003-11-04 **virus worm network Web Internet SMTP engine**

NIPC/DHS

November 03, vnunet.com — Destructive MiMail variant hits Web.

Antivirus firms have warned of a destructive worm that has just emerged in the wild. The W32/Mimail.c@MM, also known as Mimail.c, is a dangerous worm that bears similarities to W32MiMail@MM. Mimail.c contains its own SMTP engine for constructing messages, and mails itself as a zip or upx attachment. After being executed, Mimail.c e-mails itself out as an attachment with the filename 'Photos.zip'. Target e-mail addresses are harvested from the victim's machine and are written to the file eml.tmp in WinDir. Users should immediately delete any email containing the following 1) Subject: Re[2]: our private photos [plus additional spaces then random characters] 2) Attachment: 'photos.zip' (12,958 bytes) which contains 'photos.jpg.exe' (12,832 bytes). Also, in a bid to make the virus e-mails less conspicuous, the 'From' address of infected outgoing messages may be spoofed with james@(target domain.com) - for example, james@abc.com.

Category 14.2 *Worms*

2003-11-28 **worms malware mobile phones cellular spam SMS**

NYT http://www.nytimes.com/2003/11/28/technology/28cell.html?th

In Asia, where mobile phones are more popular than in the rest of the world, users are increasingly reporting problems due to worms — the electronic kind. Already, in Japan, there have been two worm attacks (in 2000 and in 2001) which caused cell phones to call emergency numbers. Antispam filters already block 55% of all messages to phones in the largest service providers in Japan, NTT DoCoMo. Cell phone manufacturers are designing new phones with the capability for fast software downloads to help fight malicious code and spam.

Category 14.2 *Worms*

2003-12-24 **Sober virus worm network anti-virus threat file sharing peer-to-peer mass-mailer**

NIPC/DHS

December 22, eSecurity Planet — Sober mutant starts to squirm. Anti-virus vendors on Monday, December 22, issued upgraded threat warnings for a mutant of the W32/Sober-C worm now squirming its way through e-mail in-boxes. The mass-mailer, which also spreads via file-sharing on P2P networks, has added a bilingual element and arrives with a range of attachment filenames—EXE, SCR, PIF, COM, CMD or BAT. Chris Beltoff of Sophos Inc. said the increased sightings of a mass-mailing virus at the height of the Christmas shopping season puts new PC owners at the highest risk. "The risk is high because of the new, unprotected computers that are being sold off the shelf. Depending on how long that PC has been sitting on the shelf, it's likely new PCs are unprotected against the latest viruses. Remember, the average consumer isn't going to make patching his main priority on a new computer, Beltoff said. Network Associates warned that 80 percent of the intercepted virus comes from Germany and said the characteristics of Sober-C has put Germans or users in German-speaking regions at higher risk.

Category 14.2 *Worms*

2004-01-02 **virus worm network Internet infestation MSN Panda Jitux.A aggressive malicious code**

NIPC/DHS; http://www.web−user.co.uk/news/47502.html

December 13, Web User — MSN virus hits the net.

Anti-virus company Panda Software has warned net users to watch out for a new virus, a worm called Jitux.A, which is spread via MSN Messenger. Jitux.A is an aggressive code that contains a link to the web page http://www.home.no// jituxramon.exe. Once open, the file JITUXRAMON.EXE automatically downloads, infecting your computer. The worm file stores itself in the computer's memory and sends new infected messages every five minutes to all contacts in your Messenger's Contact List. Users should update their anti-virus patch as soon as possible.

Category 14.2 Worms

2004-01-08 **new worm network warning Sophos**

NIPC/DHS; http://www.esecurityplanet.com/alerts/article.php/3295121

January 05, esecurityplanet.com — Multi-component worm searches for weak system passwords.

Sophos issued a low-level alert for W32/Randon-AB, a multi-component network worm that attempts to spread by copying components of itself to and executing them on remote ADMIN$ shares with weak passwords, on Monday, January 5. One component of the worm, B4AK.EXE, then attempts to download and execute a copy of the worm from a remote URL as a file called C:\SVCHOST.EXE. The main file is an SFX EXE which creates a folder called AL within the Windows system folder and drops and executes several files, some of which are legitimate utilities or innocuous files. The worm adds an entry to the registry Run Key to run H00D.EXE on system restart. Instructions for removing worms are at http://www.sophos.com/virusinfo/analyses/w32randonab.htm l

---

Category 14.2 Worms

2004-01-08 **MSBlaster worm network patch clean-up removal tool infection Microsoft Windows XP Nachi**

NIPC/DHS; http://www.theregister.co.uk/content/56/34751.html

January 07, Register — Microsoft releases Blaster clean-up tool.

Microsoft this week released a tool to clean up systems infected by the infamous Blaster worm and its sundry variants. The software should eradicate the worm from infected Windows XP and Windows 2000 machines. However, users will still have to apply the original patch to prevent re-infection. Normally, such clean-up technology is left to antivirus firms. But this isn't a normal viral epidemic: ISPs say the worm is still generating malicious traffic, months after its first appearance. Microsoft's Windows Blaster Worm Removal Tool will disinfect machines infected with either the Blaster or Nachi worms. Nachi, released shortly after the first appearance of Blaster in August, was designed to patch vulnerable systems. Rather than help out, Nachi has instead become a serious nuisance. Its aggressive scanning behavior blighted the operation of many networks - hence the need to kill the "cure", along with the original Blaster worm. The tool is available at http://www.microsoft.com/downloads/details.aspx?FamilyID=e70a0d8b-fe98-493f-ad76-bf673a38b4cf&displaylang=en

---

Category 14.2 Worms

2004-01-09 **worm variant Mimmail network e-mail Sophos**

DHS/IAIP Update; http://www.sophos.com/virusinfo/analyses/w32mimailn.html

January 08, esecurity Planet — Yet another Mimail variant surfaces.

On the heels of the Mimail.P worm surfacing on Wednesday, January 7, security vendor Sophos issued an alert for the N variant on Thursday, January 8. Like Mimail.P, W32/Mimail-N is a mass-mailing worm that disguises itself as a legitimate form from Paypal credit card information. If a network connection is detected on execution then two forms are displayed asking for credit card and personal information. Once this information is filled in, it is sent to a remote web site. If a network connection is not detected then the start page of Internet Explorer is changed to a web site with a satirical picture. The worm copies itself to ee98af.tmp and winmgr32.exe in the Windows folder and sets the following registry entry so that the latter is run on system startup: HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WinMgr32. This variant also creates a zipped copy of itself as zipzip.tmp in the Windows folder and drops the fake forms as index.hta and index2.hta to the root folder. The worm scans files on the hard disk for email addresses and stores the result in outlook.cfg in the Windows folder. Instructions for removing this variant are at
http://www.sophos.com/virusinfo/analyses/w32mimailn.html

Category 14.2 Worms

2004-01-09 **worm variant Mimmail network e-mail Sophos**

NIPC/DHS; http://esecurityplanet.com/alerts/article.php/3297071

January 08, esecurity Planet — Yet another Mimail variant surfaces.

On the heels of the Mimail.P worm surfacing on Wednesday, January 7, security vendor Sophos issued an alert for the N variant on Thursday, January 8. Like Mimail.P, W32/Mimail-N is a mass-mailing worm that disguises itself as a legitimate form from Paypal credit card information. If a network connection is detected on execution then two forms are displayed asking for credit card and personal information. Once this information is filled in, it is sent to a remote web site. If a network connection is not detected then the start page of Internet Explorer is changed to a web site with a satirical picture. The worm copies itself to ee98af.tmp and winmgr32.exe in the Windows folder and sets the following registry entry so that the latter is run on system startup:HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WinMgr32. This variant also creates a zipped copy of itself as zipzip.tmp in the Windows folder and drops the fake forms as index.hta and index2.hta to the root folder. The worm scans files on the hard disk for email addresses and stores the result in outlook.cfg in the Windows folder. Instructions for removing this variant are at
http://www.sophos.com/virusinfo/analyses/w32mimailn.html

Category 14.2 Worms

2004-01-20 **worm Bagle-A speading Microsoft calculator disguise**

NewsScan

NEW COMPUTER WORM: BAGLE-A

A new computer worm called Bagle-A carries an expiration date, giving security experts concern that it might be followed by more robust versions of the now-buggy program. Daniel Zatz, security director for Computer Associates Australia, says, "One of our biggest concern is that if we look back a year ago at the Sobig variants, they all had drop-dead dates, and every time one hit that drop dead date a new variant came out; a new and improved variant of it." Bagle-A arrives in e-mail inboxes as a message containing text suggesting the e-mail may be from a system administrator, as well as an executable attachment. PC users should not open the attachment; if they suspect their computers may be infected with the virus, they should look for a file called bbeagle.exe in their Windows System directory. The file disguises itself under the Microsoft calculator icon. (CNet/New York Times 20 Jan 2004)

Category 14.2 Worms

2004-01-20 **worm networkshare infect weak password**

NIPC/DHS; http://esecurityplanet.com/alerts/article.php/3299981

January 15, eSecurityPlanet — Worm copies itself to network shares with weak passwords.

W32/Rirc-A is a worm that spreads by copying itself to network shares protected by weak passwords at random IP addresses, according to Sophos, which issued an alert Thursday, January 15. When first run, W32/Rirc-A copies itself to the Windows System folder and appends its pathname to the shell= line in the [Boot] section of \System.ini, so that it is run automatically each time Windows is started. On versions of Windows NT, 2000 and XP the worm also appends its pathname to the following registry entry to run itself on startup:HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell. Each time the worm runs it tries to connect to random IP addresses on port 139. The worm attempts to logon to the Administrator account of remote computers using a list of 'weak' passwords and if the schedule service is active on the remote computer the worm schedules a new job to run the worm. It also attempts to connect to a remote IRC server and join a specific channel, then sends status information to this channel. More information and instructions for removing the worm can be found at:
http://www.sophos.com/virusinfo/analyses/w32rirca.html

Category 14.2 Worms

2004-01-21 **Bagle Internet worm infect spread**

NIPC/DHS; http://www.cnn.com/2004/TECH/internet/01/19/bagle.virus.ap/index.html

January 20, Associated Press — 'Bagle' e-mail worm spreading fast.

A new Internet virus was spreading fast throughout Asia, Australia and Europe but computer security experts were divided on the seriousness of the threat from the "Bagle" worm. Experts expected some impact in the U.S. when people returned to work Tuesday, January 20, after a holiday weekend. The "Bagle" or "Beagle" worm arrives in an e-mail with the subject "hi" and the word "test" in the message body. If the accompanying attachment is executed, the worm is unleashed and tries to send itself to all e-mails listed in the user's address book. Sometimes the attachment is designed to look like a Microsoft calculator, said David Perry, spokesman for antivirus software firm Trend Micro Inc. The virus only affects machines running Microsoft Windows operating systems. The worm started spreading on Monday, January 19, and most corporations have already protected themselves against it, Perry said. Carey Nachenberg, chief architect of Symantec Research Labs, said home users, not corporations, were most at risk because companies had protected themselves quickly. "We could see this fizzle out in several days," Nachenberg said. "Or we could also see a lot of people infected" if they don't update their antivirus software.

Category 14.2 Worms

2004-01-27 **MyDoom virus worm e-mail executable spread**

NewsScan

'MYDOOM' VIRUS MAKES THE ROUNDS

A new worm is wending its way through corporate networks, masquerading as a normal e-mail message but containing malicious code that propagates itself by mass-mailing more messages at the rate of 200 per minute. It also props open a "backdoor" that leaves the infected computer vulnerable to further misuse. Symantec said the worm — dubbed "Mydoom," "Novarg" or "WORM—MIMAIL.R" — appears to contain a program that logs keystrokes on infected machines, enabling it to collect the username and passwords of unsuspecting users. Network Associates, however, disputed that assertion, saying it had not found any keylogging program. The Mydoom worm spread rapidly yesterday, with about 3,800 infections found within 45 minutes of its initial discovery. "As far as I can tell right now, it's pretty much everywhere on the planet," says Vincent Gullotto, VP of Network Associates' virus response team. The subject lines can vary, but may include phrases like "Mail Delivery System" or "Mail Transaction Failed." The attachments are generally ".exe," ".scr," ".cmd," or ".pif" files and may be compressed as a Zip file. (AP/New York Times 27 Jan 2004)

Category 14.2 Worms

2004-01-29 **worm peer-to-peer Kazaa MyDoom denial-of-service DoS**

NewsScan

MYDOOM: SAME STUPID SONG, SECOND STUPID VERSE

The e-mail worm Mydoom (also called Novarg or MiMail.r) is back now in a new variant, Mydoom b — which like its predecessor is spread through the Kazaa file-sharing network and is disguised as an e-mail error message. The message bears a variety of subject lines, text and attachment names. Mydoom.b launches a denial-of-service attack in which networks are flooded with junk traffic. The Mydoom code includes a message from its creepy author: "I'm just doing my job, nothing personal, sorry." Warning: Don't open an e-mail attachment that you haven't requested or that you have any reason to be suspicious about. (San Jose Mercury News 29 Jan 2004)

Category 14.2 Worms

2004-02-02 **MyDoom SCO worm SoBig denial-of-service DoS network Internet**

RISKS 23 17

MYDOOM AND SCO

Contributor Steve Wildstrom writes about the effects of worm MyDoom's denial-of-service attack on SCO's Website in February 2004. He thinks MyDoom had little impact "on the performance of the Internet as a whole." He says that sco.com was not available for the most part starting from Wednesday, January 28. Because of the worm, SCO had to move its Website to www.thescogroup.com. Wilstrom says that judging from the way they handled MyDoom, network administrator were getting better at mitigating worm attacks. In another article about MyDoom, contributor Chris Smith discusses why the worm affected his e-mail account badly. The week of January 26, 2004, Smith received over 30,000 e-mail due to MyDoom. This was about 1000MB worth of messages. He thinks he was so badly hit because he has the popular last name 'Smith', but refuses to believe that his own name is a security risk. Smith thinks MyDoom could have been stopped by the "[I]mplementation of something like Sender Permitted From (SPF)" information in e-mails.

Category 14.2 Worms

2004-02-03 **Microsoft MyDoom DoS denial of service worm network attack**

DHS IAIP Daily;
http://story.news.yahoo.com/news?tmpl=story&cid=569&ncid=738&e=1&u=/nm/20040203/tc_nm/tech_microsoft_dc

February 03, Reuters — Microsoft site appears to weather MyDoom attack.

Microsoft Corp. appeared to have survived the worst the MyDoom worm could throw at it Tuesday. Experts say the virus, a variant of the myDoom.A virus that knocked out another company's Website Sunday, was programmed to fire continuous volleys of debilitating data at Microsoft's site Tuesday. But there was no visible impact on the software company's Web site, which barely flickered as the MyDoom.B Internet worm's trigger time of 8:09 EST passed. MyDoom.B is a low-grade variant of the original MyDoom.A virus, the fastest-spreading e-mail contagion to ever hit the Internet. MyDoom.A has infected hundreds of thousands, and possibly over one million, PCs, generating a torrent of spam e-mails and crippling corporate e-mail servers, plus slowing traffic for some Internet service providers.

Category 14.2 Worms

2004-02-09 **worm virus network attack Microsoft MyDoom variant**

NewsScan

'DOOMJUICE' SQUEEZES MICROSOFT

A new worm dubbed "Doomjuice," which some are describing as a variant of the earlier MyDoom worm, is piggybacking on the damage already done by its predecessor by targeting already-infected computers. "It's only looking for machines that are compromised by MyDoom A or B," says Vincent Gullotto, VP of the antivirus emergency response team at Network Associates. Its ultimate target is Microsoft's Web site, which it seeks to overwhelm with distributed denial of service attacks. Microsoft said its Web site is still up and running but the company has offered a $250,000 bounty for information leading to the capture of MyDoom's author. (Reuters 9 Feb 2004)

Category 14.2 Worms

2004-02-25 **worm damage destructive file deletion**

http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci952225,00.html?track=NL-102

Yet another Mydoom worm has hit. The new variant targets the Web sites of eternal whipping boy Microsoft and song-swapper foe Recording Industry Association of America.

Mydoom-F works in a way very similar to Mydoom-A — so much so that experts think the creator of Mydoom-F used the source code of the Mydoom-A to create it. The code for Mydoom-A is widely available because Mydoom-B dropped the source code for A on victims' computers.

Mydoom-F does something different than its predecessors. The worm randomly deletes files such as Excel spreadsheets and pictures. This is the first time in recent memory that a worm has been so randomly destructive.

Category 14.2 Worms

2004-02-26 **Netsky worm UK email vector F-Secure propagation**

DHS IAIP Daily; http://www.vnunet.com/News/1153081

February 26, Vnunet.com — Security vendor mass-mails worm to clients.

Antivirus firm F-Secure has apologized for sending the Netsky.B virus to several thousand of its UK customers and partners via a mailing list. The e-mail apology said: "Because of a human error, you may have received an email infected with the Netsky.B virus that was relayed through our external email list server and was resent to our UK mailing list. The virus did not originate from our network -- it was sent by an unknown party to the list address. If you had up-to-date antivirus installed, the virus has been stopped automatically already and no further steps are necessary on your part." Mikko Hypponen, F-Secure's director of antivirus research, said the mailing list was outside of the firm's normal e-mail scanning. The Netsky.B worm spreads itself in e-mails inside a .zip archive or as an executable attachment. It also copies itself to shared folders of all available drives. This allows the worm to spread through peer-to-peer and local networks.

Category 14.2 *Worms*

2004-03-04 **worm network attach Bagle variant Netsky e-mail**

NIPC/DHS

March 03, eWEEK — Tenth variant of Bagle worm hits the Net.

Anti-virus researchers discovered the existence of Bagle.J, the tenth variant of the worm to hit the Internet, late Tuesday, March 2. Officials at Network Associates Inc. have rated the worm as a medium risk and said they saw 50 unique samples of Bagle.J in a 90-minute period. Bagle.I also surfaced Tuesday, with Bagle.H appearing Monday. Recent speculation among anti-virus researchers that the creators of the NetSky and Bagle viruses may be engaged in some kind of competition or war has now apparently been proven true. The virus writers have been leaving profane, derogatory messages for one another in the new variants of their respective viruses during the last few days, experts say. Like its predecessors, this version relies heavily on social engineering to entice recipients into opening the e-mail and infected attachment.

Category 14.2 *Worms*

2004-03-08 **worm network Sober.D SMTP engine masquerading Microsoft update e-mail attachment executable**

NewsScan

NEW WORM MASQUERADES AS MS UPDATE

The latest variation on the Sober worm — Sober.D — tries to trick recipients into opening it by disguising itself as a Microsoft Update message. "It arrives in an e-mail that pretends to be a patch to protect against a version of MyDoom," says a senior consultant at antivirus firm Sophos. "The e-mail appears to be a Microsoft patch so people will of course double-click on that attachment." Once a user clicks on the file, the worm scans the PC to see if it's already infected — if not, it installs itself and uses its own SMTP engine to send copies of itself to e-mail addresses found on the victim's PC. Microsoft emphasizes that it does not send patches via e-mail and that users should ignore such messages. (ZDNet 8 Mar 2004)

Category 14.2 *Worms*

2004-03-15 **Internet worm network password trick foil filters Bagle**

NewsScan

LATEST E-MAIL WORMS USE PASSWORD TRICK TO FOIL FILTERS

The most recent versions of the pesky Bagle worm — Bagle N and Bagle O — arrive in a compressed and password-locked .zip or .rar file with the password included in the body of the e-mail along with a message urging the recipient to open it right away. This latest technique is designed to foil corporate e-mail filters that may block ordinary zipped attachments but allow password-protected documents to pass through the network's defenses unimpeded. Once the attachment is unlocked, the worm is then forwarded to everyone in the victim's e-mail address book. "The worm's author is sneakily trying to make it more difficult for antivirus products to scan inside the password-protected files," says Graham Cluley, a researcher with U.K cybersecurity firm Sophos. (New Scientist 15 Mar 2004)

Category 14.2 *Worms*

2004-03-16 **worm network attack defense failure Bagle variant ZIP**

NIPC/DHS

March 15, TechWeb News — New Bagle worm variants sneak past defenses.

Two new versions of the Bagle worm, Bagle.n and Bagle.o, were spotted over the weekend. Unlike earlier editions of Bagle, which tried to circumvent anti-virus software by placing the worm payload into an encrypted .zip archive, the new Bagles may also use a different archive format, .rar, a file type that consumers are unfamiliar with and enterprises may not block at the gateway. Additionally, Bagle.n and Bagle.o include the password to the .rar and .zip files in the message not as text, but as an embedded graphic, a tactic often used to discourage automated e-mail account creation by spammers or by Websites to prevent spam bots from harvesting e-mail addresses. When Bagle first turned to encrypted .zip files to disguise its payloads, anti-virus firms reacted by scanning the message for the in-text password. Shifting to an image of the password may make it tougher for anti-virus programs to unlock the .rar file. The new Bagles randomly attach their code to 32-bit executables on the infected machine's hard drive and then re-infect a supposedly cleaned system once the executable runs.

Category 14.2 *Worms*

2004-03-19 **worm network Internet Bagle Outlook flaw exploit**

NIPC/DHS

March 18, ZDNet UK — Bagle uses Outlook flaw to speed replication.

Until the appearance of Bagle variants Q, R and S, users had to click on an e-mailed attachment to be infected by the worm. The latest Bagle incarnation has done away with the attachment altogether and spreads when a vulnerable user opens the email using an unpatched version of Microsoft Outlook. If their Outlook preview pane is open, the victim's machine will be compromised automatically. Graham Cluley of Sophos said: "This has the potential to spread very quickly because so many people, particularly home users, have not applied the patches." Mikko Hyppönen of F-Secure said that the latest variant uses a list of about 600 IP addresses, which all seem to be home computers connected to an ADSL service that have been infected by previous versions of Bagle. These "zombie" machines have been updated and are now used to send copies of the new worm to any computer on which the victim uses a vulnerable copy of Outlook to view an infected email message. Outlook uses elements of Internet Explorer to render the HTML for its preview pane, so to avoid the new Bagle worms, users should apply a patch for Internet Explorer that Microsoft released in October 2003.

Category 14.2 *Worms*

2004-03-22 **worm network attack security vulnerability flaw exploit firewall BlackIce RealSecure denial-of-service hard disk**

NIPC/DHS

March 20, Washington Post — 'Witty' worm wrecks computers.

A quickly spreading Internet worm exploited a security flaw in a firewall program designed to protect PCs from online threats on Saturday, March 20, computer experts said. The "Witty" worm writes random data onto the hard drives of computers equipped with the Black Ice and Real Secure Internet firewall products, causing the drives to fail and making it impossible to restart the PCs. Unlike many recent worms that arrive as e-mail attachments, it spreads automatically to vulnerable computers without any action on the part of the user. At least 50,000 computers have been infected so far, according to computer security firm iDefense and the SANS Institute. Most infected computers will have to be rebuilt from scratch unless their owners instead decide to buy new ones, said Ken Dunham of iDefense. Joe Stewart of security services company Lurhq said he expects the worm to die out over the next few hours as vulnerable computers quickly become useless hosts. A patch is available the deveoper of the firewalls, Internet Security Systems:
http://xforce.iss.net/xforce/alerts/id/167

Category 14.2 *Worms*

2004-03-23 **worm network Internet Netsky variant security vulnerability flaw hole exploit**

NIPC/DHS

March 22, eWEEK — Netsky.P spreads through ancient security hole.

A new variant of the Netsky worm, Netsky.P, is spreading quickly. This new variant is very much like other Netsky versions with two differences, according to Vincent Gullotto of the McAfee Avert Virus and Vulnerability Emergency Response Team. The initial seating of the worm, referring to the initial group of users to whom the virus author distributed it, appears to have been in Australia. It's not clear whether or how this would facilitate spreading of the worm, but it is unusual. The other unusual characteristic of this worm is that it utilizes a very old vulnerability in Internet Explorer, the Incorrect MIME Header (MS01-020) bug. This bug, patched almost three years ago, allowed a hostile HTML e-mail to execute arbitrary code if viewed in the preview pane of a mail client. Like other Netsky variants, this one spreads mainly through a built-in SMTP engine to e-mail addresses harvested out of the user's files.

Category 14.2 Worms

2004-03-29 **worm network Internet Bagle variant e-mail TCP**

NIPC/DHS

March 26, eWEEK — New spawn of Bagle worm unleashed.

Yet another version of the Bagle worm is on the loose and is already causing trouble in parts of Europe. Bagle.U appeared early Friday, March 26, and has begun spreading quickly, even though it contains none of the social engineering tricks that Bagle's author has used to help previous versions succeed. This variant arrives in an e-mail with a blank subject line and no body text. The sending address, as always, is spoofed, and the name of the infected executable attachment is completely random. After execution, the worm mails itself to all of the addresses in the infected machine's address book. Bagle.U does include a backdoor component that listens on TCP port 4751 and connects to a Web server in a German domain, www.werde.de, according to Network Associates Inc. Once it establishes a connection with the remote server, the worm generates a unique ID number for each specific infected machine and sends that number and the number of the port on which it is listening to the server. Bagle.U is set to expire on January 1, 2005.

Category 14.2 Worms

2004-03-31 **worm network Internet NetSky mass-mailing e-mail**

NIPC/DHS

March 29, CNET News — NetSky variant a greater threat than thought.

Security company Symantec raised its severity rating of the latest incarnation of the NetSky worm. NetSky.Q was upgraded from a level 2 to level 3 threat on the security firm's five-point rating system. The company said it has received 379 reports of the worm since its discovery Sunday, March 28. NetSky is a mass-mailing worm that uses a bogus sender address and continually changes its subject line and content. An e-mail attachment usually carries an .exe, .pif, .scr or .zip file extension. The worm distributes itself to e-mail addresses in a victim's hard drive and copies itself into shared folders via file-sharing programs. NetSky.Q is expected to release a denial-of-service attack between April 8 and April 11 on several Websites, including those of eDonkey2000, Kazaa, eMule, Cracks.am and Cracks.st, according to Symantec.

Category 14.2 Worms

2004-04-08 **worm virus network Netsky e-mail**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/virus/story/0,10801,91978,00.html

April 08, IDG News Service — New Netsky worms change their stripes.

New versions of the Netsky e-mail worm are spreading on the Internet. Netsky.S appeared Monday, April 5, and Netsky.T was detected Tuesday, April 6. They are the 19th and 20th editions of an e-mail virus that first appeared in February. Like its predecessors, the new Netsky variants target machines running versions of Microsoft's Windows operating system. The viruses arrive as files enclosed in e-mail messages that have faked (or "spoofed") sender addresses and vague subjects such as "Re: My details," "Request" and "Thank You!" according to anti-virus company Symantec Corp. Earlier versions of the Netsky variant abstained from opening communications ports that could be used as back doors that remote attackers could use to gain access to compromised systems. However, the latest Netsky variants open a back door on TCP Port 6789 that could be used to receive instructions or malicious code from the worm author.

Category 14.2 Worms

2004-04-28 **Netsky worm Website Internet denial-of-service Bagle education Windows registry**

DHS IAIP Daily; http://www.techweb.com/wire/story/TWB20040428S0006

April 28, TechWeb — Netsky.x lays out Websites.

The Netsky.x worm, which hit the Internet over a week ago and targeted a trio of educational Websites for denial-of-service (DoS) attacks, has laid low two of the three in the first day of its scheduled three-day assault. Version X of the persistent Netsky worm launched a DoS attack on nibis.de, medinfo.ufl.edu, and educa.ch, educational sites from Germany, the United States, and Switzerland, respectively. The DoS attacks, which began Wednesday, April 28, by Netsky.x-infected computers, and is to run through Friday, effectively shut down the German and U.S. sites, according to Ken Godskind of AlertSite, a Web monitoring firm. Other variants released after Netsky.x--including Netsky.y and Netsky.z--also targeted the three sites for DoS attacks that could run as long as May 5. The two most recent Netskys, however, dubbed Netsky.aa and Netsky.ab -- which appeared Monday and today, respectively, don't take aim at the educational sites. Instead, Netsky.ab tries to delete the entries of several variations of its rival, Bagle, from the Windows Registry.

Category 14.2 Worms

2004-05-02 **worm virus malicious code malware Microsoft Windows vulnerability Sasser**

DHS IAIP Daily;
http://www.computerworld.com/securitytopics/security/virus/story/0,10801,92851,00.html?SKC=news92851

May 02, Computerworld — Worm unleashed that exploits latest Windows security holes, Microsoft warns.

Microsoft Corp. issued an unusual weekend security warning Saturday that a worm has been unleashed on the Internet taking advantage of a security hole announced publicly last month. Microsoft once again urged users to install its most recent critical Windows updates. "Microsoft has verified that the worm exploits the Local Security Authority Subsystem Service (LSASS) issue addressed in Microsoft Security Update MS04-011 on April 13, 2004," the company said in an announcement posted yesterday and updated 3 a.m. PDT this morning, May 2. In its security update, Microsoft included a tool that checks for system infection by the Sasser worm. Versions of Windows XP and 2000 are vulnerable, although not XP 64-Bit Edition Version 2003, Microsoft said. Both Symantec Corp. and Network Associates Inc.'s McAfee antivirus unit currently rate Sasser as medium risk, while Computer Associates rates it low risk. Trend Micro Inc. says it issued a yellow alert to its customers. For further information: http://www.microsoft.com/security/incident/sasser.asp

---

Category 14.2 Worms

2004-05-03 **worm virus malicious code malware Microsoft Windows vulnerability Sasser**

DHS IAIP Daily;
http://www.reuters.com/newsArticle.jhtml?type=internetNews&storyID=5016252&section=news

May 03, Reuters — Sasser worm strikes hundreds of thousands of PCs.

The fast-spreading "Sasser" computer worm has infected hundreds of thousands of PCs globally and the number could soon rise sharply, a top computer security official said on Monday, May 3. "If you take a normal Windows PC and connect to the Internet, you will be infected in 10 minutes without protection," said Mikko Hypponen, Anti-Virus Research Director at Finnish data security firm F-Secure. F-Secure says the worm, which surfaced at the weekend, automatically spreads via the Internet to computers using the Microsoft Windows operating system, especially Windows 2000 and XP. "We have already seen three versions of Sasser during the weekend, and we could see more today," Hypponen said. The current worm does not need to be activated by double-clicking on an attachment, and can strike even if no one is using the PC at the time. When a machine is infected, error messages may appear and the computer may reboot repeatedly.

Category 14.2 Worms

2004-05-03 **worm virus malicious code malware Microsoft Windows vulnerability Sasser**

DHS IAIP Daily;
http://story.news.yahoo.com/news?tmpl=story&cid=1510&ncid=1510&e=2&u=/afp/20040503/tc_afp/internet_virus_taiwan_040503133241

May 03, Agence France Presse — Taiwan's post office hit by worm.

The new Internet worm, Sasser, that is disrupting computers across the world paralyzed a third of the offices of Taiwan's national post office. Some 1,600 work stations at 430 Chunghwa Post Co. offices, 300 of them in the greater Taipei area, were shut down by the virus Monday, May 3. "We started to receive complaints from offices at around 10:00 am saying their computers kept shutting down and rebooting automatically," a company official told Agence France Presse. "Subsequently manual processes had to be initiated while computer systems were down," the official said. The company said the computer virus had not damaged its computer systems and it expected the virus to be removed by 10:00 pm.

Category 14.2 Worms

2004-05-03 **worm virus malicious code Finland bank Sasser infection denial of service DoS**

DHS IAIP Daily;
http://www.heraldsun.news.com.au/common/story_page/0,5478,94
60659%255E1702,00.html

May 03, Agence France-Presse — Bank closes to ward off virus.

Sampo, Finland's third largest bank, closed its 130 branch offices across the country on Monday, May 3, to prevent the Sasser Internet worm from infecting its systems, officials said. The Sasser bug has so far contaminated millions of computers worldwide, making them shut down and restart in an endless loop. "We decided to close our offices as a precaution, since we knew that our virus protection hadn't been updated," Sampo spokesman Hannu Vuola said. Sampo is Finland's third largest bank with over a million customers nationwide. Its corporate and Internet banking 3 services were not affected by the shutdown, Vuola said.

Category 14.2 Worms

2004-05-03 **worm virus malicious code malware Microsoft Windows vulnerability Sasser Netsky**

DHS IAIP Daily; http://www.esecurityplanet.com/alerts/article.php/3348571

May 03, eSecurityPlanet — Mass-mailing worm copies itself to Windows folder.

Security vendors Monday, May 3, issued an alert for W32/Netsky-AC, a mass mailing worm that copies itself to the Windows folder as comp.cpl and creates a helper component wserver.exe in the same folder. W32/Netsky-AC sets the following registry entry to ensure it is run on user logon: HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ wserver = wserver.exe. Trend Micro also issued an alert for Worm_Netsky.AC, and reports that this memory-resident worm propagates using its own Simple Mail Transfer Protocol (SMTP) engine. It obtains target email addresses from files with certain extension names, which it searches in drives C to Z (except for CD-ROM drives).

Category 14.2 Worms

2004-05-03 **worm virus malicious code malware Microsoft Windows vulnerability Sasser Netsky link**

DHS IAIP Daily; http://www.pcworld.com/news/article/0,aid,115964,00.asp

May 03, IDG News Service — Experts probe Sasser, Netsky link.

Analysis of the Sasser and Netsky code reveals many similarities between the two worms, even as a new version of the Netsky e-mail worm appeared on Monday, May 3, that capitalized on fears caused by Sasser Internet worms by posing as an antivirus software patch, experts say. Netsky-AC is the thirtieth version of the mass-mailing e-mail worm to be released since Netsky-A appeared in February. Like earlier versions of Netsky, the AC-variant uses e-mail messages and infected file attachments to spread from computer to computer. A message buried in the worm's code and directed to antivirus vendors claims responsibility for Sasser, which first appeared on Friday, April 30. "Hey av firms, do you know that we have programmed the sasser virus?!? Yeah, thats true," the message reads, in part. The message is attributed to "the Skynet," a virus writing group that also claimed responsibility for other Netsky variants. The worm's author or authors included a sample of the Sasser worm raw "source" code as proof of the legitimacy of the claim, says Graham Cluley, senior technology consultant at Sophos.

Category 14.2 Worms

2004-05-03 **Sasser worm train outage Australia RailCorp virus attack**

NewsScan

SASSER EYED OVER TRAIN OUTAGE

In Australia, RailCorp has dispatched software engineers to find the source of the outage that left up to 300,000 commuters stranded yesterday, saying the new Sasser worm, which has already spawned two variants, is being evaluated as a possible cause. A RailCorp spokesman confirmed that software engineers were investigating the problem, which prevented drivers from talking to signal boxes. A virus attack was one possibility being investigated. RailCorp was unable to confirm when the investigation would be complete. RailCorp chief executive Vince Graham raised the possibility of a virus attack at a press briefing yesterday: "There is no evidence that hacking is an issue here, the viral infection could have been introduced by one of our own people not taking sufficient care." (The Australian 3 May 2004)

Category 14.2 Worms

2004-05-03 **sasser worm F-Secure reboot computers new areas windows Mikko Hypponen threat**

NewsScan

SASSER WORM IS LATEST THREAT

A fast spreading worm known as "Sasser" surfaced over the weekend and is making its way around the globe, warn computer security experts at Finland's F-Secure. The worm shares many characteristics with the Blaster worm that infected hundreds of thousands of PCs last year, says F-Secure antivirus research director Mikko Hypponen, who notes that both worms exploit relatively new holes in the Windows operating system and frequently cause computers to repeatedly reboot. However, this time more companies appear to be ready to take preventative action, which may mitigate Sasser's damage potential. "With Sasser it seems that companies are (using software) patches better and more quickly than last year (with Blaster), but for those that are hit, they are hit hard," says Hypponen, who adds that he believes Sasser originated in Russia. The worm does not need to be activated by double-clicking on an attachment and can strike even if no one is using the PC at the time. (Reuters/Washington Post 3 May 2004)

Category 14.2 Worms

2004-05-04 **worm virus malicious code malware Microsoft Windows vulnerability Sasser**

DHS IAIP Daily;
http://www.theadvertiser.news.com.au/common/story_page/0,593
6,9462787%255E421,00.html

May 04, The Australian — Red alert as web worm hits banking.

Staff at Australian banking giant Westpac were forced to revert to pen and paper yesterday as an internet-based computer virus struck Australia and threatened to cause further chaos in the U.S. overnight. Unlike many other viruses, Sasser does not travel by e-mail or attachments and can spread by itself to any unprotected computer linked to the internet. It attacks through a flaw in recent versions of Microsoft's Windows -- Windows 2000, Windows Server 2003 and Windows XP- - and causes the computer to shut down, before rebooting it and repeating the process several times. While it slows down computers, it is not believed to cause long-term damage to the hard drive. Internet security company Trend Micro on Monday, May 3, upgraded Sasser to a "red alert" -- its highest warning level. Westpac confirmed Monday it was investigating network problems caused by Sasser. Branches had switched to pen and paper manual systems to allow them to keep trading, but the bank's ATM and internet banking networks were not hit, spokesperson Julia Quinn said. The bank expected the problem to be resolved and all systems available at the start of business Tuesday, May 4, she said.

Category 14.2 Worms

2004-05-04 **worm IP addresses Windows patch**

http://www.nytimes.com/2004/05/04/business/04worm.html?th=&pagewanted=
print&position=

The Sasser worm hit the world on April 30, 2004.

The worm spreads through the Internet without user intervention by exploiting a vulnerability in Windows 2000 and Windows XP that had a patch issued by Microsoft on April 12. In addition, "W32.Sasser.Worm can run on (but not infect) Windows 95/98/Me computers. Although these operating systems cannot be infected, they can still be used to infect the vulnerable systems to which they are able to connect." [Symantec Security Response]

Category 14.2 Worms

2004-05-04 **computers invaded sasser worm half million PC infect windows**

NewsScan

AT LEAST A HALF MILLION COMPUTERS INVADED

The new computer worm called Sasser has already infected hundreds of thousands of computers and caused some networks to crash continually. The worm automatically scans Internet addresses in an infected computer to find another vulnerable PC it can infect. The Microsoft site has a software patch that Windows users should download and install. (New York Times 4 May 2004)

Category 14.2 Worms

2004-05-05 **worm virus malicious code malware Microsoft Windows vulnerability Sasser Netsky**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily-updates/25838-1.html

May 05, Government Computer News — Sasser worms slowing the Internet.

The Sasser family of worms appears to be slowing down Internet traffic and making some destinations unavailable, according to observations by Keynote Systems Inc., a Web performance management company. "Reachability has crept down and we saw a spike in that at 8 p.m. Eastern Time, Tuesday, May 4, accompanied by an upward spike in packet loss," said Kirsten Husak, a consulting manager in the San Mateo, CA, company's professional services division. "It is definitely more than normal Internet variability." But the worms' impact is not as severe as some past outbreaks, such as last year's Slammer. "This doesn't seem to be affecting Web sites nearly as much." Sasser, which exploits a Microsoft vulnerability announced with the release of a patch in mid-April, first appeared May 1, and began spreading rapidly. It is believed to be the first self-executing worm and does not require any recipient action to propagate. It instructs vulnerable systems to download and execute the viral code. By May 3, four variants of the worm were in the wild, and thousands of computers had been infected. The number of infected computers has since been estimated at more than one million.

Category 14.2 Worms

2004-05-05 **worm virus malicious code malware Microsoft Windows vulnerability Sasser Netsky**

DHS IAIP Daily;
http://www.cnn.com/2004/TECH/internet/05/05/sasser.worm.reut /index.html

May 05, Reuters — Hunt on for Sasser worm culprit.

Security experts began the daunting task on Wednesday, May 5, of trying to track down the authors of "Sasser," a tenacious computer worm expected to infect millions of machines before it runs its course. Home users, corporations, and government agencies throughout Europe, North America and Asia have been hit. Once infected, the vulnerable PC reboots without warning as the compact program hunts for more machines to infiltrate. Microsoft (MSFT.O) said on Wednesday it had not made a decision to issue a reward for information leading to the arrest of the Sasser author. Over the past six months, the software giant has offered three separate $250,000 rewards for previous outbreaks -- so far, with no results. Microsoft said it is working with U.S. law enforcement authorities, including the Federal Bureau of Investigation, to flush out the culprits.

Category 14.2 Worms

2004-05-05 **sasser creator authorities U.K. teaming up security experts Netsky**

NewsScan

AUTHORITIES TEAM UP ON HUNT FOR SASSER CREATOR

Security experts in the U.K. are teaming up with U.S. law enforcement officials to track down the author or authors of the Sasser worm and are investigating the theory that the creator is part of a Russian group calling itself the "Skynet antivirus group," which also was responsible for the Netsky e-mail virus outbreak. A message found in the code of a recent Netsky variant claimed responsibility for Sasser, but the reasoning behind this latest Internet assault is still murky. "With Sasser, the author seems to be showing off his coding capabilities, but otherwise I have no idea what the motive is," says Raimund Genes, European president of antivirus group Trend Micro. And while Microsoft has yet to decide whether to offer a reward for information leading to culprit, most experts agree if the originators are linked to criminal groups, a bounty offer will have little effect. "If the person doesn't disclose his identity, we will never know the author of this worm or the author of those worms that have caused global epidemics in the past," says Eugene Kaspersky, co-founder of Moscow's Kaspersky Labs. Over the past six months, Microsoft has offered three separate $250,000 rewards for previous outbreaks, but with no results. (Reuters/Washington Post 5 May 2004)

Category 14.2 Worms

2004-05-06 **worm virus malicious code malware Microsoft Windows vulnerability Sasser**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/virus/story/0,10801,92936,00.html

May 06, Reuters — Security experts warn of nastier Sasser worm.

Computer security experts warned Wednesday, May 5, that the Sasser worm could merge with earlier viruslike programs to wreak more havoc on the Internet. Since appearing over the weekend, the fast-moving Sasser computer worm has hit PC users around the world who run the ubiquitous Microsoft Windows 2000, NT and XP operating systems. It is expected to slow down as computer users download antivirus patches. But Sasser could mutate by combining with the 2-month-old Netsky worm and become a launching pad for further Web attacks, putting it on par with Blaster, the destructive worm that appeared last year and used infected computers to attack Microsoft Corp.'s Web site. "My expectation is that Netsky and Sasser variants will merge and become what we call one 'abundant threat' that attacks through e-mail and software vulnerabilities," said Jimmy Kuo, a research fellow at Network Associates Inc.'s McAfee antivirus unit.

Category 14.2 Worms

2004-05-10 **worm virus malicious code malware Microsoft Windows vulnerability Sasser**

DHS IAIP Daily;
http://www.cnn.com/2004/TECH/internet/05/10/computer.worm.ap/index.html

May 10, Associated Press — New Sasser worm may be circulating.

An 18-year-old German who confessed to creating the "Sasser" computer worm apparently released a new version of the program shortly before he was arrested last week, investigators said Monday, May 10. German investigators said Microsoft had reported some computer users were having problems with "Sasser e," a variation of the original worm. Frank Federau, a spokesperson for the state criminal office in Hanover, said the worm was "a slightly modified form" of the program that raced around the world over the past week, exploiting a flaw in Microsoft's Windows operating system. The suspect likely programmed it "immediately before his discovery," he said. Four versions of Sasser were already known. Police have said the German teenager was responsible for all of them in addition to the "Netsky" virus. The teenager has told officials that his original intention was to create a virus, "Netsky A," that would combat the "Mydoom" and "Bagle" viruses, removing them from infected computers. During that effort, he developed the Netsky virus further -- and after modifying it created Sasser.

Category 14.2 Worms

2004-05-11 **worm virus malicious code malware Microsoft Windows vulnerability lsass**

DHS IAIP Daily; http://www.esecurityplanet.com/alerts/article.php/3352151

May 11, eSecurity Planet — New worm mimics Sasser, exploits LSASS vulnerability.

The arrest of the alleged creator of the Sasser worms has not been accompanied by a lull in the momentum of computer viruses. Panda Labs has detected the appearance of a new worm, Cycle.A W32/Cycle.A.worm, which, like Sasser and its variants, exploits the LSASS vulnerability affecting some Windows versions in order to infect computers through the Internet. The scenario has changed, however, as indicated by the text found inside the virus code. In this text, the virus creator -- alias Cyclone -- claims to be Iranian and refers to the social and political situation in his country. Cycle.A tries to enter computers through communications port TCP45 in order to check if the system is vulnerable. If it is, the worm causes the affected computer to download a copy of itself called CYCLONE.EXE. However, this will only take place if the application TFTP.EXE is installed on the system. Additionally, and regardless of whether the worm has managed to copy itself to the targeted computer, the attempt by the virus to enter the system causes a failure in the application LSASS.EXE which makes the computer restart every 60 seconds. Users should install the Microsoft patch available from: http://www.microsoft.com/technet/security/bulletin/MS04-011. mspx.

Category 14.2 Worms

2004-05-12 **worm virus malicious code malware Microsoft Windows vulnerability Sasser German police raid**

DHS IAIP Daily;
http://story.news.yahoo.com/news?tmpl=story&ncid=1212&e=6&u=
/afp/20040512/tc_afp/internet_virus_germany&sid=96001018

May 12, Agence France-Presse — German police raid homes in Sasser computer worm probe.

German police have raided the homes of five people who had been in contact with a teenager arrested last week on suspicion of creating the Sasser computer worm, police spokesman Detlef Ehrike said. Investigators "suspect that other people took part in spreading the worm. The Verden prosecutors office ordered raids in the Rotenburg an der Wuemme region," Ehrike said. The 18-year-old German, whom police have not identified by name, was arrested Friday, May 7, after a raid on his parents' house turned up incriminating evidence. Acting on a tip off from computer giant Microsoft, investigators seized several items from the house, including the teen's personal computer. He faces up to five years in prison for "computer sabotage" if found guilty of creating and spreading the computer worm. The Sasser worm struck on May 1, and in less than a week affected thousands of companies and as many as 18 million computers worldwide, forcing some businesses to shut temporarily in order to debug their systems. The teenager is also suspected of creating Netsky.ac; a worm that also spread across the Internet early last week. "Two suspects have admitted receiving from the author of Sasser the source code for the Netsky worm," Ehrike said, adding that one of them had admitted to "taking part in spreading the Netsky worm."

Category 14.2 Worms

2004-05-17 **worm virus malicious code malware Microsoft Windows vulnerability Sasser Dabber "good" worm**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/virus/s
tory/0,10801,93154,00.html

May 17, IDG News Service — New worm targets Sasser code flaw.

A new Internet worm called Dabber is believed to be the first worm that spreads by specifically targeting a flaw in another worm's code, according to LURHQ Corp., a managed security services company. Using code written to exploit the FTP flaw, the recently released worm scans the Internet for Port 5554 to identify computers running Microsoft Corp.'s Windows operating system that are infected with Sasser, LURHQ said. When it finds vulnerable hosts, it connects to the victim and uses a built-in FTP server to transfer the worm file, named package.exe, to the system. When it runs, the Dabber worm installs itself on Windows and then shuts down the Sasser worm and other worm processes, preventing them from running again. Dabber also opens TCP Port 9898 as a back door, which can be used by a remote attacker to download other code or communicate with the infected host, LURHQ said. The original advisory and insturctions for shutting down and removing Dabber are available here: http://www.lurhq.com/dabber.html

---

Category 14.2 Worms

2004-05-17 **worm vulnerability IRC chat worm krisworm**

DHS IAIP Daily; http://www.esecurityplanet.com/alerts/article.php/3354731

May 17, eSecurity Planet — Worm acts with MIRC client to allow remote access.

IRC/Krisworm-C is a worm used in conjunction with a MIRC client to allow remote access to the host computer, according to Sophos, which issued an alert Monday, May 17. It has the same characteristics as W32/Krisworm-A, a worm that spreads by targeting computers with weak administrator and user passwords. The worm installs several files in the fonts subfolder of the Windows fonts folder, and also attempts to propagate via peer-to-peer (P2P) file-sharing networks. It can also propagate via IRC and via newsgroups. It terminates running antivirus and firewall software. It runs on Windows 95, 98, ME, NT, 2000, and XP. More information at: http://www.sophos.com/virusinfo/analyses/irckriswormc.html

---

Category 14.2 Worms

2004-06-03 **Harry Potter game masquerading worm virus Internet Sophos**

NewsScan

POTTER-MANIA FUELS NETSKY.P WORM

The popularity of the latest Harry Potter film, which debuted in Britain Monday, is spurring the resurgence of the Netsky.P worm, which is now disguising itself as a Potter game, warn antivirus experts. Computer security firm Sophos says it has spotted thousands of copies in the last few days. "Echoing a technique used in 2000 by the Pikachu worm, Netsky.P targets young computer users by sometimes posing as content connected with the Harry Potter books and movie franchise," says Sophos senior tech consultant Graham Cluley. "Parents need to educate their children against the threats of viruses, to ensure the popularity of Potter doesn't cast a nasty spell on their computer systems." (BBC News 3 Jun 2004)

Category 14.2 Worms

2004-08-03 **MyDoom variant Yahoo People Search Internet proliferation SANS report**

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1630964,00.asp

August 03, eWEEK — New MyDoom variant uses Yahoo People Search.

Another new version of MyDoom is worming its way through the Internet. MyDoom.P arrives via e-mail, with a spoofed sending address and a subject line designed to make it look like the message is related to one that the recipient sent. The body of the e-mail contains any of a number of sentences, some of which refer to the included Zip file. Once opened, the executable file copies itself to the Windows system directory as "winlibs.exe." The executable contains a list of dozens of common first and surnames that it puts through Yahoo's People Search in an attempt to find more e-mail addresses to mail itself to, according to the Internet Storm Center at The SANS Institute. Researchers on Monday discovered a new version of the Gaobot worm, which spreads through the back doors installed by MyDoom variants, among other avenues of infection. Gaobot.BAJ connects to an IRC server on port 6667 and waits for instructions from the attacker. It then begins scanning the local network for machines sharing resources with the infected PC and tries to copy itself to those machines. Afterward, it begins scanning for PCs infected with any of the MyDoom worms and attempts to install itself through the back door these worms place on infected computers.

Category 14.2 Worms

2004-08-09 **Bagle worm variant ZIP file Trojan creation viral download**

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1633739,00.asp

August 09, eWEEK — Bagle variant exacts a 'price' with infected zip files.

Another variant of the Bagle worm began making its way across the Internet on Monday, August 9. Bagle.AQ arrives via an e-mail message with a spoofed sending address and no subject line. The only text in the message body is typically one or two words, either "price" or "new price." The name of the infected Zip file that accompanies the message is some variation on that theme as well. The files often are named Price.zip or New_price.zip, and may have a number appended to the end of the file name. Some users reported getting as many as 100 infected messages in an hour. If a user opens the Zip file with an application such as Windows Internet 13 Explorer that is not a standalone Zip file handler, the user will see an HTML file that contains exploit code. The file will then execute an included .exe file, which is a Trojan, according to McAfee Inc.'s analysis. The Trojan then connects to a number of remote sites to download the actual viral code. Because it can inject itself into the Explorer process space, the worm's outgoing traffic will appear legitimate to most firewalls.

Category 14.2 Worms

2004-08-12 **MS Blaster virus worm network creator writer teenager guilty plead Minnesota**

NewsScan

TEEN PLEADS GUILTY OVER BLASTER

A Minnesota teenager has pleaded guilty to creating and spreading a variant of the MS Blaster virus that wreaked havoc on thousands of computers around the world last year. He now faces between 18 months and three years in jail and could be ordered to pay millions of dollars in restitution for the damage. (The Australian 12 Aug 2004) Rec'd from J. Lamp

---

Category 14.2 *Worms*

2004-08-16 **MyDoom worm variant e-mail spread executable file photo Trojan Horse Internet download**

DHS IAIP Daily; http://www.theregister.co.uk/2004/08/16/mydoom_spam/

August 16, The Register — Infected PCs spew MyDoom variant.

The MyDoom worm saga continued Monday, August 16, with the release of yet another variant of the e-mail worm. The latest variant -- MyDoom-S (AKA MyDoom-Q or MyDoom-R) -- poses as a funny photographs in order to dupe users into opening an infectious attachment called photos_arc.exe. MyDoom-S runs when a Windows user clicks on this malicious attachment. Thereafter the worm mass-mails itself to email addresses harvested from the infected machine with the subject line "photos" and message body "LOL!;))))". Like other variants of MyDoom, MyDoom-S tries to download a backdoor Trojan (in this case Surila-G) from one of a number of Websites onto infected PCs. The Trojan allows infected machines to be controlled remotely by attackers in order to send spam, for example.

Category 14.2 *Worms*

2004-08-17 **unsecure unprotected personal computer PC worm infection 20 twenty minutes Internet SANS**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/26967−1.html

August 17, Government Computer News — Unprotected PCs can expect infection in minutes.

The average survival time for an unprotected networked computer dropped from 40 minutes to 20 minutes over the last year, according to the SANS Institute of Bethesda, MD. That means that an unprotected PC can expect to become infected by a worm within 20 minutes of being connected to an unprotected network. "The actual time it will take for a specific computer to be compromised will vary widely depending on any filters applied by the Internet Service Provider and the configuration of the operating system," the institute said. But the trend reflects the narrowing window of opportunity for users to adequately protect networked computers from known vulnerabilities. Survival time is figured from daily reports submitted to SANS' Internet Storm Center by volunteers in 70 countries. ISC receives more than one billion reports of probes each month from organizations that manage more than 500,000 Internet addresses. The 20-minute figure represents the overall average time between probes on a targeted PC.

Category 14.2 *Worms*

2004-08-19 **Internet worm spread instant messenger IM ICQ Outlook PivX**

DHS IAIP Daily; http://www.pcworld.com/news/article/0,aid,117481,00.asp

August 19, IDG News Service — New worm travels by IM.

Security researchers at PivX Solutions have intercepted new malicious code closely resembling that from widespread attacks in June credited to a worm named "Scob" or "Download.ject." The Scob in June attacks were attributed to a Russian hacking group known as the "HangUP team." The attacks begin with instant messages sent to people using America Online's AOL Instant Messenger or ICQ instant messaging program inviting recipients to click on a link to a Web page. The messages could appear to be sent from strangers or from regular IM correspondents, Larholm says. Victims are routed to Websites hosted on servers in Uruguay, Russia, and the United States. The code on the sites takes advantage of vulnerabilities in Microsoft Internet Explorer and Outlook. Though Microsoft patched those vulnerabilities in MS03-025 and MS03-040, released in 2003, the attackers are attempting to exploit unpatched systems. In addition to opening a "back door" on the victim's computer, the new attacks change the victim's Web browser home page or Outlook e-mail search page to Websites featuring adult content, Thor Larholm of PivX says. "And as with the Scob attacks, this is all about money--in this case, driving ad revenue for specific people."

Category 14.2 *Worms*

2004-12-09 **worm outbreak Netsky-P worst Sophos Security report German teenager Sven Jaschan**

DHS IAIP Daily; http://www.govtech.net/?pg=news/news&id=92407

NETSKY-P TOPS LIST OF YEAR'S WORST VIRUS OUTBREAKS

Sophos, a leading security company, released a report revealing the hardest hitting viruses of 2004. In a year which saw a 51.8 percent increase in the number of new viruses, the Netsky-P worm has accounted for almost a quarter of all virus incidents reported, making it the hardest hitting virus of 2004. Sophos researchers have identified 10,724 new viruses so far in 2004 bringing the total viruses in existence to 97,535. German teenager Sven Jaschan, who wrote both the Netsky and Sasser worms, is responsible for more than 55 percent of all virus reports in 2004. Jaschan was apprehended and confessed to his involvement in May 2004, but his worms continue to spread. In November 2004, eight months since its original discovery in March, Jaschan's Netsky-P worm was still the world's most widely reported virus. Also, the United States continues to lead the world in spam, accounting for more than two of every five spam emails. Over 40 percent of spam comes from PCs that have been hijacked by viruses. Despite an increase in law enforcement, the volume of threats, such as viruses and spam, continues to rise.

Category 14.2 *Worms*

2004-12-28 **Cabir smart phone worm source code released Internet Kaspersky F-Secure**

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1745949,00.asp

December 28, eWeek — Source code for Cabir cell phone worm released.

Anti-virus vendors are bracing for a deluge of new and potentially dangerous mutants of the Cabir worm on smart phones running the Symbian Series 60 software. That's because the source code used to create the original Cabir worm has been posted on the Internet by a member of an international virus-writing group. According to an advisory from Kaspersky Lab senior virus analyst Aleks Gostev, the Cabir source code was previously accessible only to a limited number of people, including members of 29A, an international virus-writing group. According to information released by security research firm F-Secure, at least seven Cabir variants and one new strain of the Skulls Trojan have been detected this month alone. The first Cabir worm was discovered in June. F-Secure virus tracker Jarno Niemela said all the new variants appear to be recompiled versions based on original Cabir source code, confirming fears that the source code has been made public. Even though the worm has not been directly destructive or malicious, it is capable of blocking normal Bluetooth connectivity and completely draining the battery power from the infected phone.

Category 14.2 *Worms*

2005-01-17 **virus worm masquerading Tsunami disaster donation hoax mass mailer**

DHS IAIP Daily; http://www.sophos.com/virusinfo/articles/vbsuna.html

TSUNAMI DISASTER DONATION E-MAIL PLEA IS REALLY A VIRUS

Virus experts at Sophos have discovered a mass-mailing worm that poses as a plea for donations to help with the Indian Ocean tsunami disaster. The W32/VBSun-A worm spreads via e-mail, tempting innocent users into clicking onto its malicious attachment by pretending to be information about how to donate to a tsunami relief effort. However, running the attached file will not only forward the virus to other internet users but can also initiate a Denial of Service attack against a German hacking website. E-mails sent by the worm have the subject line: "Tsunami Donation! Please help!" Although there have only been a small number of reports of the W32/VBSun-A worm, Sophos recommends computer users ensure their anti-virus software is up-to-date.

Category 14.2 *Worms*

2005-01-21 **worm Crowt-A CNN headline masquerading Trojan Horse installation keystroke logger mailer anti-virus update**

DHS IAIP Daily; http://www.sophos.com/virusinfo/articles/newsheadline.html

NEW WORM POSES AS BREAKING NEWS HEADLINES FROM CNN

Virus researchers have identified a new worm which poses as information on the latest news stories. Crowt-A(W32/Crowt-A) takes its subject lines, message content and attachment names from headlines gathered in real-time from the CNN Website. It attempts to send itself by e-mail to addresses found on infected computers. Crowt-A's subject line and attachment share the same name, but continually change to mirror the front-page headline on the CNN news site. Crowt-A also installs a backdoor Trojan function that attempts to log keystrokes on infected PCs and sends gathered data to a remote user. These Trojans are often used by hackers to gain unauthorized control of PCs and to steal personal information such as bank passwords. Companies and individuals are urged to secure their desktop and servers with automatically updated anti-virus protection.

Category 14.2 *Worms*

2005-01-27 **MySQL worm Microsoft Windows infection common password attack bot software**

DHS IAIP Daily;
http://news.com.com/MySQL+worm+hits+Windows+systems/2100−734 9_3−5553570.html?tag=nl

MYSQL WORM SPREADS AMONG WINDOWS SYSTEMS

A worm that takes advantage of administrators' poor password choices has started spreading among database systems. The malicious program, known as the "MySQL bot" or by the name of its executable code, SpoolCLL, infects computers running the Microsoft Windows operating system and open-source database known as MySQL. Early indications suggest that more than 8,000 computers may be infected so far. The worm gets initial access to a database machine by guessing the password of the system administrator, using common passwords. It then uses a flaw in MySQL to run another type of program, known as bot software, which then takes full control of the system.

Category 14.2 *Worms*

2005-01-27 **Bagle worm variants spreading rapidly Internet Trojan Horse backdoor code execution attack peer-to-peer P2P**

DHS IAIP Daily; http://www.internetnews.com/security/article.php/3465321

NEW VERSIONS OF BAGLE WORM SPREADING RAPIDLY

Security firms are reporting on the emergence of new Bagle virus variants that are proliferating in the wild. There are likely two different variants that are new, experts said. Many security firms have raised the threat level for the variants from moderate to severe or critical, as more instances of the rapidly spreading worm are reported. The Bagle worm contains a Trojan backdoor that allows a remote user to execute arbitrary code on the infected PC. In addition to having its payload distributed via an e-mail attachment, the latest variants are also proliferating via peer-to-peer (P2P) applications as well. Instead of random subject names for e-mail, the polymorphic worm creates random file names of popular applications.

Category 14.2 *Worms*

2005-03-01 **worm Bagle variant spread Internet mass mailing Trojan Horse antivirus vendor report ZIP attachment**

DHS IAIP Daily; http://news.com.com/Watchdog−attacking+Bagle+ramps+up/2100−7 349_3−5594201.html?tag=nefd.top

NEW BAGLE VARIANT RAMPS UP

A new variant of Bagle is spreading rapidly, security companies have warned. Rather than a mass-mailing worm, BagleDl-L is a Trojan horse that damages security applications and attempts to connect with a number of Websites. It has been sent via spam lists to millions of addresses in the past 12 hours, said security company McAfee, which has upgraded it to a "medium" risk. The new variant could also have boosted overall Bagle traffic, which has increased five times in the past 24 hours, e-mail security vendor Postini said Tuesday, March 1. According to antivirus companies F-Secure and Sophos, the Websites linked to by the new Bagle currently contain no malicious code. However, Trojan and worm writers have been known to add malicious code to a Website after the initial attack has calmed down. For this Trojan to work, users must manually open a ZIP-file attachment that displays the programs "doc_01.exe" or "prs_03.exe," which must be run manually to infect a computer.

Category 14.2 *Worms*

2005-03-07 **first mobile messaging worm antivirus vendor report Symbian Series 60 F-Secure address book**

DHS IAIP Daily; http://www.pcworld.com/news/article/0,aid,119918,00.asp

ANTIVIRUS COMPANIES REPORT FIRST MOBILE MESSAGING WORM

The first mobile-phone virus that spreads using the popular Multimedia Messaging Service (MMS) is circulating among Symbian Series 60 mobile phones, antivirus companies have warned. Antivirus vendors first spotted the new virus, dubbed CommWarrior.A, on Monday, March 7. When an infected attachment is opened, the virus places copies of itself on vulnerable mobile phones and uses the phone's address book to send copies of itself to the owner's contacts using MMS. Antivirus experts believe CommWarrior, which has been spreading slowly among cell phone users since January, is not a serious threat. However, the virus could herald a new age of malicious and fast-spreading cell phone threats, according to Mikko Hyppönen of F-Secure Corporation. MMS is a popular text messaging technology that allows mobile phone users to send multimedia content, such as sound files or photos, between MMS-compliant mobile phones.

Category 14.2 *Worms*

2005-04-14 **Kelvir worm Reuters instant messaging system IM attack shut down denial of service DoS**

DHS IAIP Daily;
http://news.com.com/Worm+attack+forces+Reuters+IM+offline/21 00−7355_3 −5671139.html?tag=nefd.top

WORM ATTACK FORCES REUTERS INSTANT MESSAGING OFFLINE

Reuters has shut down its instant messaging (IM) system after suffering an onslaught from a new Kelvir worm, the company confirmed Thursday, April 14. The London-based international media company decided to take its Reuters Messaging system completely offline after noticing the attack on its network earlier on Thursday. The new variant attempted to spread by sending fake instant messages to people in contact lists on infected systems. The messages, crafted to look exactly like legitimate IM correspondence, attempted to lure people to a Website where their computers would be infected with Kelvir. Unlike the free IM software marketed by America Online, Microsoft and Yahoo, Reuters Messaging was created as a corporate tool, closed off from public subscribers and for internal company use only. But in recent years, the company has moved to connect its consumers with those networks. Technical workers at Reuters said they believe the new Kelvir attack could also target other IM systems. No other companies with messaging software had reported such a threat as of midday Thursday, however.

Category 14.2 *Worms*

2005-06-15 **new worm AOL Instant Messaging IM AIM**

DHS IAIP Daily; http://news.com.com/New+worm+hits+AIM+network/2100− 7349_3−57 48646.html

NEW WORM HITS AOL INSTANT MESSAGING NETWORK

A new worm spread quickly on America Online's AIM instant messaging service Wednesday afternoon, June 15, but was contained within hours, experts said. The worm spread in instant messages with the text: "LOL LOOK AT HIM" and included a Web link to a file called "picture.pif." If that file was downloaded and opened, the worm would send itself to all contacts on the victim's AIM Buddy List, according to representatives from IM security companies Facetime and IMlogic. Both IMlogic and Facetime were investigating the picture.pif file to determine exactly what it does. Facetime and IMlogic received several inquiries on the worm, signaling that it was widespread. The worm hit employees at Hewlett-Packard and prompted tech support at the company to send out an alert to employees. The worm is the latest in an increasing number of cyberthreats that use instant messaging to attack Internet users. Just as with attachments and links in e-mail, instant message users should be careful when clicking on links that arrive in instant messages--even messages from people they know, experts have warned.

Category 14.2 *Worms*

2005-08-04 **worm activity behavior dodge Net traps intrusion sensors**

DHS IAIP Daily; http://news.zdnet.com/2100−1009_22−5819293.html

WORMS COULD DODGE NET TRAPS

In a pair of papers presented at the Usenix Security Symposium in Baltimore, MD, Thursday, August 4, computer scientists said would-be attackers can locate such sensors, which act as trip wires that detect unusual activity. Internet sensor networks are groups of machines that monitor traffic across active networks and chunks of unused IP space. The sensor networks generate and publish statistical reports that permit an analyst to track the traffic, sniff out malicious activity and seek ways to combat it. The locations of the Internet sensors are kept secret. In a paper titled "Mapping Internet Sensors with Probe Response Attacks," a team of computer scientists from the University of Wisconsin discovered that the sensor maps furnish just enough information for someone to create an algorithm that can map the location of the sensors. All an attacker would have to do is throw packets of information at IP addresses and then check to see whether the activity showed up on the sensor reports. Researchers from Japan came to a similar conclusion in a paper titled "Vulnerabilities of Passive Internet Threat Monitors." The threat could be diminished, both studies said, if the information in the networks' public reports was less detailed.

Category 14.2 Worms

2005-08-14 **worm attack Microsoft Plug and Play vulnerability Windows XP**

DHS IAIP Daily; http://www.securityfocus.com/news/11281

WORM SPREADING THROUGH MICROSOFT PLUG-AND-PLAY FLAW

A worm started spreading on Sunday, August 14, using a flaw in the Windows operating system's Plug-and-Play functionality, according to two security groups, who advised users to update systems using a patch released by Microsoft Tuesday, August 9. Researchers at anti-virus firm F-Secure, who dubbed the worm, dubbed Zotob, do not believe that the worm will widely infect computer systems. The worm does not infect computers running Windows XP Service Pack 2 nor Windows 2003, as those systems are somewhat protected against the Windows Plug-and-Play vulnerability. Machines that block port 445 using a firewall will also not be vulnerable, the company said. On Friday, the Internet Storm Center upgraded their threat level for the Internet to yellow, because three different groups had published code for taking advantage of the Microsoft Windows' Plug-and-Play flaw to compromise Windows machines. Microsoft's investigation into the worm indicated that it only infects Windows 2000 systems. The company verified that any system patched by its update released last Tuesday will not be infected by the worm.

Category 14.2 Worms

2005-08-17 **computer worms attack each other F-Secure software security virus-writing gangs Microsoft Windows 2K 2000**

DHS IAIP Daily; http://tech.nytimes.com/reuters/technology/tech−viruses−fsec
ure−c.html

COMPUTER WORMS ARE ATTACKING EACH OTHER ACCORDING TO ANALYST

Computer worms that have brought down systems around the world in recent days are starting to attack each other, an analyst from Finnish software security firm F-Secure said on Wednesday, August 17. “We seem to have a botwar on our hands,” said Mikko Hypponen, chief research officer at F-Secure. “There appear to be three different virus-writing gangs turning out new worms at an alarming rate, as if they were competing to build the biggest network of infected machines,” said Hypponen. Hypponen said in a statement that varieties of three worms -- Zotob, Bozori and IRCbot -- were still exploiting a gap in Microsoft Corp.'s Windows 2000 operating system on computers that had not had the flaw repaired and were not shielded by firewalls.

Category 14.2 Worms

2005-08-17 **worm attack media outlet computers Microsoft Windows 2K 2000**

DHS IAIP Daily;
http://www.bloomberg.com/apps/news?pid=10000103&sid=aPrKdHO1
jQOI&refer=us

MEDIA OUTLET COMPUTERS ATTACKED BY WORM

CNN, SBC Communications Inc. and other media outlet computers were shut down on Tuesday, August 16, by a computer worm that targets Microsoft Corp.'s Windows software. The destructive program is a strain of an existing worm known as Zotob affecting computers running the Windows 2000 operating system, said Stephen Toulouse, security program manager at Microsoft. “Our analysis has revealed that the reported worms are different variations of the existing attack called Zotob,” Toulouse wrote in an e-mailed statement. Customers who had updated their software or are using other operating system versions such as Windows XP, weren't affected, he said. CNN spokesperson Laurie Goldberg said there were computer failures in Atlanta and New York. ABC Inc. had computers on the U.S. East and West coasts affected, spokesperson Jeff Schneider said. Production of the London-based Financial Times newspaper was disrupted by the infection, said spokesperson Katy Hemmings. Some computers were affected at number two U.S. phone carrier SBC Communications call centers, forcing employees to manually enter orders, said spokesperson Michael Coe. Computers at the New York Times Co., the third-largest newspaper publisher, were also hit. Security hole patch: http://www.microsoft.com/technet/security/Bulletin/MS05-039. mspx

---

Category 14.2 Worms

2005-08-25 **worm attack Microsoft MSN Messenger multiple languages Windows operating system OS**

DHS IAIP Daily; http://www.networkworld.com/news/2005/082505−msn−messenger−w orm.html?fsrc=rss−security

NEW MICROSOFT MESSENGER WORM WORKS IN MULTIPLE LANGUAGES

Users of Microsoft's MSN Messenger should be aware of a new "smart" worm that checks the configuration of their Windows client and sends a message in the appropriate language, according to security companies Akonix Systems and Symantec. The Kelvir.HI worm, a variant of the Kelvir IM malware that surfaced earlier this year, appears to be the first instant-message bug capable of checking systems settings and communicating in the victim's native tongue. When the worm penetrates a system, it sends a message in one of several languages, including Dutch, English, French, German and Greek as well as Portuguese, Swedish, Spanish and Turkish. The message in English is: "haha i found your picture!" If a user clicks on a link included with the message, a copy of the W32.Spyboot worm is automatically downloaded to their computer. Spyboot is a backdoor program that can, among other things, close security applications and help further spread the worm. The Kelvir.HI worm affects computers running Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003 and Windows XP, according to a Symantec advisory.

Category 14.2 Worms

2005-09-19 **worm Google spoofing warning peer-to-peer P2P game download browser corruption**

DHS IAIP Daily; http://www.snpx.com/cgi−bin/news55.cgi?target=109996736?−2622

SECURITY VENDOR WARNS OF GOOGLE-SPOOFING WORM

There is a new Google worm, called P2Load.A and it is being spread on peer-to-peer programs like Shareaza and Imesh. According to Forrest Clark, senior manager of consumer product marketing with antivirus vendor Panda Software, the worm is posing as a free version of the Lucasfilm game "Knights of the Old Republic II." P2Load.A first began spreading on Wednesday and is most widely spread in the U.S. and Chile, Clark said. Users that download this game are finding themselves installing a new work and then receiving poor Google search results. This is done in installation which changes the browser when a user is trying to access Google. Instead of reaching Google the user is directed to a spoof site, hosted on a server in Germany.

Category 14.2 Worms

2005-10-13 **malicious code malware javascript Web page myspace friend denial of service DoS**

RISKS; http://fast.info/myspace/ 24 07

IDIOT HACKER SHUTS DOWN MYSPACE USING JAVASCRIPT WORM

A criminal hacker ("Samy") using the myspace.com service decided to falsify his popularity ratings: "Let's see here…what would make my profile rock. Well, the most popular profiles on myspace pretty much consist of people with the IQ and English delivery skills of Kanye West so I don't want to mimic those, but popularity begets popularity. I need some more friends. I need people to love me. I delved into the bug and found that I could basically control the web browsing of anyone who hit my profile. In fact, I was able to develop something that caused anyone who viewed my profile to add my name to their profile's list of heroes. It's villainous. I was ecstatic. But it wasn't enough. I needed more. So I went deeper. A Chipotle burrito bol and a few clicks later, anyone who viewed my profile who wasn't already on my friends list would inadvertently add me as a friend. Without their permission. I had conquered myspace. Veni, vidi, vici."

Unfortunately, this idiot wasn'st satisfied with linear growth of his fake popularity: "But it wasn't enough.

If I can become their friend…if I can become their hero…then why can't their friends become my friend…my hero. I can propagate the program to their profile, can't I. If someone views my profile and gets this program added to their profile, that means anyone who views THEIR profile also adds me as a friend and hero, and then anyone who hits THOSE people's profiles add me as a friend and hero… So if 5 people viewed my profile, that's 5 new friends. If 5 people viewed each of their profiles, that's 25 more new friends. And after that, well, that's when things get difficult. The math, I mean. Some people would call this a worm. I call it popularity. Regardless, I don't care about popularity, but it can't hurt, right?"

Within 20 hours, he had 1,005,831 friend requests (all fake).

[Original pointer by Paul Bissex; summary byMK]
Myspace had to shutdown temporarily to clean up the mess.

Category 14.2 *Worms*

2005-10-17 **Teen worm ratings MySpace Websites Los Angeles data information networks profile XSS HTML**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/story/0 ,10801,105484,00.html?SKC=security−105484

TEEN USES WORM TO BOOST RATINGS ON MYSPACE.COM

Using a self-propagating worm that exploits a scripting vulnerability common to most dynamic Websites, a Los Angeles teenager made himself the most popular member of community Website MySpace.com earlier this month. While the attack caused little damage, the technique could be used to destroy Web site data or steal private information-even from enterprise users behind protected networks, according to Jeremiah Grossman, chief technical officer at Santa Clara, Calif.-based WhiteHat Security Inc. The 19-year-old, who used the name "Samy," put a small bit of code in his user profile on MySpace, a 32-million-member site, most of whom are under age 30. Whenever Samy's profile was viewed, the code was executed in the background, adding Samy to the viewer's list of friends and writing at the bottom of their profile, "... and Samy is my hero." The worm spread by copying itself into each user's profile. Because of MySpace's popularity, the worm spread quickly. The attack depended on a long-known but little-protected vulnerability called cross-site scripting (XSS). XSS arises because many Websites-apart from static sites that use only simple HTML code-are dynamic, allowing users to manipulate Website source code.

Category 14.2 *Worms*

2005-11-01 **Frankenstein AIM worm attack AOL instant messaging buddy icon adware rootkit infection remote control**

DHS IAIP Daily; http://www.pcworld.com/news/article/0,aid,123350,00.asp

'FRANKENSTEIN' ATTACK HITS AIM

A new worm is targeting America Online instant messenger users. The worm is installing rootkit types of backdoors on infected machines. The attack starts by the user opening a link of an AOL “buddy.” This link contains an infection sequence with drops adware files and the rootkit itself. Once on the PC, the malware shutsdown the antivirus software and installs new software that allos the PC to be remotely controlled.

Category 14.2 *Worms*

2005-11-15 **instant messaging IM worm spread mutation update too slow**

DHS IAIP Daily; http://www.techweb.com/wire/security/173603062

IM WORMS MUTATING AT AN ALARMING RATE

Instant-messaging (IM) threats are mutating at an alarming rate, as virus writers attempt to bypass security-system updates that corporations use for protection. A record number of IM threat mutations have been recorded by IMlogic Inc., which has found that 88 percent of all worms tracked by its threat center also have mutations. The worst chameleon is the Kelvir worm, which has mutated 123 times during the last 11 months, the Waltham, Mass., vendor said. Art Gilliland, vice president of product for IMlogic, said, "IM threats are different than email threats. Updating virus signatures doesn't work well for IM, because the mutations are exceedingly fast and so is the speed with which these threats propagate."

Category 14.2 *Worms*

2005-11-28 **worm Sober variant rise e-mail circulation social engineering**

DHS IAIP Daily; http://www.infoworld.com/article/05/11/28/HNsobervariantrise _1.html

SOBER VARIANT ON RISE, SECURITY FIRM WARNS

The latest variant of the Sober worm is proliferating, with a staggering one in 14 e-mails circulated on the Internet containing it as of Monday morning, November 28, according to the antivirus vendor Sophos. Around 85 percent of all viruses reported to Sophos are what the company calls Sober-Z, up from around 60 percent last week, said Graham Cluley, senior technology consultant. Right now, Sober-Z ranks as the third most prevalent virus for the year, behind Netsky-P in first and Zafi-D in second, he said. It first appeared around November 22 using several forms of social engineering to trick users into executing the attachment. Messages purporting to be from the U.S. Federal Bureau of Investigation warn recipients that they have been visiting illegal Websites and ask them to read a list of attached questions. Other versions pretend to be from the U.S. Central Intelligence Agency or offer video clips of Paris Hilton and Nicole Richie from the TV show "The Simple Life." While most antivirus vendors have updates that can remove the worm, the "clever" social engineering ploys are still effective, Cluley said.

Category 14.2 *Worms*

2005-12-02 **virus worm Sober MSN Hotmail denial-of-service DoS Comcast**

DHS IAIP Daily;
http://news.com.com/Sober+worm+stalls+MSN,+Hotmail/2100−7349 _3−
5980987.html?part=rss&tag=5980987&subj=news

SOBER WORM STALLS MSN, HOTMAIL

A variant of Sober known as Win32/Sober.Z@mm is to blame for disrupting e-mail traffic between Comcast account holders and user's of Hotmail and MSN Friday, December 2. These Microsoft-based e-mail servers are getting pummeled with an "unusually high mail load," causing delays in e-mail delivery to Hotmail and MSN customers, said Brooke Richardson, MSN's lead product manager. Richardson also indicated that Internet service providers besides Comcast may be having problems directing e-mail to Hotmail and MSN servers. "We are working with Comcast and other ISPs to address [the] issues," Richardson said. Blog reports say that some Comcast subscribers, when sending e-mail to a Hotmail or MSN account, have received an error message saying their message was not received. However, Microsoft says that all e-mails, while some may be delayed, are eventually getting through.

Category 14.2 *Worms*

2005-12-05 **Blaster worm active Microsoft Windows malicious software removal tool**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1896373,00.asp

TWO YEARS LATER, BLASTER WORM STILL THRIVING

More than two years after the Blaster Worm proliferated, the worm is still very much alive and there are fears within Microsoft that thousands of Windows machines will never be completely dewormed. According to statistics culled from Microsoft's Windows malicious software removal tool, between 500 and 800 copies of Blaster are removed from Windows machines per day. "The continued prevalence of [Blaster] is likely due to infected computers which, for one reason or another, will never be updated or disinfected. These computers will serve as eternal carriers for the worm," says Matthew Braverman, a program manager in Microsoft's Anti-Malware Engineering Team. In a case study on Blaster presented to the Virus Bulletin conference in October, Braverman said Blaster ranked in the top five of the most prevalent worms removed by the anti-malware utility. Braverman said the worm continues to be prevalent on a whopping 79 percent all Windows XP (Gold) machines and 21 percent of all Windows XP SP1 systems. On Windows XP SP2, infections are almost nonexistent, Braverman said, pointing out that XP SP2 systems went through a major post-Blaster security overhaul that means those systems cannot be infected through Blaster's main replication vector.

Category 14.2 *Worms*

2005-12-06 **instant messaging AOL AIM worm chat dupe payload activation IMLogic**

DHS IAIP Daily;
http://news.com.com/New+IM+worm+chats+with+intended+victims/ 2100−
7349_3−5984845.html?tag=cd.top

NEW INSTANT MESSENGER WORM CHATS WITH INTENDED VICTIMS

A new worm that targets users of America Online's AOL Instant Messenger (AIM) is believed to be the first that actually chats with the intended victim to dupe the target into activating a malicious payload, IM security vendor IMlogic warned Tuesday, December 6. According to IMlogic, the worm, dubbed IM.Myspace04.AIM, has arrived in instant messages that state: "lol thats cool" and included a URL to a malicious file "clarissa17.pif." When unsuspecting users have responded, perhaps asking if the attachment contained a virus, the worm has replied: "lol no its not its a virus", IMlogic said. The malicious file disables security software, installs a backdoor and tweaks system files, the company said. Then it starts sending itself to contacts on the victim's buddy list. Another worm discovered Tuesday, dubbed Aimdes.E, targets AIM users and arrives with the message: "The user has sent you a Greeting Card, to open it visit:" followed by a link, according to security specialist Akonix Systems. Once the target clicks on the link, the worm installs itself on the system. It opens a backdoor on the computer and sends itself to contacts on the buddy list, Akonix said.

Category 14.2 Worms

2005-12-07 **worm virus attack Sober January 2005 German Nazi Party formation political agenda**

DHS IAIP Daily; http://www.techweb.com/wire/security/174904530

NEXT SOBER ATTACK SLATED FOR JANUARY 5

The next big Sober worm attack is scheduled to take place Thursday, January 5, 2006, a date probably picked because it's the 87th anniversary of the founding of a precursor to the Nazi Party, a security firm said Wednesday, December 7. January 5, 2006, was the date embedded in the most recent Sober variants, said Ken Dunham, a senior engineer with Reston, VA-based VeriSign iDefense, a security intelligence firm. "We did reverse engineering on the variants, and found this date in the code," said Dunham. "The way this works is that at a pre-determined time, computers already infected with Sober will connect with specified servers and download a new payload, which will likely be spammed out in the millions, as was the last version." Sober, which boasts more than 30 variants, debuted more than two years ago, and is characterized by bilingual messages (English or German) that are mass-mailed in huge quantities. The worm's creator doesn't appear to be motivated by money. Instead, the creator -- who is assumed to be German -- has a political agenda, said Ramses Martinez, iDefense's director of malicious code operations. "There hasn't been one variant that did anything but send out right-wing German spam."

Category 14.2 Worms

2005-12-09 **anti-virus vendors Sober code cracked FBI CIA e-mail spoofing F-secure blog**

DHS IAIP Daily; http://news.com.com/Sober+code+cracked/2100−7349_3−5989094.html?tag=nl

ANTIVIRUS COMPANIES: SOBER CODE CRACKED

The latest variant of the Sober worm caused havoc in November by duping users into executing it by masking itself as e-mails from the Federal Bureau of Investigation and the Central Intelligence Agency. Antivirus companies were aware that the worm somehow knew how to update itself via the Web. The worm's author programmed this functionality to control infected machines and, if required, change their behavior. On Thursday, December 8, Finnish antivirus firm F-Secure revealed that it had cracked the algorithm used by the worm and could now calculate the exact URLs the worm would check on a particular day. Mikko Hypponen, chief research officer at F-Secure, explained that the virus' author has not used a constant URL because authorities would easily be able to block it. "Sober has been using an algorithm to create pseudorandom URLs which will change based on dates. Ninety-nine percent of the URLs simply don't exist...However, the virus' author can pre-calculate the URL for any date, and when he wants to run something on all the infected machines, he just registers the right URL, uploads his program and BANG! It's run globally on hundreds of thousands of machines," Hypponen wrote in his blog.

Category 14.2 Worms

2005-12-16 **worm virus Dasher outbreak Internet Microsoft Windows spyware payload**

DHS IAIP Daily; http://news.com.com/Dasher+worm+gallops+onto+the+Net/2100−10 02_3−5999114.html?part=rss&tag=5999114&subj=news

DASHER WORM GALLOPS ONTO THE INTERNET

A Windows-targeted worm that drops spying software on vulnerable PCs is spreading across the Internet, security experts have warned. The Dasher.B worm exploits a flaw in Microsoft Windows Distributed Transaction Coordinator, or MDTC, security companies said Friday, December 16. Microsoft announced and patched the hole in the component for transaction processing in October. However, initial glitches with the update may have left some users without a properly implemented fix, Sophos said. Dasher.B is a network worm that has the potential to open a back door on computers with the MSDTC flaw, security experts said. The infected systems are then prompted to connect to a remote computer for instructions. Once connected, it downloads a malicious program that tracks keystrokes. A third version of the worm emerged Friday, Dasher.C, which almost looks identical to Dasher.B, said Oliver Friedrichs, senior manager at Symantec's Security Response Center. Three versions of Dasher -- B, C and A, which emerged earlier this week -- have infected at least 3,000 systems worldwide, Friedrichs said, noting the growth rate of the infection has since leveled off.

Category 14.2 Worms

2006-01-09 **Sober worm stops spreading**

DHS IAIP Daily; http://www.vnunet.com/vnunet/news/2148257/quiet−sober−front 23

SOBER WORM INFECTION RATES ARE PLUMMETING.

The Sober worm, which was due to activate last Thursday, January 5, has stopped spreading and its author has held back from uploading malware onto any machines. Sober was the most common infection in November and December last year, and was programmed to download software from remote Websites. It was feared that host machines across the world would start sending spam or take part in denial of service attacks. Instead the virus writer has stayed undercover and the worm has ceased trying to spread itself. "When the Sober.Y download deadline passed on 6 January all infected machines started download attempts from the five different sites. At the same time, the virus stopped e-mailing itself around," said Mikko Hyppönen, chief research officer at security firm F-Secure. "As a result, the virus that had held the number one position since November 2005 just disappeared from the stats." Hyppönen added that infection rates for the worm over the past week were running at 18,000 PCs per day but are now plummeting.

Category 14.2 Worms

2006-01-18 **new worm VB.bi threat charts January 2006**

DHS IAIP Daily; http://www.informationweek.com/news/showArticle.jhtml?articleID=177101528 23

NEW WORM HITS THE TOP OF THE THREAT CHARTS

A worm that debuted Tuesday, January 17, had quickly climbed the malware chart to the number three spot by Wednesday, January 18, a Finnish security company said. With a variety of names -- F-Secure calls it VB.bi, Symantec dubs it Blackmal.e, McAfee labels it MyWife.d -- the worm, said Helsinki-based F-Secure, is a simple Visual Basic (VB) construction that arrives as an e-mail file attachment. The worm also spreads through shared folders, and when activated tries to disable a number of security programs, including those sold by Symantec, McAfee, Trend Micro, and Kaspersky Labs. One of its distinguishing features, noted the Internet Storm Center (ISC) in its alert is that "the attachment can be either an executable file or a MIME file that contains an executable file." The latter tactic is meant to conceal the payload's danger; the MIME format is rarely used by attackers. One of the last great MIME-based attacks was the Nimda worm of 2001. Symantec, which tagged the worm with a "2" in its 1 through 5 threat scale, has posted a free-of-charge removal tool on its Website that deletes all traces of the malware.

Category 14.2 Worms

2006-01-20 **worm malicious code Microsoft Office documents F-Secure**

DHS IAIP Daily; http://www.techweb.com/showArticle.jhtml?articleID=177102371 23

NEW WORM CORRUPTS MICROSOFT DOCUMENTS.

A new worm that already accounts for one in every 15 pieces of malicious code carries a "nuclear option" payload that corrupts data in a slew of popular file formats, a security company warned Friday, January 20. The Nyxem.e worm, said Finnish security firm F-Secure, carries code that instructs it to replace data in files with .doc, .xls, .mdb, .mde, .ppt, .pps, .zip, .rar, .pdf, .psd, or .dmp extensions with the useless string "DATA Error [47 0F 94 93 F4 K5]" on the third of the month. This list includes the native document formats for Microsoft Word, Excel, PowerPoint, and Access, as well as for Adobe PhotoShop and Acrobat. Nyxem.e is similar to the VB.bi/Blackmal/MyWife.d worm that climbed the charts earlier last week, added F-Secure. The worm arrives as an attachment to e-mail messages with a variety of subject headlines, many of which tout porn with phrases. It also tries to delete selected security software, and can spread through shared folders as well as by hijacking addresses from infected PCs.

Category 14.2 Worms

2006-01-24 **Kama Sutra worm ActiveX Windows digital signature spoofing**

DHS IAIP Daily; http://www.securitypipeline.com/news/177103403;jsessionid=BWMKMS524JJFQQSNDBGCKHSCJUMEKJVN 23

KAMA SUTRA WORM SPOOFS DIGITAL CERTIFICATES.

The Kama Sutra worm can fool Windows into accepting a malicious ActiveX control by spoofing a digital signature, a security company said Tuesday, January 24. Sunnyvale, CA-based Fortinet said the worm -- which also goes by names such as Nyxem.e, MyWife.d, Grew.a, and Blackmal.e -- adds 18 entries to the Windows Registry to slip the ActiveX control by the operating system's defenses. "By creating the following entries, the control is considered 'safe' and digitally signed," said the Fortinet advisory. The ActiveX control, added Fortinet, is used by the worm to automatically run its code each time the PC is turned on and Windows boots. "The threat of worms like this will make them much more dangerous in the future," said Bojan Zdrnja, an analyst for the Internet Storm Center, on the group's site. As of late Monday, January 23, the Kama Sutra worm had infected more than 630,000 systems, said the Internet Storm Center. The worm is considered particularly dangerous because it contains code that triggers an overwrite of all .doc, .xls, .mdb, .mde, .ppt, .pps, .zip, .rar, .pdf, .psd, and .dmp files on the third of each month.

Category 14.2 Worms

2006-01-30 **worm Kama Sutra Blackworm Blackmal MyWife Nyxem India Peru infection**

DHS IAIP Daily; http://www.techweb.com/wire/security/177105325;jsessionid=FICPCUF4MHL4YQSNDBOCKHSCJUMEKJVN 23

KAMA SUTRA WORM HITS INDIA, PERU HARDEST.

The worm set to overwrite important Microsoft and Adobe documents Friday, February 3, has struck India five times harder than the U.S., and Peru three times harder, a security company claimed. According to Chicago-based LURHQ, the worm -- dubbed Kama Sutra, Blackworm, Blackmal, MyWife, Nyxem, and nearly two-dozen other names -- has infected nearly 80,000 PCs in India. Peru sports almost 55,000 compromised computers. In comparison, the U.S. has about 15,000 machines contaminated with the worm. "Viruses don't always spread uniformly," LURHQ said in its report. "There are many factors at play which are hard to quantitize, such as the initial seeding, social engineering, AV deployment, and random chance. And, as with all statistics, take [these] with a grain of salt." LURHQ tagged the total number of Blackworm-infected computers at around 300,000, even though a Web-based infection counter claims a number in the millions. LURHQ, however, was able to strip out bogus "clicks" on that counter to arrive at is estimate. "An attempt was made by an unknown party to artificially inflate the counter using a set of 279 distributed (presumably compromised) computers," said LURHQ. LURHQ's report: http://www.lurhq.com/blackworm-stats.html

---

Category 14.2 Worms

2006-02-03 **Kama Sutra worm hype damage mitigation mediate attention**

DHS IAIP Daily; http://wireservice.wired.com/wired/story.asp?section=Technology&storyId=1154343 23

EXPERTS: HYPE MAY HAVE MITIGATED KAMA SUTRA WORM.

Companies and individuals heeded this week's warning about a file-destroying computer worm known as "Kama Sutra," helping minimize its damage Friday, February 3, security experts said. One Italian city shut down its computers as a precaution, but otherwise the worm's trigger date arrived with relatively few reports of problems. Hundreds of thousands of computers were believed to be infected, but security vendors say many companies and individuals had time to clean up their machines following the alarm, carried by scores of media outlets. "The importance of media attention from an awareness and educational standpoint has been a very good thing," said Marc Solomon, director of product management at security vendor management McAfee Inc. "It alerts users to what may have happened and the destruction that could have occurred." David A. Milman, chief executive of the Syracuse, NY-based Rescuecom, said, "the hype was probably what prevented the disaster from happening."

Category 14.2 Worms

2006-02-07 **Kama Sutra worm hype overblown Microsoft anti-malware team manager blog**

DHS IAIP Daily; http://www.securitypipeline.com/news/179101481 23

MICROSOFT SAYS KAMA SUTRA WORM OVERBLOWN.

As users and security firms reported little damage done by the Kama Sutra worm, a manager of Microsoft's anti-virus development team warned that overhyping threats could lead to a "cry wolf" syndrome where future alerts aren't taken seriously. "Too much hype in situations that end in false alarms ends up diluting the meaning of warnings for true worldwide threats," wrote Matt Braverman, a program manager with Microsoft's anti-malware team, on the group's blog. In particular, Braverman criticized those who called out warnings based on a Web counter that, though initially reporting the number of Kama Sutra infections accurately, was manipulated later in the process to claim millions of machines had been compromised. Braverman's comments were in sync with earlier positions taken by Microsoft in January on the worm.

Category 14.2 Worms

2006-02-15 **Google hacking trend worm search phpBB server attack**

DHS IAIP Daily; http://www.vnunet.com/articles/print/2150292 23

GOOGLE 'HACKING' OCCURS WITH THE OBJECTIVE TO FIND SENSITIVE INFORMATION ON THE INTERNET.

Malware authors are increasingly creating digital pests that use Google to find their next victim. Using the search tool for automated vulnerability detection is the latest trend in a technique known as 'Google hacking.' George Kurtz, senior vice president for risk management at security firm McAfee, told VNUNet about the phenomenon after a presentation at the RSA Conference in San José. The Santy.a worm, for instance, targeted a known vulnerability in some versions of the phpBB open source bulletin board application to deface Websites. It found its victims through an automated Google search query. Google eventually stopped the worm from spreading by blocking all searches that would turn up servers running the application. But the search engine is able to detect the abuse only if the queries stand out from other searches. Google 'hacking' does not mean breaking into the company's servers but involves online criminals using Google and other search engines to find sensitive information on the Internet. Pictures and screenshots of 'Google hacks': http://www.siliconvalleysleuth.com/2006/02/things_you_dont.html

---

Category 14.2 Worms

2006-02-21 **prediction worm threat impact low Mambo content management system CMS**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/story/0 23
,10801,108868,00.html

IMPACT OF WORM TARGETING MAMBO CMS LOW, SAY RESEARCHERS.

F-Secure Corp. is warning of a network worm that targets vulnerabilities in the Mambo Content Management System (CMS) and PHP XML-RPC, a library of code for PHP programmers that allows procedures to run between computers with different operating systems. F-Secure calls the worm Mare.D, saying it installs several backdoors on a compromised system. The worm scans random hosts for those running vulnerable installations of the Mambo open source Website content management system or the PHP XML-RPC library. Two of the backdoors -- "cb" and "ping.txt" -- are connectback shell backdoors that are connected to a remote host via port 8080, F-Secure said. The third is controlled by Internet Relay Chat and written in the Perl language. The main component of the worm listens on User Datagram Protocol port 27015 for commands, F-Secure said. Mambo wrote on its Website that it has issued fixes for versions 4.5.3 and 4.5.3h. Those fixes can be downloaded from Mambo's Website. It also recommended that users upgrade their software if they have a version earlier than 4.5.3. Mambo's Website: http://www.mamboserver.com/

Category 14.2 Worms

2006-03-03 **new Bagle worm social engineering legal action threat**

DHS IAIP Daily; http://www.informationweek.com/news/showArticle.jhtml?articl 23
eID=181500852&subSection=Columns

NEWEST BAGLE WORM THREATENS LEGAL ACTION.

Another Bagle worm appeared Friday, March 3. Bagle.do, said UK-based Sophos, spreads in e-mails with subject lines such as "Lawsuit against you." The attached file, with names like "lawsuit.exe," purports to be supporting legal documents. Launching the executable file infects the PC with a backdoor and lowers the machine's security settings, and may end up with more malicious code downloaded to the system from a slew of Websites.

Category 14.2 Worms

2006-03-29 **new Bagle worm rootkit Trojan features F-Secure report mass infection**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1944133,00.asp 23

LATEST BAGLE WORM HAS STEALTH CAPABILITIES

Malicious hackers have fitted rootkit features into the newest mutants of the Bagle worm, adding a stealthy new danger to an already virulent threat. According to virus hunters at F-Secure, of Helsinki, Finland, the latest Bagle.GE variant loads a kernel-mode driver to hide the processes and registry keys of itself and other Bagle-related malware from security scanners. The use of offensive rootkits in existing virus threats signals an aggressive push by attackers to get around existing anti-virus software and maintain a persistent and undetectable presence on infected machines. The Bagle threat started as a simple e-mail executable in 2004 but has grown and evolved over the years to become one of the most active threats against PC users. Security researchers estimate that the numerous Bagle variants have infected more computers than any other virus group.

Category 14.2 Worms

2006-04-18 **hackers issue patch spam spyware warning F-Secure Bagle worm family**

DHS IAIP Daily; http://www.esecurityplanet.com/article.php/3599831 23

HACKERS ISSUE OWN 'PATCH' TO INFECTED COMPUTERS.

The gang of virus writers behind the virulent Bagle family of worms has issued a patch to its malicious code. This past Sunday, April 16, computers infected with several different variants of the Bagle worm began downloading an updated version -- a new spam tool used by hackers to send out unwanted bulk e-mail. "They've programmed the virus to contact the central Website to see if there's an update available and if there is, they will download and run this new malicious code. This technique -- we call it second-state activation -- is a way the virus writers can add additional programs and run them on the infected machines," says Mikko Hypponen chief research officer for F-Secure Corp.

14.3 Virus/worms

Category 14.3 Virus/worms

1998-04-14 **auto-executable Trojan macro virus logic bomb e-mail QA**

RISKS 19 67

In April, highly-respected security guru A. Padgett Peterson wrote in RISKS that the MS-Outlook mail-reader product in Windows 98 allows automatic execution of binary e-mail attachments. So much for the familiar assurance, "You can't get hurt merely by opening an e-mail message" in response to anguished questions about "Good Times" and other hoaxes. "Times are about to become `interesting'. Caveat Y'all."

Category 14.3 Virus/worms

1998-12-21 **virus network encryption executables Windows NT**

PC Week http://www.zdnet.com/zdnn/stories/news/0,4586,2178239,00.html

In December 1998, a new and dangerous network worm called the Remote Explorer attacked executables at MCI WorldCom, causing serious damage to data on several thousand of its servers and workstations. The press reported the program as a "smart virus" but it appears that it did not integrate itself into programs; instead, reports indicated that the attacking program spread through networks. The large (120 Kb) worm compressed (encrypted) executables and propagated through Windows NT networks; a clever twist increased the rate of propagation during the 15:00-06:00 window, when network management is usually at a lower level than during peak hours. In addition, the worm encrypted .DOC and .XLF files. The worm appeared to be a C program and was itself partly encrypted, making reverse engineering more difficult. Network Associates Inc. successfully cryptanalyzed the compression algorithm and issued updates to their antivirus signature strings.

Category 14.3 Virus/worms

1999-03-27 **virus e-mail Trojan Outlook address book spam**

CERT, news wires

On Friday 26 March 1999, the CERT-CC received initial reports of a fast-spreading new MS-Word macro virus. "Melissa" was written to infect such documents; once loaded, it uses the victim's MAPI-standard e-mail address book to send copies of itself to the first 50 people on the list. The virus attaches an infected document to an e-mail message with subject line "Subject: Important Message From <name>" where <name> is that of the inadvertent sender. The e-mail message reads, "Here is that document you asked for ... don't show anyone else ;-)" and includes a MS-Word file as an infected attachment. The original infected document, "list.doc" was a compilation of URLs for pornographic Web sites. However, as the virus spread it was capable of sending any other infected document created by the victim.

Because of this high replication rate, the virus spread faster than any previous virus in history. On many corporate systems, the rapid rate of internal replication saturated e-mail servers with outbound automated junk e-mail. Initial estimates were in the range of 100,000 downed systems. Anti-virus companies rallied immediately and updates for all the standard products were available within hours of the first notices from CERT-CC.

The Melissa macro virus was quickly followed by the PAPA MS-Excel macro virus with similar properties.

Category 14.3 Virus/worms

1999-03-30 **Excel macro virus e-mail ping denial of service**

CERT-CC, news wires

Hot on the heels of the Melissa macro-virus outbreak, a similar virus attacking MS-Excel spreadsheets appeared on the Net at the end of March. The PaPa macro virus was more virulent than the Melissa virus in that it sent out copies of itself to 60 names drawn from the victim's e-mail address book but did so every time an infected document was opened. In addition, the virus launched denial-of-service ping attacks on two IP addresses. The subject line of the automated junk e-mail was "Fwd: Workbook from all.net and Fred Cohen" and the text was "Urgent info inside. Disregard macro warning."

Category 14.3 Virus/worms

1999-04-01 **information warfare virus mail bombing denial of service**

Daily Telegraph

The onslaught of the Melissa, Papa and Mad Cow viruses caused significant operational difficulties for NATO military forces in their attacks on the Serbian state. E-mail servers were taken down for disinfection; US Navy ships were infected; and a Belgrade computer tried to swamp NATO e-mail in a simple denial-of-service attack involving 2,000 e-mail messages a day.

Category 14.3 *Virus/worms*

1999-04-02 **virus aftermath policies defenses management planning**

OTC, AP

The Melissa worm spread explosively through corporate e-mail systems and the Internet in late March. The worm spread through e-mail attachments in MS-Word ".doc" format and mailed itself to the first 50 addresses in each victim's standard e-mail address book. The worm created a false message with a deceptive subject line and content. The worm was traced to virus-writer(s) called "VicodinES."

Category 14.3 *Virus/worms*

1999-04-02 **virus worm e-mail battle information warfare malicious**

Dow Jones, Wall Street Journal

Shortly after the outbreak of the Melissa worm, the Papa worm was released with a component that caused a flood of junk e-mail to the mailbox of Dr Fred Cohen in an attempted denial-of-service attack (foiled by proper configuration management).

Category 14.3 *Virus/worms*

1999-04-15 **virus defense CERT-CC education reporting**

TechWeb

Keith Rhodes, Technical Director for Computers and Telecommunications Accounting and Information Management at the General Accounting Office, warned that Melissa was just a harbinger of trouble to come: "It is likely that the next virus will propagate faster, do more damage, and be more difficult to detect and to counter." He urged software makers to take responsibility for providing better protection in their own products against malicious code. Michael Vatis, Director of the FBI's National Infrastructure and Protection Center, warned, "Because of the ease of writing and disseminating destructive and disruptive viruses, deterring people from engaging in such conduct is the surest method of prevention." Richard Pethia, Director of Carnegie Mellon University's Computer Emergency Response Team Coordination Center at the Software Engineering Institute <http://www.cert.org> argued that only fundamental redesign would accomplish this goal. Currently, software such as MS-Word has extended its functionality at the expense of security. But Pethia added, "If we're ever faced with simultaneous infections at Internet speed, we won't be able to handle it." Only secure default configurations, strong identification and authentication and integrated virus resistance will prevent future disasters due to portable executable code.

Category 14.3 *Virus/worms*

1999-12-02 **virus worm e-mail attachment Trojan misleading subject automatic excecution double-click open spread virulent**

DOW JONES BUSINESS NEWS; Australian

At the end of November, anti-virus experts reported a flurry of infections by the Mini-Zip e-mail enabled virus/worm, a variant of the Worm.ExploreZip virus that appeared in June. This virus/worm was compressed, so it was not recognized using the known signature strings for the original virus/worm. Once resident, the Mini-Zip program reads the addresses of new e-mail in MS-Outlook and automatically sends itself as a responseusing the "RE: " convention. The fraudulent message text is, "Hi <recipient-name>! I received your e-mail and I shall send you an e-mail ASAP. Till then, take a look at the attached zipped docs. bye." However, the attachment is actually a dropper program that installs the viral code in memory on Windows 9x and Windows NT systems and continues the spread of the attachment through e-mail. In addition, the virus code resets file lengths on the C: drive to zero, causing major damage and making it hard to recover files on the damaged disk.

In December, more than 120 of Australia's largest companies were hit by the virus, causing two days of downtime. Reports that Compaq Australia may have been the first Australian site hit by the virus and therefore responsible for sending out infected e-mail caused embarrassment to that company.

Category 14.3 *Virus/worms*

1999-12-03 **virus worm BIOS checksum Y2K new year trigger date format hard drive boot error message**

Dow Jones, Computerworld
http://www.computerworld.com/home/news.nsf/all/9912035y2kworm

The upsurge in e-mail-enabled worms and viruses in late 1999 supported the predictions of anti-virus experts who said that the Y2K transition would see a flurry of new viruses and variants that would contribute to confusion about the source of software problems following New Year's Day 2000.

Nancy Weil, writing in ComputerWorld <http://www.computerworld.com/home/news.nsf/all/9912035y2kworm>, suggested that the Worm.Mypic (aka W32/Mypics.worm) identified in the first days of December demonstrated the kind of problem we were to face in the following weeks. Worm.Mypic arrives as an executable attachment (Pics4You.exe with a length of 34,304 b). If executed, the program e-mails itself to the usual first 50 names in the MS-Outlook address list (and continues to try to do so at regular intervals). As soon as the date changes to 1 Jan 2000, the resident virus overwrites checksum data for the computer's BIOS, interfering with the boot sequence. The virus also attempts to format C: and D: drives.

As usual, everyone agreed that it was critically important to update virus-signature files even more freqently than usual as we approached the new year.

Category 14.3 *Virus/worms*

1999-12-07 **virus Trojan**

PR Newswire

Computer Associates issued a warning about the W.95.Babylonia virus, described as an extensible virus whose payload could be modified remotely by its author. The December outbreak of Babylonia in the wild involved a Trojan disguised as a Y2K bug fix for Internet Relay Chat (IRC) users. The Trojan would send itself to other users and also poll an Internet site in Japan looking for updated plugins to alter the effects of the malicious software.

Category 14.3 *Virus/worms*

1999-12-08 **virus overview**

Age (Melbourne, Australia)

Computer Associates (Australia) reported a major rise in damage from a rash of new and increasingly virulent viruses. Apparently one of the most serious viruses in Australia was W32/Mypics.

Category 14.3 Virus/worms

2001-01-17 **worldwide virus worm infection data top ten infectors malware**

Symantec Antivirus Research Center (SARC)

In January, David Banes, Editor of the the Symantec Antivirus Research Center (SARC) Newsletter, summarized the findings of the year 2000 infection rates. The top ten malware types were as follows:

1. Wscript.KakWorm
 - www.sarc.com/avcenter/venc/data/wscript.kakworm.html
2. W95.MTX
 - www.sarc.com/avcenter/venc/data/w95.mtx.html
3. VBS.LoveLetter
 - www.sarc.com/avcenter/venc/data/vbs.loveletter.a.html
4. W95.Hybris.gen
 - www.sarc.com/avcenter/venc/data/w95.hybris.gen.html
5. VBS.Stages.A
 - www.sarc.com/avcenter/venc/data/vba.stages.a.html
6. W32.HLLW.Qaz.A
 - www.sarc.com/avcenter/venc/data/qaz.trojan.html
7. Happy99.Worm
 - www.sarc.com/avcenter/venc/data/happy99.worm.html
8. W32.Navidad
 - www.sarc.com/avcenter/venc/data/w32.navidad.html
9. VBS.Network
 - www.symantec.com/avcenter/venc/data/vbs.network.html
10.W32.FunLove.4009
 - www.symantec.com/avcenter/venc/data/w32.funlove.4099.html

Category 14.3 Virus/worms

2001-04-01 **Windows shares virus/worm modem autodial data destruction**

SANS

SANS issued an alert about a new type of worm on (unfortunately) 1 April 2001. The text reads as follows:

At 8:00 am on Saturday, April 1 (This is not an April Fool's joke!) the FBI announced it had discovered malicious code wiping out the data on hard drives and dialing 911. This is a vicious virus and needs to be stopped quickly. That can only be done through wide- scale individual action. Please forward this note to everyone who you know who might be affected.

The FBI Advisory is posted at
http://www.nipc.gov/nipc/advis00- 038.htm

The 911 virus is the first "Windows shares virus." Unlike recent viruses that propagate though eMail, the 911 virus silently jumps directly from machine to machine across the Internet by scanning for, and exploiting, open Windows shares. After successfully reproducing itself in other Internet-connected machines (to assure its continued survival) it uses the machine's modem to dial 911 and erases the local machine's hard drive. The virus is operational; victims are already reporting wiped-out hard drives. The virus was launched through AOL, AT&T, MCI, and NetZero in the Houston area. The investigation points to relatively limited distribution so far, but there are no walls in the Internet.

---------- Action 1: Defense ----------

Verify that your system and those of all your coworkers, friends, and associates are not vulnerable by verifying that file sharing is turned off.

* On a Windows 95/98 system, system-wide file sharing is managed by selecting My Computer, Control Panel, Networks, and clicking on the File and Print Sharing button. For folder-by-folder controls, you can use Windows Explorer (Start, Programs, Windows Explorer) and highlight a primary folder such as My Documents and then right mouse click and select properties. There you will find a tab for sharing.

* On a Windows NT, check Control Panel, Server, Shares.

For an excellent way to instantly check system vulnerability, and for detailed assistance in managing Windows file sharing, see: Shields Up! A free service from Gibson Research (
http://grc.com/)

---------- Action 2: Forensics ----------

If you find that you did have file sharing turned on, search your hard drive for hidden directories named "chode", "foreskin", or "dickhair" (we apologize for the indiscretion - but those are the real directory names). These are HIDDEN directories, so you must configure the Find command to show hidden directories. Under the Windows Explorer menu choose View/Options: "Show All Files". If you find those directories: remove them. And, if you find them, and want help from law enforcement, call the FBI National Infrastructure Protection Center (NIPC) Watch Office at 202-323- 3204/3205/3206. The FBI/NIPC has done an extraordinary job of getting data out early on this virus and deserves both kudos and cooperation. You can help the whole community by letting both the FBI and SANS (intrusion@sans.org) know if you've been hit, so we can monitor the spread of this virus.

---------- Moving Forward ----------

The virus detection companies received a copy of the code for the 911 Virus early this morning, so keep your virus signature files up- to-date. We'll post new information at www.sans.org as it becomes available.

Category 14.3 *Virus/worms*

2001-06-11 **e-mail enabled worm child pornography evidence police law enforcement**

NewsScan

SOFTWARE "WORM" SEARCHES YOUR COMPUTER FOR PORNOGRAPHY
A new computer virus called VBS.Noped.a now circulating invades computer memories in a hunt for picture files with pornographic-sounding names and reports them to the police. The virus (a "worm") arrives from an unknown source as an e-mail attachment with the subject line: "FWD: Help us ALL to END ILLEGAL child porn NOW." If it finds suspected pornography, it sends a message to the police saying: "This is Antipedo2001. I have found a PC with known child pornography files on the hard drive. I have included a listing below and included a sample for your convenience." An executive of the National Center for Missing and Exploited Children has repudiated the rogue effort and says his group "does not support unlawful means even to achieve meritorious ends." (New York Times 11 Jun 2001)
http://www.nytimes.com/2001/06/11/technology/11VIRU.html

Category 14.3 *Virus/worms*

2001-09-25 **hoax e-mail enabled virus worm social engineering**

NewsScan

PHONY "PEACE" MESSAGE CARRIES COMPUTER VIRUS [25 Sep 2001]
Beware of an e-mail virus circulating with the subject line "Peace Between America and Islam" and containing an attachment labeled "WTC.exe." The message reads in part "Let's Vote To Live in Peace," and continues: "AmerRiCa... Few Days WiLL Show You What We Can Do!! It's Our Turn. ZaCkER is So Sorry For You." (Los Angeles Times 25 Sep 2001)
http://www.latimes.com/technology/la-000076747sep25.story?coll=la%2Dheadline s%2Dtechnology

---

Category 14.3 *Virus/worms*

2001-11-01 **e-mail enabled worm virus Trojan dropper file infector junk e-mail spam**

NewsScan

NEW VIRUS: NIMDA [19 Sep 2001]
Saying it has no connection to the terrorist event of last week, U.S. Attorney General John Ashcroft reported the existence of a new computer virus called Nimda, which spreads in a variety of ways, including e-mail with "readme.exe" attachments, as well as infected Web sites that generate a stealth file called readme.eml. The virus can crash mail servers by creating massive loads of junk messages. (San Jose Mercury News 19 Sep 2001)
http://www.siliconvalley.com/docs/news/svfront/worm091901.htm

On the 25th of September, Peter Håkanson reported that all public hospitals in Gothenburg Sweden were crippled by NIMDA. He wrote in RISKS 21.67, "The hospitals in "Västra Götaland" sweden (west coast, population 1M) were isolated fron Internet during 23 Sep 2001. Some of internal networks had to be partitioned to prevent nimda spreading further. Reservations and computer-based medical records were unavailable."
http://www.vgregion.se

NEW VERSION OF THE NIMDA VIRUS [1 Nov 2001]
A new version of the Nimda computer virus, Nimda.E, has been detected on computer networks this week; however, the federally funded computer security organization Computer Emergency Response Team says the CERT has not seen a significant surge in the virus since it was first identified. On Tuesday, Nimda.E disrupted access to the Internet by New York Times employees, but the newspaper's computer operations are now back to normal. (New York Times 1 Nov 2001)
http://partners.nytimes.com/2001/11/01/technology/01VIRU.html

---

Category 14.3 *Virus/worms*

2002-05-04 **worm e-mail enabled virus Outlook address books flooding spam**

NIPC Daily Report

On 4 May, an outbreak of the "W32.Magister" computer virus [worm] has apparently struck businesses in Europe, the U.S., and elsewhere. Businesses reported receiving dozens of unsolicited e-mail. Replies and requests to be removed from any mailing lists involved only resulted in a flood of additional e-mail. Companies in the Netherlands, France, New Zealand, the U.K. and the U.S. were similarly affected, including such large multinationals as Unilever and Diageo. Many of the recipients were businesses in the food industry that subscribed to an e-mail newsletter service from Foodnavigator.com. The culprit appears to be the W32.Magistr.24876@mm virus. The virus infects Windows Portable Executable files. It then gathers e-mail addresses from Outlook and Outlook Express mail folders, Windows address books, and the sent items file in Netscape, and sends out multiple e-mail messages. According to the Symantec Anti-virus Research Center, the virus was first discovered on 13 March, and there have been at least 50 confirmed infections affecting more than ten sites since then. (Source: Newsbytes, 5 May)

Category 14.3 Virus/worms

2004-02-17 **virus worm Bagle network Internet spread momentum**

DHS IAIP Daily;
http://www.eweek.com/article2/0,4149,1528349,00.asp?kc=EWRSS03119TX1K00
00594

February 17, eWEEK — New Bagle virus gaining momentum.

A new version of the Bagle virus is making the rounds of the Internet. Known as Bagle.B, the virus is a mass-mailer like the original Bagle and also includes a component that notifies the author each time a new machine is infected. The new variant arrives in an e-mail with a spoofed sending address and a subject line that contains the term "ID" followed by a string of random characters. The text of the message simply says: "Yours ID" followed by another bunch of random characters. The attachment is an executable file with a random file. Once the user executes the file, the virus mails itself to all of the names found on the user's hard drive, with the exception of addresses in the Hotmail, MSN, Microsoft and AVP domains. Bagle.B also opens port 8866 and begins listening for remote connections, according to Network Associates Inc. The virus also sends an HTTP notification, presumably to the author, notifying him that the machine is infected.

Category 14.3 Virus/worms

2004-02-18 **Netsky worm virus network Internet variant warning Netsky.B**

DHS IAIP Daily;
http://www.computerworld.com/securitytopics/security/virus/story/0,10801,9026
4,00.html

Experts warn of new NetSky worm variant.

Anti-virus software companies are warning that a new version of the NetSky e-mail worm is circulating on the Internet. NetSky.B, also known as Moodown.B, first appeared Wednesday, February 18, and is spreading through infected e-mail messages and shared network folders. Once installed, NetSky tries to disable antivirus software, steal e-mail addresses and copy itself to shared network folders, anti-virus companies said. The new worm is a modified version of NetSky.A, which appeared on Monday. Like its predecessor, NetSky.B arrives in e-mail messages that have randomly generated subject lines such as "something for you," "hello" or "fake." The worm file is contained in a zipped attachment that also has a randomly generated name and file type such as "document" "stuff" or "party." Most copies of the worm appear to be coming from the Netherlands and elsewhere in Europe. Users are advised to update their anti-virus software as soon as possible.

Category 14.3 Virus/worms

2004-02-18 **Netsky worm virus network Internet variant warning Netsky.B**

DHS IAIP Daily;
http://www.computerworld.com/securitytopics/security/virus/story/0,10801,9026
4,00.html

February 18, Federal Computer Week — Experts warn of new NetSky worm variant.

Anti-virus software companies are warning that a new version of the NetSky e-mail worm is circulating on the Internet. NetSky.B, also known as Moodown.B, first appeared Wednesday, February 18, and is spreading through infected e-mail messages and shared network folders. Once installed, NetSky tries to disable antivirus software, steal e-mail addresses and copy itself to shared network folders, anti-virus companies said. The new worm is a modified version of NetSky.A, which appeared on Monday. Like its predecessor, NetSky.B arrives in e-mail messages that have randomly generated subject lines such as "something for you," "hello" or "fake." The worm file is contained in a zipped attachment that also has a randomly generated name and file type such as "document" "stuff" or "party." Most copies of the worm appear to be coming from the Netherlands and elsewhere in Europe. Users are advised to update their anti-virus software as soon as possible.

Category 14.3 *Virus/worms*

2004-02-26 **Netsky new virus worm variation pornography hacking MP3 deception social engineering**

DHS IAIP Daily; http://www.web−user.co.uk/news/48008.html

February 26, Webuser (UK) — New version of Netsky worm appears.

A new version of the Netsky worm has been detected that snares internet users by disguising itself as pornography or documents about hacking or MP3s. Once one of these files is opened, the Netsky.C infects the user's computer and sends a copy of itself to e-mail addresses on the infected computer. It can also spread via file sharing networks such as Kazaa and the ICQ chat system. According to security experts, Netsky.C is similar to its predecessor Netsky.B as both spread by e-mail and file sharing networks. When it spreads via e-mail it selects random names for the subject line and file name. When first run, Netsky.C copies itself to the Windows folder as winlogon.exe and creates the following registry entry: HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ICQNet= \winlogon.exe -stealth', so that winlogon.exe is run automatically each time Windows is started. Netsky.C also copies itself to folders on drives C to Z whose name contains the sequence of letters 'Shar', this includes shared folders and explains how it spreads through P2P file sharing where users download from each others' shared folders.

Category 14.3 *Virus/worms*

2004-05-12 **worm virus malicious code malware Microsoft Windows media player vulnerability Wallon**

DHS IAIP Daily; http://news.zdnet.co.uk/0,39020330,39154533,00.htm

May 12, ZDNet (UK) — Wallon virus wrecks Windows Media Player.

A new mass-mailing virus called Wallon was discovered in Europe on Tuesday, May 11. Maikel Albrecht of security company F-Secure said that because of recent virus outbreaks, users are less willing to open e-mail attachments, which is why Wallon's author is counting on users clicking on an e-mail link instead. "The link in the email points to the actual virus, so if you click the link you download the virus," said Albrecht. However, once the PC is infected, Wallon remains dormant until the user tries to run a media file such as an MP3 or a video. If by default the system uses Windows Media Player, the virus is activated and attempts to send HTML emails, each with a link to the virus file, to any email addresses in the computer's address book. Wallon requires intervention by the user before it can replicate, so Albrecht expects it will not spread very quickly. But unlike common viruses, Wallon is destructive because it replaces the wmplayer.exe file, which means that users infected by the worm will need to reinstall Media Player. Stuart Okin of Microsoft UK said anyone worried about Wallon should install Microsoft's MS04-13 patch, which was released in mid-April and solves the problem.

Category 14.3 *Virus/worms*

2004-06-18 **Sasser worm creator writer interview Germany**

NewsScan

SASSER CREATOR INTERVIEWED

In an interview with the German magazine Stern, Sven Jaschan, the author of the Sasser worm that hit Windows users at the beginning of last month, says it was one of his friends who tipped off Microsoft in an attempt to claim a reward. (The friend is now also under suspicion for his involvement with writing and distributing the virus, and Microsoft has indicated there will be no reward.) Jaschan says he inserted into Sasser a piece of code he found on the Internet that "malfunctioned" and caused PCs to reboot. He claims this was not his intention, and that he was
"thoughtless" in not considering the consequences or the damage his worm would cause. (The Age 18 Jun 2004) Rec'd from John Lamp, Deakin U.

Category 14.3 *Virus/worms*

2005-08-19 **denial of service DoS virus failure backup systems business continuity**

RISKS 24 02

US CUSTOMS COMPUTERS FALL TO VIRUS INFECTION

A U.S. Customs database system in Virginia shut down for about 5.5 hours beginning around 6pm on 18 August. The system is used to process incoming international air passengers, but its absence caused havoc at Miami International Airport, where up to 2000 people were waiting to clear immigration. Airports in the NYC area were able to use backup systems. The cause was subsequently blamed on a virus.

[Abstract by Peter G. Neumann]

Category 14.3 Virus/worms

2005-09-22 **US-CERT malware virus worm Trojan horse naming plan obstacles**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1862251,00.asp

US-CERT MALWARE NAMING PLAN FACES OBSTACLES

US-CERT, the U.S. Computer Emergency Readiness Team, will begin issuing uniform names for computer viruses, worms, and other malicious code next month, as part of a program called the Common Malware Enumeration initiative. The program is intended to clear up confusion that results from the current decentralized system for naming Internet threats, which often results in the same virus or worm receiving different names from different anti-virus vendors. New malicious code samples are held for two hours and, if no other example of the new code is submitted, assigned a CME number.

Category 14.3 Virus/worms

2005-10-06 **Common Malware Enumeration CME taxonomy disagreement security experts malicious software**

EDUPAGE; http://news.com.com/2100-7348_3-5890038.html

MALWARE NAMING SCHEME PROMPTS DISAGREEMENT

Security experts are of two minds concerning the release of a scheme to provide common names for malicious software. The Common Malware Enumeration (CME) system is designed to eliminate the confusion that often arises when a new piece of malware begins circulating the Internet. As different security companies identify the code, they typically assign different names, causing confusion among computer users as to whether there are multiple threats that need to be addressed or simply one new threat with several names. Starting with the most common and damaging pieces of malware, CME will assign a unique number to each. Trend Micro's David Perry criticized the program for not covering all malware, however. He also said the scheme won't provide any benefit for consumers. His comments were echoed by IBM's Martin Overton, who said CME will make matters worse, and by Boeing's Jeanette Jarvis. Graham Cluley of Sophos, on the other hand, applauded the new system. Larry Bridwell, content security programs manager for security watchdog ICSA, also supports the naming scheme, calling it a good first step and pointing out that it was "never designed to solve the naming problem" but rather to serve "as an index." CNET, 6 October 2005

Category 14.3 Virus/worms

2005-10-06 **Vnunet Security virus US CERT Internet worms threats CME malware CVE**

DHS IAIP Daily; http://www.vnunet.com/vnunet/news/2143314/security−
industry− gathers

SECURITY INDUSTRY ADOPTS UNIFORM VIRUS NAMES

The US Computer Emergency Readiness Team (US-CERT) has kicked of an initiative to create common names for Internet worms and threats. Common Malware Enumeration (CME) aims to reduce confusion with the public caused by disparate naming schemes for Internet threats. Currently Internet worms are often named using information about the virus or a follow a description the author entered when crafting the malware. The new scheme will use a sequential CME number, beginning with CME-1. A similar naming system already exists for security vulnerabilities in software, which uses a Common Vulnerability and Exposure (CVE) identifier. However, CME differs from CVE in that the worm naming initiative will not include the date.

Category 14.3 *Virus/worms*

2005-10-26 **Zotob damage businesses worm Cybertrust Internet vulnerabilities Nimba MSBlast Windows**

DHS IAIP Daily;
http://news.com.com/Zotob+damage+deep+but+not+widespread/2100−7355_3−5915591.html?tag=nefd.top

ZOTOB DAMAGE DEEP BUT NOT WIDESPREAD

Fewer businesses fell victim to the Zotob worm that struck corporate networks in August than previous attacks, according to a report released on Wednesday, October 26, by computer security firm Cybertrust. Of 700 organizations surveyed, 13 percent were disrupted by the worm. Six percent of survey respondents said Zotob's impact on their company was moderate to major, which was defined as more than $10,000 in losses and at least one major business system affected, such as e-mail or Internet connectivity. According to the study, Zotob did far less damage than did other major worms designed to exploit Windows vulnerabilities. For example, the Nimda and 8 MSBlast worm made a moderate to major impact on 60 percent and 30 percent of companies, respectively. Zotob was less widespread, in part, because it targeted only PCs running Windows 2000. The worm exploited a hole in the operating system's plug-and-play feature, and let attackers take control of infected machines. Twenty-six percent of Zotob victims noted that infections occurred because they had no firewall in place. The health care industry was hit hardest, with more than a quarter of that sector's organizations reporting some impact. Cybertrust report: http://www.cybertrust.com/pr_events/2005/20051026.shtml

---

Category 14.3 *Virus/worms*

2006-02-03 **no expected Kama Sutra worm damage McAfee F-Secure comments**

EDUPAGE; http://news.com.com/2100-7349_3-6034706.html 23

EXPECTED DAMAGE FROM KAMA SUTRA WORM DOESN'T MATERIALIZE

The latest high-profile worm making the rounds on the Internet has so far failed to unleash the damage that some had predicted. The Kama Sutra worm, also known as Nyxem.E, MyWife, and Blackworm, was scheduled to attack infected computers on Friday and begin deleting files and causing other headaches for users. However, Paul Ducklin, head of technology at Sophos Asia-Pacific, said there have been no reports of problems so far. Ducklin attributed the lack of consequence to effective efforts by businesses to identify the worm and keep computers from becoming infected. Allan Bell, marketing director for McAfee, echoed Ducklin's remarks. "No local outbreaks reported," he said, "and very few reports of infections." F-Secure's Mikko Hypponen noted, however, that home users are typically much less aware of security threats and therefore much more widely affected by such worms. "The full scope of the problem won't come to light until during the weekend or early next week," he said, when home users turn on their computers.

Category 14.3 *Virus/worms*

2006-04-17 **Bagle virus attack computer infection worm F-Secure report**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1950098,00.asp 23

NEW ATTACK IS AIMED AT COMPUTERS INFECTED WITH BAGLE VIRUS.

A new attack aimed at computers infected with the Bagle virus threatens to generate scads of spam e-mail campaigns, and anti-malware experts concede that the threat remains a major headache. Researchers at anti-virus specialist F-Secure, based in Helsinki, Finland, described the attack, dubbed "SpamTool.Win32.Bagle.g," and said it involves a new set of URLs being sent to machines infected with Bagle. The variant is meant to use the computers to launch waves of spam messages and involves a download link that provides a new, uniquely repacked version of the attempted spam execution every 50 seconds or so, according to F-Secure. The new attack involved at least five different URLs used to distribute the new SpamTool execution, at least four of which have already been shut down, F-Secure said.

14.4 Trojans & rootkits

Category 14.4 *Trojans & rootkits*

1997-04-29 **Trojan AOL**

EDUPAGE

The Department of Energy's Computer Incident Advisory Capability (CIAC) warned users not to fall prey to the AOL4FREE.COM Trojan, which tries to erase files on hard drives when it is run. A couple of months later, the NCSA worked with AOL technical staff to issue a press release listing the many names of additional Trojans; these run as TSRs (Terminate - Stay Resident programs) and capture user IDs and passwords, then send them by e-mail to Bad People. Reminder: do NOT open binary attachments at all from people you don't know; scan all attachments from people you do know with anti-virus and anti-Trojan programs before opening.

Category 14.4 *Trojans & rootkits*

1997-07-31 **AOL Trojan Horse**

Reuters, Newsbytes

AOL announced its "Download Sentry" to warn its naïve users about the dangers of executing binary file attachments that may contain Trojans. Recently AOL has been plagued by attachments that act as keystroke-capture programs and e-mail user IDs and passwords to criminals for fraudulent access to the network.

Category 14.4 *Trojans & rootkits*

1997-11-06 **phone fraud web pornography Trojan**

RISKS, EDUPAGE, news wires 18 80 ff

MOLDOVAN TROJAN
Viewers of pornographic pictures on the sexygirls.com site were in for a surprise when they got their next phone bills. Toronto victims who downloaded a "special viewer" were actually installing a Trojan program that silently disconnected their connection to their normal ISP and reconnected them (with the modem speaker turned off) to a number in Moldova in central Europe. The long-distance charges then ratcheted up until the user disconnected the session — sometimes hours later, even when the victims switched to other, perhaps less prurient, sites. The same fraud was reported in Feb in New York City, where a federal judge ordered the scam shut down. An interesting note is that AT&T staff spotted the scam because of unusually high volume of traffic to Moldova, not usually a destination for many US phone calls. In November, the FTC won $2.74M from the bandits to refund to the cheated customers.

Category 14.4 *Trojans & rootkits*

1998-01-05 **Trojans ISP criminal hackers naïve gullible trusting theft**

Wall Street Journal

Jared Sandberg, writing in the Wall Street Journal, reported on widespread fraud directed against naïve AOL users using widely-distributed Trojan Horse programs ("proggies") that allow them to steal passwords. Another favorite trick that fools gullible users is the old "We need your password" popup that claims to be from AOL administrators. AOL reminds everyone that no one from AOL will ever ask users for their passwords.

Category 14.4 *Trojans & rootkits*

1999-01-29 **Trojan horse backdoor quality assurance QA**

RISKS 20 18

Peter Neumann summarized a serious case of software contamination in RISKS 20.18: At least 52 computer systems downloaded a TCP wrapper program directly from a distribution site after the program had been contaminated with a Trojan horse early in the morning of 21 Jan 1999. The Trojan horse provided trapdoor access to each of the contaminated systems, and also sent e-mail identifying each system that had just been contaminated. The 52 primary sites were notified by the CERT at CMU after the problem had been detected and fixed. Secondary downloads may also have occurred."

Category 14.4 *Trojans & rootkits*

1999-02-12 **QA quality assurance auditing Y2K consultants fraud embezzle**

RISKS 20 21

Bruce Martin pointed out in RISKS that the frantic efforts to remediate the Y2K bugs in production software offer a perfect cover for criminals to insert Trojan code in financial software. Such Trojans could, for example, cause monetary transfers around the Y2K transition out of clients' accounts to the criminals' accounts in offshore banks. The expected confusion at the end of 1999 could cause serious difficulties for auditors as they tried to piece together the reasons for various losses experienced at the turn of the century.

Category 14.4 *Trojans & rootkits*

1999-05-11 **virus Trojan e-mail**

South China Morning Post (Hong Kong)

In May 1999, reports surfaced of a Chinese Trojan called picture.exe that had been circulating widely in China since December 1998. The program, also known as manager.exe, was circulated via an e-mail vector and would send infected-system configuration data to e-mail addresses in the PRC.

Category 14.4 *Trojans & rootkits*

1999-05-28 **Trojan back door malicious code spam attachment**

MSNBC

Network Associates Inc. anti-virus labs warned of a new Trojan called BackDoor-G being sent around the Net as spam in May. Users were tricked into installing "screen savers" that were nothing of the sort. The Trojan resembled the previous year's Back Orifice program in providing remote administration — and back doors for criminals to infiltrate a system. A variant called "Armageddon" appeared within days in France.

Category 14.4 *Trojans & rootkits*

1999-06-11 **virus e-mail attachment Windows worm executable**

Wall Street Journal

The Worm.Explore.Zip (aka "Trojan Explore.Zip) worm appeared in June as an attachment to e-mail masquerading as an innocuous compressed WinZIP file. The executable file used the icon from WinZIP to fool people into double-clicking it, at which time it began destroying files on disk. Within a week of its discovery in Israel on the 6th of June the worm had spread to more than 12 countries. Network Associates reported that ~70% of its largest 500 corporate customers were infected. [Readers should remember that the larger the number of computers in a company, the more likely that at least one will be infected even when infection rates are low. If the probability of infecting one system is "p" and there are "n" targets in a group each of which can be infected independently, the likelihood of at least one infection in the group is P = {1 - (1 - p)^n} which rises rapidly as n increases.]

Category 14.4 *Trojans & rootkits*

1999-09-20 **virus worm Trojan e-mail Y2K countdown clock fix Internet passwords**

San Francisco Chronicle

A couple of new Y2K-related virus/worms packaged as Trojan Horses were discovered in September. One e-mail Trojan called "Y2Kcount.exe" claimed that its attachment was a Y2K-countdown clock; actually it also sent user IDs and passwords out into the Net by e-mail. Microsoft reported finding eight different versions of the e-mail in circulation on the Net. The other, named "W32/Fix2001" came as an attachment ostensibly from the system administrator and urged the victims to install the "fix" to prevent Internet problems around the Y2K transition. Actually, the virus/worm would replicate through attachments to all outbound e-mail messages from the infected system. [These malicious programs are called "virus/worms" because they integrate into the operating system (i.e., they are virus-like) but also replicate through networks via e-mail (i.e., they are worm-like).]

Category 14.4 *Trojans & rootkits*

2000-01-02 **Trojan e-mail password stealer**

SecurityPortal.com (reprinted with permission), Symantec
http://www.symantec.com/avcenter/venc/data/pwsteal.trojan.html

PWSteal.Trojan is a Trojan which attempts to steal login names and passwords. These passwords are often sent to an anonymous email address. Symantec: PWSteal.Trojan Virus

---

Category 14.4 Trojans & rootkits

2000-01-03 **Trojan operating system corruption damage**

SecurityPortal.com (reprinted with permission),
http://securityportal.com/topnews/finjan19991229.html

Finjan Software Blocks Win32.Crypto the First Time: Finjan Software, Inc. announced that its proactive first-strike security solution, SurfinShield Corporate, blocks the new Win32.Crypto malicious code attack. Win32.Crypto, a Trojan executable program released in the wild today, is unique in that infected computers become dependant on the Trojan as a "middle-man" in the operating system. Any attempt to disinfect it will result in the collapse of the operating system itself. It is a new kind of attack with particularly damaging consequences because attempting to remove the infection may render the computer useless and force a user to rebuild their system from scratch.

Category 14.4 Trojans & rootkits

2000-08-29 **Trojan mobile computers palmtop**

NewsScan, New York Times
http://partners.nytimes.com/library/tech/00/08/biztech/articles/30palm-virus.html

Software companies . . . reported that the first . . . [malware] to target the Palm operating system has been discovered. The bug, which uses a "Trojan horse" strategy to infect its victims, comes disguised as pirated software purported to emulate a Nintendo Gameboy on Palm PDAs and then proceeds to delete applications on the device. The . . . [malware] does not pose a significant threat to most users, says Gene Hodges, president of Network Associates' McAfee division, but signals a new era in technological vulnerability: "This is the beginning of yet another phase in the war against hackers and virus writers. In fact, the real significance of this latest Trojan discovery is the proof of concept that it represents." (Agence France Presse/New York Times 29 Aug 2000)

Category 14.4 Trojans & rootkits

2000-10-27 **criminal hacker Trojan horse passwords e-mail industrial espionage source code penetration**

NewsScan, Associated Press, New York Times
http://partners.nytimes.com/2000/10/27/technology/27WIRE-MSHACK.html ,
Washington Post http://washingtonpost.com/wp-dyn/articles/A40244-2000Oct30.html

Microsoft's internal computer network was invaded by the QAZ "Trojan horse" software that caused company passwords to be sent to an e-mail address in St. Petersburg, Russia. Calling the act "a deplorable act of industrial espionage," Microsoft would not say whether or not the hackers may have gotten hold of any Microsoft source code. (AP/New York Times 27 Oct 2000)

However, within a few days, Microsoft . . . [said] that network vandals were able to invade the company's internal network for only 12 days (rather than 5 weeks, as it had originally reported), and that no major corporate secrets were stolen. Microsoft executive Rick Miller said: "We started seeing these new accounts being created, but that could be an anomaly of the system. After a day, we realized it was someone hacking into the system." At that point Microsoft began monitoring the illegal break-in, and reported it to the FBI. Miller said that, because of the immense size of the source code files, it was unlikely that the invaders would have been able to copy them. (AP/Washington Post 30 Oct 2000)

Category 14.4 Trojans & rootkits

2002-01-19 **Trojan horse back door porn fraud scumware**

RISKS 21 87

A patch for a vulnerability in the AOL Instant Messenger (AIM) program was converted into a Trojan horse that initiated unauthorized click-throughs on advertising icons, divulged system information to third parties and browsed to porn sites.

Category 14.4 Trojans & rootkits

2002-03-11 **Trojan horse executable attachment patch social engineering worm**

RISKS 21 94

The "Gibe" worm was circulated in March 2002 as a 160KB EXE file attached to a cover message pretending to be a Microsoft alert explaining that the file was a "cumulative patch" and pointing vaguely to a Microsoft security site. Going to the site showed no sign of any such patch, nor was there a digital signature for the file. However, naive recipients were susceptible to the trick.

[MORAL: keep warning recipients not to open unsolicited attachments in e-mail.]

Category 14.4 *Trojans & rootkits*

2002-04-03 **P2P peer-to-peer Trojan distributed computing storage EULA end-user license agreement**

RISKS, http://news.com.com/2100-1023-873181.html 22 02

Nicholas C. Weaver warned in RISKS that the company Brilliant Digital (BD) formally announced distribution of Trojan software via the Kazaa peer-to-peer network software. The BD software would create a P2P server network to be used for distributed storage, computation and communication -- all of which would pose serious security risks to everyone concerned. Weaver pointed out that today's naïve users appear to be ready to agree to anything at all that is included in a license agreement, whether it is in their interests or not.

Category 14.4 *Trojans & rootkits*

2002-05-20 **Java Scrip Trojan HTML Web page e-mail data corruption integrity**

Security Wire Digest 4 39

MALICIOUS PORN ADS STALK USERS
Antivirus experts say users no longer need to be concerned about JS.Fortnight, a Java Script Trojan that was embedded in a now-defunct Web page. Upon visiting that site, a user's Outlook Express signature would be modified to include a link back to the porn site in every message sent.

Category 14.4 *Trojans & rootkits*

2003-02-14 **Trojan horse social engineering pornography**

NewsScan

'REVEALING' CELEBRITIES PHOTOS USED FOR TROJAN HORSE
E-mail purporting to offer revealing photos of Catherine Zeta-Jones, Britney Spears, and other celebrities is actually offering something quite different: the secret installation of Trojan horse software that can be used by intruders to take over your computer. Users of the Kazaa file-sharing service and IRC instant messaging are at risk. (Reuters/USA Today 14 Feb 2003)

Category 14.4 *Trojans & rootkits*

2003-05-22 **Kaspersky labs trojan internet explorer startpage vulnerability automatic send function java script executes**

NIPC/DHS

May 22, ITWEB — New Trojan exploits known Internet Explorer vulnerability.

Data security software developer Kaspersky Labs reports that a new Trojan program, StartPage, is exploiting an Internet Explorer vulnerability for which there is no patch. If a patch is not released soon, other viruses could exploit the vulnerability. StartPage is sent to victim addresses directly from the author and does not have an automatic send function. The program is a Zip-archive that contains an HTML file. Upon opening the HTML file, an embedded Java-script is launched that exploits the "Exploit.SelfExecHtml" vulnerability and clandestinely executes an embedded EXE file carrying the Trojan program.

Category 14.4 *Trojans & rootkits*

2003-07-14 **porn ads 2000 windows-based computers hijacked Migmaf Migrant Mafia trojan spam website Network Associate's**

NIPC/DHS; http://www.lurhq.com/migmaf.html

July 14, Reuters — Program hijacks PCs to send porn ads.

Close to 2,000 Windows-based PCs with high-speed Internet connections have been hijacked by a stealth program and are being used to send ads for pornography, computer security experts warned. It is unknown exactly how the trojan (dubbed "Migmaf" for "migrant Mafia") is spreading to victim computers around the world, whose owners most likely have no idea what is happening, said Richard M. Smith, a security consultant in Boston. The trojan turns the victim computer into a proxy server which serves as a middle man between people clicking on porn e-mail spam or Web site links, according to Smith. The victim computer acts as a "front" to the porn Web site, enabling the porn Web servers to hide their location, Smith said. Broadband Internet users should always use firewalls to block such stealth activity, he said. Computers with updated anti-virus software will also be protected, said Lisa Smith of network security company Network Associate's.

Category 14.4 Trojans & rootkits

2003-11-11 **Linux kernel back door source code open source software operating system security**

RISKS; http://kerneltrap.org/node/view/1584; 23 2
http://www.smh.com.au/articles/2003/11/07/1068013371170.html

Thwarted Linux backdoor

Douglas W. Jones discusses an attempt by a hacker to insert a back door into the Linux kernel. Somone broke into a kernel.kbits.net server and inserted code for a backdoor into the sys_wait4() function--if allowed to run, this code would a hacker root privileges surreptitiously. The attack was discovered by a group of experienced Linux programmers. Mr. Jones feels that this important attack has not received the publicity it deserves.

Category 14.4 Trojans & rootkits

2004-01-08 **Trojan horse malicious agent back door HTML**

NIPC/DHS; http://www.esecurityplanet.com/alerts/article.php/3295891

January 06, esecurityplanet.com — Trojan sends spammed message with woman's picture.

BackDoor-AWQ.b is a remote access Trojan written in Borland Delphi, according to McAfee, which issued an alert Tuesday, January 6. An email message constructed to download and execute the Trojan is known to have been spammed to users. The spammed message is constructed in HTML format. It is likely to have a random subject line, and its body is likely to bear a head portrait of a lady (loaded from a remote server upon viewing the message). The body contains HTML tags to load a second file from a remote server. This file is MIME, and contains the remote access Trojan (base64 encoded). Upon execution, the Trojan installs itself into the %SysDir% directory as GRAYPIGEON.EXE. A DLL file is extracted and also copied to this directory (where %Sysdir% is the Windows System directory, for example C:\WINNT\SYSTEM32) The following Registry key is added to hook system startup: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion \RunOnce "ScanRegedit" = "%SysDir%\GRAYPIGEON.EXE" The DLL file (which contains the backdoor functionality) is injected into the EXPLORER.EXE process on the victim machine. More information, including removal instructions, can be found at: http://us.mcafee.com/virusInfo/default.asp?id=description &virus_k=100938

Category 14.4 Trojans & rootkits

2004-01-09 **malware Microsoft trojan horse Windows Update social engineering swen Xombe Dloader-L**

NewsBits; http://www.gcn.com/vol1_no1/daily-updates/24599-1.html
http://computerworld.com/securitytopics/security/story/0,10801,88940,0

New malware masquerades as Microsoft update

A Trojan horse program that appears to be a Microsoft Corp. security update can download malicious code from a remote Web site and install a back door on the compromised computer, leaving it vulnerable to remote control. Idefense Inc., a Reston, Va., computer security company, said the malicious code is the latest example of so-called social engineering to fool Windows users. It is similar to the W32Swen worm, which last year passed itself off as a Microsoft patch.

Category 14.4 Trojans & rootkits

2004-01-12 **Trojan horse malware spoofing masquerade Microsoft update**

NIPC/DHS; http://www.gcn.com/vol1_no1/daily−updates/24599−1.html

January 09, Government Computer News — New malware masquerades as Microsoft update.

A Trojan horse program that appears to be a Microsoft security update can download malicious code from a remote Web site and install a back door on the compromised computer, leaving it vulnerable to remote control. IDefense Inc., computer security company, said the malicious code is the latest example of so-called social engineering to fool Windows users. It is similar to the W32Swen worm, which last year passed itself off as a Microsoft patch. "The success of Swen in 2003 encouraged virus writers to put effort into creating official-looking e-mails and Web sites," said Ken Dunham, director of malicious code for iDefense. The Trojan arrives as an attachment to an e-mail that appears to be from Windowsupdate@microsoft.com. The subject line says, "Windows XP Service Pack (Express)-Critical Update." The message describes the attachment, WinxpSp1.A, as a cumulative patch that corrects security flaws in versions of Microsoft Internet Explorer, Outlook and Outlook Express. It downloads an executable file that will open a TCP port to listen for remote commands from the attacker.

Category 14.4 *Trojans & rootkits*

2004-03-17 **Trojan horse peer-to-peer P2P software threat Phatbot disable antivirus**

NewsScan

THE PHATBOT TROJAN

The U.S. Department of Homeland Security has alerted computer security experts about the Phatbot Trojan, which snoops for passwords on infected computers and tries to disable firewall and antivirus software. Phatbot . . . Has proved difficult for law enforcement authorities and antivirus companies to fight.... Mikko Hypponen, director of the antivirus software company F-Secure in Finland says, "With these P2P Trojan networks, even if you take down half of the affected machines, the rest of the network continues to work just fine"; security expert Russ Cooper of TruSecure warns, "If there are indeed hundreds of thousands of computers infected with Phatbot, U.S. e-commerce is in serious threat of being massively attacked by whoever owns these networks." (Washington Post 17 Mar 2004)

Category 14.4 *Trojans & rootkits*

2004-05-12 **bot zombie Trojan Horse malicious code phatbot**

DHS IAIP Daily;
http://www.theregister.co.uk/2004/05/12/phatbot_zombie_trade /

May 12, The Register — Phatbot arrest throws open trade in zombie PCs.

The arrest of the suspected author of the Phatbot Trojan Friday, May 7, in the southern German state of Baden-Wuerttemberg could lead to valuable clues about the illicit trade in zombie PCs. The arrest was overshadowed by the unmasking of the admitted Sasser author. But the Phatbot case may shed the most light into the dark recesses of the computer underground. Phatbot is much less common than NetSky but is linked much more closely with the trade in compromised PCs to send spam or for other nefarious purposes. Viruses such as MyDoom and Bagle (and Trojans such as Phatbot) surrender the control of infected PCs to hackers. This expanding network of infected, zombie PCs can be used either for spam distribution or as platforms for DDoS attacks, such as those that many online bookies have suffered in recent months. By using compromised machines-instead of open mail relays or unscrupulous hosts-spammers can bypass IP address blacklists. Phatbot is a variant of Agobot, a big family of IRC bots. Networks of compromised hosts (BotNets) are commonly traded between virus writers, spammers and middlemen over IRC networks. The price of these BotNets (DoSNets) was roughly $500 for 10,000 hosts last summer when the MyDoom and Blaster (the RPC exploit worm) first appeared on the scene.

Category 14.4 *Trojans & rootkits*

2004-05-12 **Trojan Horse Mac Apple Applescript**

DHS IAIP Daily;
http://www.macworld.co.uk/news/top_news_item.cfm?NewsID=8665

May 12, Macworld — Trojan is attacking Macs.

Intego has identified a Trojan horse -- AS.MW2004.Trojan -- that affects Mac OS X. This Trojan horse, when double-clicked, permanently deletes all the files in the current user's home folder. Intego has notified Apple, Microsoft and the CERT, and has been working in close collaboration with these companies and organizations. The AS.MW2004.Trojan is a compiled AppleScript applet, a 108 KB self-contained application, with an icon resembling an installer for Microsoft Office 2004 for Mac OS X. This AppleScript runs a Unix command that removes files, using AppleScript's ability to run such commands. The AppleScript displays no messages, dialogs or alerts. Once the user double-clicks this file, their home folder and all its contents are deleted permanently. All Macintosh users should only download and run applications from trusted sources.

Category 14.4 *Trojans & rootkits*

2004-05-18 **worms Trojans blended threats kibuv bobax**

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1594860,00.asp

May 18, eWeek — Kibuv worm, Bobax Trojan try many methods.

Security experts are tracking two new threats that have emerged in the past few days, including a worm that uses seven mechanisms to spread itself. The worm is known as Kibuv, and researchers first noticed its presence Friday, May 14. Kibuv affects all versions of Windows from 98 through Windows Server 2003 and attempts to spread through a variety of methods, including exploiting five Windows vulnerabilities and connecting to the FTP server installed by the Sasser worms. The worm has not spread too widely as of yet, but with its variety of infection methods, experts say the potential exists for it to infect a large number of machines. The second piece of malware that has surfaced is a Trojan that is capable of spreading semi-automatically. Known as Bobax, the Trojan can only infect machines running Windows XP and seems to exist solely for the purpose of sending out large amounts of spam. When ordered to scan for new machines to infect, Bobax spawns 128 threads and begins scanning for PCs with TCP port 5000 open. If the port is open, it exploits the Windows LSASS vulnerability. Bobax then loads a copy of itself onto the new PC, and the process repeats. Antivirus and antispam providers say they have seen just a few machines infected with Bobax as of Tuesday, May 18.

Category 14.4 *Trojans & rootkits*

2004-05-20 **Trojan Horse financial services identity theft online banking**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/story/0,10801,93281,00.html

May 20, Computerworld — Canadian online banking users fall victim to Trojan.

A Trojan horse may be responsible for an online banking scam that has cost at least two Winnipeg, Canada, customers thousands of dollars. The Winnipeg Police Service is investigating two cases where money was transferred unknowingly from bank accounts. The investigation is focused around a man who recently emigrated to Canada from an unidentified locale in Eastern Europe. According to computer security experts, online banking scams and identity theft are proliferating in Canada. While Canadian e-banking customers have yet to see a surge in identity theft similar to the U.S., the banks say the onus is on consumers and enterprises to protect themselves. Keystroke loggers are the most frequently used tactic for crooks targeting banking information, said Tom Slodichak, chief security officer of WhiteHat, an IT security provider. "Although a Web session with their financial institution is usually encrypted, the keystroke logger intercepts the keystrokes before any encryption occurs, so they will get all the information--the account numbers, the names, the passwords or PINs or whatever they need to impersonate that [individual]," he said.

Category 14.4 *Trojans & rootkits*

2004-06-29 **network vandals banking information keylogger Trojans**

NewsScan

NETWORK VANDALS WANT TO BANK WITH YOU

Computer security experts are issuing warnings that network vandals hope to steal the password and account information of online bank accounts by secretly downloading spy software to capture a PC user's keystroke activity. The problem is not widespread, but Internet Explorer users are being advised to set the security setting for their browsers to "high" (a level which, however, makes it more difficult to interact with some Web sites). (Washington Post 29 Jun 2004)

Category 14.4 *Trojans & rootkits*

2004-08-10 **Trojan Horse malicious code peer-to-peer P2P networks Windows Pocket PC Symbian smartphone attack**

DHS IAIP Daily; http://www.theregister.co.uk/2004/08/10/mosquitos_trojaned/

August 10, The Register — Trojan dialler afflicts Symbian smartphones.

Malicious code that dials premium rate numbers without a user's consent has been found in a pirated version of Mosquitos 2.0, a popular game for Symbian Series 60 smartphones. The illicit copies of the game are circulating over P2P networks. News of the Symbian Trojan dialler comes days after the arrival of the first Trojan for handheld computers running Windows Pocket PC operating system, Brador-A.

Category 14.4 Trojans & rootkits

2004-10-25 **Red Hat Linux patch malicious hoax e-mail SANS message**

DHS IAIP Daily; http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1019189,00.html

October 25, SearchSecurity — Red Hat Linux patch update a malicious hoax.

An e-mail disguised as a Red Hat patch update is a fake designed to trick users into downloading malware designed to compromise the systems they run on, the Linux vendor warned in a message on its Website. While the malicious site was taken down over the weekend, the SANS Internet Storm Center posted a message on its Website saying the hoax "is a good reminder that even though most of these are aimed at Windows users, always be suspect when receiving an e-mail asking you to download something."

Category 14.4 Trojans & rootkits

2004-11-23 **trojan mobile phones skulls Nokia Symbian vandalism denial-of-service attack**

NewsScan; http://www.enn.ie/news.html?code=9566568

TROJAN HORSE AIMED AT NOKIA CELL PHONES

A new attack by Trojan Horse software known as "Skulls" targets Nokia 7610 cell phones, rendering infected handsets almost useless. The program appears to be a "theme manager" for the phone. It replaces most of an infected phone's program icons with images of skulls and crossbones, and disables all of the default programs on the phone (calendar, phonebook, camera, Web browser, SMS applications, etc.) -- i.e., essentially everything except normal phone calls. Symbian, the maker of the Nokia 7610 operating system, says that users will only be affected if they knowingly and deliberately install the file and ignore the warnings that the phone displays at the conclusion of the installation process. Experts don't consider the Skulls malware to be a major threat, but note that it's the third mobile phone bug to appear this year -- and therefore probably means that this kind of problem is here for the foreseeable future. (ENN Electronic News.net 23 Nov 2004)

Category 14.4 Trojans & rootkits

2005-01-13 **cellery worm malware tetris bandwidth saturation denial-of-service DoS trojan**

NewsScan; http://news.bbc.co.uk/1/hi/technology/4170903.stm

CELLERY WORM PLAYS GAMES WITH VICTIMS

Users are being warned about the Cellery worm -- a Windows virus that piggybacks on the hugely popular Tetris game. Rather than spreading itself via e-mail, Cellery installs a playable version of Tetris on the user's machine. When the game starts up, the worm seeks out other computers it can infect on the same network. The virus does no damage, but could result in clogged traffic on heavily infected networks. "If your company has a culture of allowing games to be played in the office, your staff may believe this is simply a new game that has been installed -- rather than something that should cause concern," says a spokesman for computer security firm Sophos. (BBC News 13 Jan 2005)

Category 14.4 Trojans & rootkits

2005-01-24 **Trojan Horse program Symbian based phone harm useless Bluetooth reuse restore factory settings**

DHS IAIP Daily; http://www.pcworld.com/news/article/0,aid,119392,00.asp

NEW TROJAN HORSE PROGRAMS WILL RENDER SOME SYMBIAN-BASED MOBILE PHONES USELESS

Two new Trojan horse programs, Gavno.a and Gavno.b, masquerade as patch files designed to trick users into downloading them, says Aaron Davidson, chief executive officer of SimWorks International. Although almost identical with Gavno.a, Gavno.b contains the Cabir worm, which attempts to send a copy of the Trojan horse to other nearby Symbian-based phones via short-range wireless Bluetooth technology. The Gavno Trojans, according to Davidson, are the first to aim at disrupting a core function of mobile phones--telephony--in addition to other applications such as text messaging, e-mail, and address books. Gavno.a and Gavno.b are proof-of-concept Trojan horses that "are not yet in the wild," Davidson says. Davidson believes the Trojan programs originated in Russia. To fix infected phones, users will need to restore them to their factory settings.

Category 14.4 *Trojans & rootkits*

2005-02-11 **Microsoft anti-spyware trojan attack information warfare disable interfere confidentiality data theft key logging e-mail attachment**

NewsScan; http://theage.com.au/articles/2005/02/11/1108061848064.html

MICROSOFT PROBES SPYWARE ATTACK

Microsoft Corp is investigating a malicious program that attempts to turn off the company's newly released anti-spyware software for Windows computers. Stephen Toulouse, a Microsoft security program manager, said yesterday that the program, known as "Bankash-A Trojan," could attempt to disable or delete the spyware removal tool and suppress warning messages. It also may try to steal online banking passwords or other personal information by tracking a user's keystrokes. To be attacked, Toulouse said a user would have to be fooled into opening an email attachment that would then start the malicious program. (The Age 11 Feb 2005)

SOPHOS anti-malware company summarizes the Trojan's functions as follows:
* Steals credit card details
* Turns off anti-virus applications
* Deletes files off the computer
* Steals information
* Drops more malware
* Downloads code from the internet

Category 14.4 *Trojans & rootkits*

2005-04-08 **hacker bogus Microsoft update patches e-mail Trojan Horse installation**

DHS IAIP Daily; http://news.zdnet.co.uk/internet/security/0,39020375,3919430
2,00.htm

HACKERS SEND FLOOD OF BOGUS MICROSOFT UPDATES

On Thursday, April 7, the same day that Microsoft announced details of its next round of monthly patches, hackers sent out a wave of emails disguised as messages from the software company in a bid to take control of thousands of computers. The emails contain bogus news of a Microsoft update, advising people to open a link to a Web site and download a file that will secure and 'patch' their PCs. The fake Website, which is hosted in Australia, looks almost identical to Microsoft's and the download is actually a Trojan horse — a program that can give hackers remote control of a computer. Microsoft said it is looking into the situation.

Category 14.4 *Trojans & rootkits*

2005-04-20 **Trojan Horse attack Symbian cell phone wireless mobile phone industry concern SimSecure F-Secure**

DHS IAIP Daily;
http://news.com.com/Trojan+horses+take+aim+at+Symbian+cell+p hones/2100
−7349_3−5678211.html

TROJAN HORSES TAKE AIM AT SYMBIAN CELL PHONES

The recent discovery of a large number of malicious mobile phone programs should raise concerns throughout the wireless industry, according to a virus tracker. Cell phone antivirus software company SimWorks reported Wednesday, April 20, that 52 new Trojan horses are hidden inside several different cell phones games and other readily available mobile phone software. While the software appears to be safe to share or use, the Trojans actually contain malicious software that crashes many critical cell phone system components. The Trojan horses target only cell phones that use Symbian, an advanced operating system. To date, no phones have been affected, according to Aaron Davidson, chief executive officer of SimWorks. While the damage is negligible so far, the recent warnings from SimWorks and security specialist F-Secure are raising alarm bells in the wireless industry. The latest report brings the total number of known Symbian Trojan horses to more than 100.

Category 14.4 *Trojans & rootkits*

2005-06-04 **hacker attack Trojan horses botnet building warning Bagle virus code organized crime**

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1823633,00.asp

ANTI-VIRUS COMPANIES WARN OF TROJAN ATTACK THAT BUILDS BOTNETS

Anti-virus researchers are sounding the alert for a massive, well-coordinated hacker attack using three different Trojans to hijack PCs and create botnets-for-hire. The three-pronged attack is being described as "unprecedented" because of the way the Trojans communicate with each other to infect a machine, disable anti-virus software and leave a back door open for future malicious use. Roger Thompson, director of malicious content research at Computer Associates International Inc. said that this attack "… clearly points to a very well-organized group either replenishing existing botnets or creating new ones." Once the three Trojans are installed, the infected computer becomes part of a botnet and can be used in spam runs, distributed denial-of-service attacks or to log keystrokes and steal sensitive personal information. According to CA's Thompson, the success of the three-pronged attack could signal the end of signature-based virus protection if Trojans immediately disable all means of protection. He said he thinks the attack, which used virus code from the Bagle family, is the work of a very small group of organized criminals. With the rapid proliferation of new types of virus, Trojan and worm attacks, PC users are urged to be strict about following security guidance.

Category 14.4 *Trojans & rootkits*

2005-06-16 **United Kingdom UK cyber infrastructure Trojan horse attack Far East**

DHS IAIP Daily; http://www.vnunet.com/vnunet/news/2138105/uk−infrastructure− trojan−attack

UNITED KINGDOM'S CYBER INFRASTRUCTURE UNDER TROJAN ATTACK

Parts of the United Kingdom's (UK) key computer systems are being targeted by Trojan software apparently originating from the Far East, according to the National Infrastructure Security Coordination Centre (NISCC). Both the UK government and private companies are being targeted, and an NISCC bulletin lists 76 Trojan programs that have been detected. The organization claims that the IP addresses on the e-mails often come from the Far East. "Trojan capabilities suggest that the covert gathering and transmitting of otherwise privileged information is a principal goal," stated the bulletin. "The attacks normally focus on individuals who have jobs working with commercially or economically sensitive data." The bulletin also warned that firewalls and antivirus software do not protect against the Trojans as they can be modified by security code to avoid signature traces. NISCC Bulletin: http://www.niscc.gov.uk/niscc/docs/ttea.pdf

---

Category 14.4 *Trojans & rootkits*

2005-06-30 **TechWeb trojan filtering Finnish firm worms Trojan horses Windows HOSTS Microsoft RAS API IP addresses Computer Associates F-Secure McAfeen Sophos Symantec Trend Micro Mitglieder**

DHS IAIP Daily; http://www.techweb.com/wire/security/164904273

NEW TROJAN FILTERING PACKETS TO ISOLATE USERS

A new Trojan is using a sophisticated technique to cut off infected computers from anti-virus and security vendors' update sites, the Finnish firm F-Secure said Thursday, June 30. It's not uncommon for worms and Trojan horses to sever links to update sites, but the until recently, said F-Secure, the method has been different: modifying the Windows HOSTS file to redirect the domains of popular security vendors to the local host so that the browser returns a blank page or error. This Trojan, dubbed Fantibag.b by F-Secure (and Fantibag.a by Computer Associates), however, blocks access by creating packet filtering policies using the Microsoft RAS packet filtering API. The result: all inbound and outbound packets between the user's machine and any of the 100+ filtered IP addresses are then dropped, essentially cutting communication and preventing updates--such as new malware signatures--from being downloaded. Among the filtered IP addresses are those belonging to Microsoft (including Windows Update), Computer Associates, F-Secure, McAfee, Sophos, Symantec, and Trend Micro. Fantibag.b sports a tenuous connection with the more prevalent Mitglieder Trojan, said Computer Associates; the former may be downloaded to systems already compromised by Mitglieder.

Category 14.4 *Trojans & rootkits*

2005-07-04 **The Register Symbian Trojan phones Doomboot mobile smartphones Bluetooth battery Finnish**

DHS IAIP Daily;
http://www.theregister.co.uk/2005/07/04/symbian_trojan_doomb oot/

SYMBIAN TROJAN DRAINS THE LIFE FROM PHONES

Virus writers have created a new Symbian Trojan called Doomboot-A that loads an earlier mobile virus (Commwarrior-B) onto vulnerable smartphones. Doomboot-A also preventing infected phones from booting up properly. "Doomboot-A causes the phone not to boot anymore and Commwarrior causes so much Bluetooth traffic that the phone will run out of battery in less than one hour. Thus the user who gets his phone infected with Doomboot-A has less than one hour to figure out what is happening and disinfect his phone, or he will lose all data," writes Jarno Niemela, a researcher at Finnish anti-virus firm F-Secure. "The Doomboot-A installation does not give any obvious clues that something is wrong, and Commwarrior-B does not have icon and is not visible in the process list. So the installation of Doomboot-A looks very much like failed installation of pirate copied game, and [a] user has hard time noticing that something bad is happening," he added. Doomboot-A, like most Symbian Trojans, poses as a pirate copy of a Symbian game (in this case Doom 2). Users who avoid pirated games or applications should be safe from infection.

Category 14.4 *Trojans & rootkits*

2005-07-11 **trojan horse attacks alert virus companies individuals infiltrateelements threat infrastructure operations software firewalls recipients patch vulnerabilities**

DHS IAIP Daily; http://www.esecurityplanet.com/alerts/article.php/3519236

US-CERT WARNS OF LATEST TROJAN HORSE ATTACKS

The US-CERT issued an alert last week warning of heightened trojan virus attacks against companies and individuals. Although trojan attacks that infiltrate computer systems aren't new, US-CERT said the technique used in these latest attacks have two distinct elements, which pose a threat to computing infrastructure and individual business operations. First, the trojans can elude conventional protective anti-virus software and firewalls. A number of open source and tailored trojans, altered to avoid anti-virus detection, have been used. Second, the e-mails are sent to specific or targeted recipients. Unlike "phishing" attacks, the e-mails use subject lines often referring to work or other subjects that the recipient would find relevant. US-CERT made 12 recommendations for system administrators in order to head off trojan horse attacks. They include using an anti-virus scanner on all e-mail attachments, updating operating system and application software to patch vulnerabilities exploited in the past by these Trojans; and turn off 'Preview Pane' functionality in e-mail clients and set the default options to view opened e-mails as plain text. Technical Cyber Security Alert TA05-189A --Targeted Trojan Email Attacks: http://www.us-cert.gov/cas/techalerts/TA05-189A.html

---

Category 14.4 *Trojans & rootkits*

2005-10-27 **bird flu Trojan horse Microsoft Word macro security social engineering**

DHS IAIP Daily;
http://www.techweb.com/wire/security/172900939;jsessionid=DI
XRDJJ3N5GNGQSNDBCSKH0CJUMEKJVN

BIRD FLU TROJAN POSES DANGER TO WORD USERS

A new Trojan horse, dubbed "Navia.a" by Panda Software, uses subject heads of "Outbreak in North America" and "What is avian influenza (bird flu)?" to dupe recipients into opening an attached Microsoft Word document. Luis Corrons, director of Panda's research, says "Unfortunately, we were expecting something like this…This is not the first time, and won't be the last, that writers of malicious code have taken advantage of people's misfortune and anxieties to spread their Trojans and worms." To protect against a macro-based exploit, Word users should set macro security level at "Medium," which triggers a warning when a Word document containing one or macros is opened, or "High," to disable macros entirely.

Category 14.4 Trojans & rootkits

2005-10-31 **digital rights management DRM SONY CD-ROM rootkit Trojan copyright protection malware malicious software**

http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html 24 09

SONY DRM INSTALLS ROOTKIT

On Oct. 31, Mark Russinovich broke the story in his blog: Sony BMG Music Entertainment distributed a copy-protection scheme with music CDs that secretly installed a rootkit on computers. This software tool is run without your knowledge or consent -- if it's loaded on your computer with a CD, a hacker can gain and maintain access to your system and you wouldn't know it.

The Sony code modifies Windows so you can't tell it's there, a process called "cloaking" in the hacker world. It acts as spyware, surreptitiously sending information about you to Sony. And it can't be removed; trying to get rid of it damages Windows.

This story was picked up by other blogs ..., followed by the computer press. Finally, the mainstream media took it up.

The outcry was so great that on Nov. 11, Sony announced it was temporarily halting production of that copy-protection scheme. That still wasn't enough -- on Nov. 14 the company announced it was pulling copy-protected CDs from store shelves and offered to replace customers' infected CDs for free….

[The text above is the start of Bruce Schneier's analysis of the implications of the SONY DRM rootkit case -- more in the entry specifically about his analysis on 17 Nov 2005.]

Category 14.4 *Trojans & rootkits*

2005-11-17 **digital rights management DRM SONY CD-ROM rootkit Trojan copyright protection malware malicious software collusion antivirus incompetence failure false negative**

Schneir On Security; 24 09
http://www.schneier.com/blog/archives/2005/11/sonys_drm_rootk.html

SCHNEIER BLASTS INDUSTRY COLLUSION FOR TOLERATING SONY DRM ROOTKIT

In a blistering analysis of the SONY DRM rootkit debacle, security guru Bruce Schneier attacked big antivirus makers Symantec and McAfee and industry giant Microsoft for tolerating the rootkit since mid-2004. The fundamental problem is collusion:

>The story to pay attention to here is the collusion between big media companies who try to control what we do on our computers and computer-security companies who are supposed to be protecting us.

Initial estimates are that more than half a million computers worldwide are infected with this Sony rootkit. Those are amazing infection numbers, making this one of the most serious internet epidemics of all time -- on a par with worms like Blaster, Slammer, Code Red and Nimda.

What do you think of your antivirus company, the one that didn't notice Sony's rootkit as it infected half a million computers? And this isn't one of those lightning-fast internet worms; this one has been spreading since mid-2004. Because it spread through infected CDs, not through internet connections, they didn't notice? This is exactly the kind of thing we're paying those companies to detect -- especially because the rootkit was phoning home.

But much worse than not detecting it before Russinovich's discovery was the deafening silence that followed. When a new piece of malware is found, security companies fall over themselves to clean our computers and inoculate our networks. Not in this case.

McAfee didn't add detection code until Nov. 9, and as of Nov. 15 it doesn't remove the rootkit, only the cloaking device. The company admits on its web page that this is a lousy compromise. "McAfee detects, removes and prevents reinstallation of XCP." That's the cloaking code. "Please note that removal will not impair the copyright-protection mechanisms installed from the CD. There have been reports of system crashes possibly resulting from uninstalling XCP." Thanks for the warning.

Symantec's response to the rootkit has, to put it kindly, evolved. At first the company didn't consider XCP malware at all. It wasn't until Nov. 11 that Symantec posted a tool to remove the cloaking. As of Nov. 15, it is still wishy-washy about it, explaining that "this rootkit was designed to hide a legitimate application, but it can be used to hide other objects, including malicious software."

The only thing that makes this rootkit legitimate is that a multinational corporation put it on your computer, not a criminal organization.

You might expect Microsoft to be the first company to condemn this rootkit. After all, XCP corrupts Windows' internals in a pretty nasty way. It's the sort of behavior that could easily lead to system crashes -- crashes that customers would blame on Microsoft. But it wasn't until Nov. 13, when public pressure was just too great to ignore, that Microsoft announced it would update its security tools to detect and remove the cloaking portion of the rootkit.

Perhaps the only security company that deserves praise is F-Secure, the first and the loudest critic of Sony's actions. And Sysinternals, of course, which hosts Russinovich's blog and brought this to light.

Bad security happens. It always has and it always will. And companies do stupid things; always have and always will. But the reason we buy security products from Symantec, McAfee and others is to protect us from bad security.

I truly believed that even in the biggest and most-corporate security company there are people with hackerish instincts, people who will do the right thing and blow the whistle. That all the big security companies, with over a year's lead time, would fail to notice or do anything about this Sony rootkit demonstrates incompetence at best, and lousy ethics at worst.

Microsoft I can understand. The company is a fan of invasive copy protection -- it's being built into the next version of Windows. Microsoft is trying to work with media companies like Sony, hoping Windows becomes the media-distribution channel of choice. And Microsoft is known for watching out for its business interests at the expense of those of its customers.

What happens when the creators of malware collude with the very companies we hire to protect us from that malware?

We users lose, that's what happens. A dangerous and damaging rootkit gets introduced into the wild, and half a million computers get infected before anyone does anything.

Who are the security companies really working for? It's unlikely that this Sony rootkit is the only example of a media company using this technology. Which security company has engineers looking for the others who might be doing it? And what will they do if they find one? What will they do the next time some multinational company decides that owning your computers is a good idea?

These questions are the real story, and we all deserve answers.<

Category 14.4 *Trojans & rootkits*

2005-12-27 **Windows Live Messenger Trojan ignore message alternate link download file machine botnet hacker malicious spam security software blocks access vendors hijacking contact names**

DHS IAIP Daily;
http://www.crn.com/sections/breakingnews/breakingnews.jhtml?articleId=175700348

'Leaked' Windows Live Messenger really a Trojan.

F-Secure told users to ignore instant messages with the subject head "MSN Messenger 8 Working BETA" that go on to claim that "Messenger 8 BETA has been leaked!" The message, which refers to an alternate name for the upcoming Live Messenger, also contains a link. Users who click on the link, then download and run the executable file, are in reality installing the Virkel.f Trojan. Virkel.f adds the compromised machine to a botnet, from which the hacker can update the Trojan with additional malicious code, to make the PC into a spam zombie or along with others, launch a denial-of-service attack on Websites. Virkel.f also shuts down anti-virus and security software, and blocks access to sites that belong to security vendors. This bot worm spreads by hijacking IM contact names from an infected computer, then spimming those names with new messages about the "leaked" client.

Category 14.4 *Trojans & rootkits*

2006-01-23 **four new Trojan horses mobile phones PCs**

DHS IAIP Daily; 23
http://www.techworld.com/security/news/index.cfm?NewsID=5219

FOUR NEW TROJANS ON THE LOOSE.

Four new Trojans are on the loose, three aimed at mobile phones and a fourth at PCs, anti-virus companies have warned. The mobile phone worms are disguised as legitimate applications and spread via Bluetooth or multimedia messages and affect phones running Symbian. The computer worm spreads via e-mail and purports to offer pornography. The phone worms -- Bootton.E, Pbstealer.D and Sendtool.A -- have a low infection rate at the moment. The first was spotted last week by F-Secure and Symantec and is perhaps the most potentially crippling of the three to those infected. It restarts the mobile but also releases corrupted components that cause a reboot to fail, leaving the device unusable. Fortunately, the phone worms are unlikely to spread very far. Unlike worms on computers, the Trojan horses hitting cell phones spread as attachments that require users to download them. The PC worm, Nyxem, however, is spreading rapidly and carries a potentially destructive set of instructions. Also nicknamed the Kama Sutra worm, it is programmed to overwrite all of the files on computers it infects on Friday, February 3, said Mikko Hypponen, chief research officer at F-Secure Corp. So far, there's no indication where Nyxem originated.

Category 14.4 *Trojans & rootkits*

2006-01-23 **Trojan e-mail social engineering credit card warning**

DHS IAIP Daily; http://www.theregister.co.uk/2006/01/23/trojan_blitz/ 23

TROJAN BLITZ POSES AS CREDIT CARD WARNING.

Businesses in the United Kingdom faced a barrage of 115,000 e-mails containing a new Trojan on Friday, January 20, before anti-virus vendors scrambled out an update, according to e-mail filtering firm BlackSpider Technologies. The Trojan downloader malware -- called Agent-ADO -- comes in the payload to a message that poses as a warning about a user's credit card limits being exceeded. BlackSpider detected the malware at 9:10 a.m. GMT Friday, January 20. But it was three-and-a-half hours before the first anti-virus vendor used by BlackSpider issued a patch, once again illustrating the shortcomings of conventional anti-virus scanners in fighting fast-moving virus outbreaks. Infected emails commonly have the subject line "ERROR:YOUR CREDIT CARD OVERDRAFT EXCEED!" and an infected attachment, a packed executable file called FILE1185 which is 5592 bytes long. Analysis of the malware is ongoing. System administrators are encouraged to set up rules to block the malware at the gateway. Virus writers commonly use networks of compromised PCs to seed infection over a short space of time but the ferocity of the latest attack is unusual.

Category 14.4 Trojans & rootkits

2006-01-23 **Trojan attack Tianjin province China**

DHS IAIP Daily; http://www.businessweek.com/technology/content/jan2006/tc20060123_003410.htm 23

TARGETED TROJANS ON THE RISE.

It was a stealth cyberattack: Last November 18, an e-mail with a nefarious purpose was dispatched from an Internet address in the Tianjin province of China. The targets: individual employees of the U.S. and European military and pharmaceutical, petrochemical, and legal companies, according to e-mail security firm MessageLabs. Attached was an apparently innocuous Microsoft Word document with a news story from CNN. And it was designed to look like it came from a trustworthy source. In this case, the Trojan was a particularly insidious variety known as a targeted Trojan because it was directed at a specific recipient -- intended to infect the computer networks of American companies. When opened, the Word document could have become a ticking time bomb. Buried inside was special code that would allow hackers to take remote control of each employee's PC. Then, working from inside the corporate networks, the hackers could steal corporate secrets or use the compromised computers to send spam and viruses. According to computer-security experts, spam, phishing e-mails, viruses, and worms will grow more slick and secretive in 2006.

Category 14.4 Trojans & rootkits

2006-02-02 **Trojan horse e-mail attack fake bird flu epidemic malicious code WMF Windows vulnerability exploit**

DHS IAIP Daily; http://www.websensesecuritylabs.com/alerts/alert.php?AlertID=415 23

TROJAN HORSE/WMF EXPLOIT: FAKE BIRD FLU EPIDEMIC E-MAIL.

Websense Security Labs has received reports of a Trojan horse that attempts to trick users into visiting a malicious Website to run malicious code. Users receive an e-mail with the subject, "Attention Bird Flu in England." The body requests users to click on a link to go either of two Websites to get more information. The e-mail also claims the government is trying to hide the facts on the flu. Upon clicking on a link, users are directed to a Website which claims that you have been blocked from accessing it. This appears to be another trick by the attacker to make the user believe that the site has either been disabled or shutdown. However, within the HTML, an IFRAME is loaded that uses the recent WMF exploit to run code without user-intervention. The code is a Trojan horse downloader, which connects to another site to download new malicious code. The filename is "expl1.wmf," which downloads and runs "expl1.exe." In the past, the same sites have been used for phishing, fraud, and distributing malicious code. The sites are hosted in the .WS and .CC domains and were up and running at the time of this alert.

Category 14.4 Trojans & rootkits

2006-02-17 **Sony rootkit stealth software involuntary installation DHS worry regulation laws**

DHS IAIP Daily; http://www.infoworld.com/article/06/02/17/75492_HNrootkitregulation_1.html 23

SONY ROOTKIT MAY LEAD TO REGULATION; DHS WORRIED ABOUT POTENTIAL VULNERABILITIES.

A U.S. Department of Homeland Security (DHS) official warned Thursday, February 17, that if software distributors continue to sell products with dangerous rootkit software, as Sony BMG Music Entertainment recently did, legislation or regulation could follow. "We need to think about how that situation could have been avoided in the first place," said Jonathan Frenkel, director of law enforcement policy with the DHS Border and Transportation Security Directorate, who was speaking at the RSA Conference 2006 in San Jose, CA. Last year, Sony began distributing XCP software in some of its products. This digital rights management software, which used rootkit cloaking techniques normally employed by hackers, was later found to be a security risk, and Sony was forced to recall millions of its CDs. While Sony's software was distributed without malicious intent, DHS is worried that a similar situation could occur again, this time with more serious consequences. "It's a potential vulnerability that's of strong concern to the department," Frenkel said. Though DHS has no ability to implement the kind of regulation that Frenkel mentioned, the organization is attempting to increase industry awareness of the rootkit problem.

Category 14.4 Trojans & rootkits

2006-02-25 **Panda Software discovery viruses-for-sale Website**

DHS IAIP Daily; http://arstechnica.com/news.ars/post/20060225−6264.html 23

MALWARE MOVES UP, GOES COMMERCIAL.

Engineers at Panda Software uncovered evidence last week that led them to a Website touting custom-built viruses for sale. For the price of $990, a user gets his or her own pet Trojan horse, complete with tech support. If the file is discovered -- as this current model was -- the designer provides a guarantee to alter it so that it may continue to avoid detection in the face of updated antivirus software. The Trojan goes by the moniker Trj/Briz.A, and scans the user's hard drive for information that could be used for financial and identity data. It then sends that information to an attacker working behind the scenes. Additional features include the ability to gather IP addresses and in some cases, the physical location of infected computers. It can also modify the machine to prevent access to Websites devoted to antivirus products. The file that causes the Trj/Briz.A infection is called "iexplore.exe." It uses this name to pass itself off as Internet Explorer.

Category 14.4 Trojans & rootkits

2006-02-28 **Trojan cell phone Java RedBrowser Russia Kaspersky Lab**

DHS IAIP Daily; 23
http://news.com.com/Russian+phone+Trojan+tries+to+ring+up+ch arges/2100−7349_3−6044266.html

RUSSIAN PHONE TROJAN TRIES TO RING UP CHARGES.

Antivirus companies are warning of new malicious software that can infect any cell phone capable of running Java applications, not just feature-rich smart phones. The Trojan horse was first spotted by Moscow-based Kaspersky Lab, which calls it RedBrowser. The malicious code poses as an application that promises people the ability to visit mobile Internet sites using text messages instead of an actual Internet connection, Kaspersky said in a statement Tuesday, February 28. Instead, the Trojan sends messages to certain premium rate numbers that charge between $5 and $6 per message, Kaspersky said.

Category 14.4 Trojans & rootkits

2006-03-01 **cross-infection virus Trojan secrecy mystery annoyance researchers MARA**

DHS IAIP Daily; http://www.securitypipeline.com/news/181401932 23

MYSTERY OVER PC-TO-MOBILE TROJAN ANNOYS RESEARCHERS.

Anti-virus researchers complained Wednesday, March 1, that a group claiming to have proof of the first PC-to-mobile Trojan hasn't shared the sample, a normal practice among security investigators. Monday, February 27, the Mobile Antivirus Researchers Association (MARA), which bills itself as a non-commercial collection of mobile malware researchers, said it had anonymously received malicious code it dubbed "Crossover." The sample, said MARA, could cross-infect a Windows Mobile Pocket PC from a desktop PC running Windows. According to MARA, the first-of-its-kind Trojan spreads to the mobile device via Microsoft's ActiveSync, then erases all files in the My Documents directory of the Windows CE- or Windows Mobile-based gizmo. But unlike the usual practice where virus researchers share samples, MARA's not willing to let others see the code, no-strings-attached, say some commercial researchers. They're left without a way to confirm Crossover's existence or MARA's claims, or update their own signatures to defend against the attacker.

Category 14.4 Trojans & rootkits

2006-03-06 **Hacker Defender rootkit development halt Holy Father security firm truce**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1934708,00.asp 23

"HACKER DEFENDER" ROOTKIT AUTHOR HALTS DEVELOPMENT.

The author of the Hacker Defender rootkit said he's taking a break from developing the popular hacking tool, but that he may soon return to developing new rootkit programs. The author, who uses the name "Holy Father," posted a message on the Hacker Defender Website calling a truce with security companies that make anti-rootkit technology. However, in an e-mail exchange with eWEEK, "Holy Father" said he isn't throwing in the towel, and that he may return to rootkit development after taking a break from Hacker Defender to work on other projects. Hacker Defender is one of the best-known rootkit programs. Rootkits have been common in computer hacking circles for years, and allow attackers to maintain access to a computer, without being detected, long after they have compromised its defenses. Hacker Defender was initially released as an open-source program in 2004. More recently, "Holy Father" has sold updated copies of the rootkit, dubbed "Golden Hacker Defender." That version of the program had an anti-detection engine designed to thwart anti-rootkit technology.

Category 14.4 Trojans & rootkits

2006-03-08 **Trojan horse vendor Website shut down RSA Security Panda Software**

DHS IAIP Daily; 23
http://www.informationweek.com/news/showArticle.jhtml?articleID=181502074

SECURITY RESEARCHERS TERMINATE SITES SELLING TROJANS.

Several Websites selling made-to-order Trojan horses to hackers have been shut down, thanks to the cooperation between U.S.-based RSA Security and Spain's Panda Software. The two companies collaborated in the effort to identify, locate, and shutter five sites: three were marketing la carte Trojans and two were sites where the buyers could monitor the infections the malware caused.

Category 14.4 Trojans & rootkits

2006-03-13 **virtual rootkits stealth risk malware undetectable risk**

DHS IAIP Daily; http://www.theregister.co.uk/2006/03/13/virtual_rootkit/ 23

VIRTUAL ROOTKITS CREATE STEALTH RISK.

Security researchers have uncovered new techniques to hide the presence of malware on infected systems. By hiding rootkit software in virtual machine environments, hackers have the potential to avoid detection by security software, experts at Microsoft Research and the University of Michigan warn. Existing anti-rootkit tools commonly rely on comparing file system and API discrepancies to check for the presence of rootkits, a technique that wouldn't be able to unearth virtual machine malware.

Category 14.4 Trojans & rootkits

2006-03-15 **Slobodan Milosevic e-mail Trojan murder pictures social engineering**

DHS IAIP Daily; http://www.theregister.co.uk/2006/03/15/slobodan_trojan/ 23

SLOBODAN TROJAN POSES AS MURDER PICTURES.

E-mails purporting to prove that the recently deceased former Yugoslav president Slobodan Milosevic was killed contain a malicious Trojan, called Dropper-FB. Online security firm BlackSpider estimates that more than 800,000 e-mails containing the new Trojan-downloader were sent to UK businesses before the first anti-virus software firm updated their software early Wednesday morning, March 15.

Category 14.4 Trojans & rootkits

2006-03-21 **Trojan horse hearse warning Sana Security Inc. username password theft rootkit**

DHS IAIP Daily; 23
http://www.infoworld.com/article/06/03/21/76669_HNtrojanhear
se_1.html?source=rss&url=http://www.infoworld.com/article/06
/03/21/76669_HNtrojanhearse_1.html

RESEARCHERS WARN OF TROJAN HEARSE.

Security researchers at Sana Security Inc. are warning of a new type of malicious software designed to steal usernames and passwords from Web surfers. The malware, dubbed "rootkit.hearse," uses rootkit cloaking techniques, making it extremely difficult to detect. In order to steal information, however, the software must first be downloaded onto a user's system. This can be done by tricking the user into downloading the malicious code, or by infecting a computer with some other form of malware. Once installed, it sends the sensitive information to a server in Russia, that appears to have been in operation since Thursday, March 16, Sana said. For more information on rootkit hearse:
http://www.nthworld.org/archives/2006/03/on_march_20th_w.htm

14.5 Virus hoaxes

Category 14.5 *Virus hoaxes*

1997-01-19 **good times hoax joke parody**

e-mail

In late 1996, a parody of the Good Times hoax circulated through the Net. One of its most off-the-wall sections was, "Goodtimes will give you Dutch Elm disease. It will leave the toilet seat up. It will make a batch of Methamphetamine in your bathtub and then leave bacon cooking on the stove while it goes out to chase gradeschoolers with your new snowblower."

Category 14.5 Virus hoaxes

1997-05-15 **hoax urban myth rumor**

NYT

Alex Gramling, writing in the New York Times, summarized the problems caused by unverified forwarding of rumors and urban myths. Jessica Mydek, for example is not in fact a seven-year-old dying of brain cancer, and the American Cancer Society has never volunteered to donate three cents for each copy of the hoax. Tommy Hilfiger has never appeared on the Oprah Winfrey Show, let alone made racist remarks about who should wear his line of clothing. Despite attempts to counter such harmful rumors, victims have little power to overcome human stupidity and irresponsibility. [Moral: don't forward unsubstantiated stories through the net, especially if they are shocking, or make you angry. Here's some biolerplate I use to explain to gullible hoax victims how they can avoid being fooled in future:

* * * A FRIENDLY MESSAGE ABOUT THE WARNING YOU JUST SENT ME * * *

The warning you have forwarded is a hoax. The danger is imaginary and the problem is nonexistent.

Security experts request that no one circulate unverified warnings of vague, alarming dangers.

Key indicators that a message is a hoax:

* use of exclamation marks (no official warning uses them);
* use of lots of UPPERCASE text (typical of youngsters);
* misspellings and bad grammar;
* no date of origination or expiration;
* references to official-sounding sources (e.g., Microsoft, CIAC, CERT) but no URL for details;
* no valid digital signature from a known security organization;
* requests to circulate widely (no such request is made in official documents).

Some guidelines for avoiding viruses and Trojan Horse programs:
— always run a good (e.g., ICSA-certified) antivirus program in background;
— keep your virus strings up to date (e.g., at least monthly updates);
— don't execute unknown software even if you know and like the person who went it to you;
— don't forward executables unless you downloaded them from a trustworthy source (e.g., a legitimate Web site);
— if you do forward something you have personally downloaded, include the URL for the origin of the executable file.

In addition, before alerting anyone to apprehended threats, check the anti-hoax pages on the Web. See, among others,

About virus hoaxes:
http://www.vmyths.com
http://www.icsa.net/html/communities/antivirus/hoaxes/

About other hoaxes:
http://ciac.llnl.gov/ciac/CIACHoaxes.html
http://www.urbanlegends.com/
http://www.cwrl.utexas.edu/~roberts/gullibility.html
http://www.urbanmyths.com/

For a scholarly (and fascinating) analysis of why hoaxes spread, see the paper by Sarah Gordon entitled "Hoaxes & Hypes" at
http://www.av.ibm.com/InsideTheLab/Bookshelf/ScientificPapers/Gordon/HH.html

and also her excellent overview entitled "Received. . . and Deceived" at
http://www.infosecuritymag.com/sept/cover.htm

For some more advice from M. E. Kabay on handling chain letters, see
http://www.av.ibm.com/current/Feature2/index.html

For a series of articles on protecting Internet users against various types of danger and fraud, see
http://www2.norwich.edu/mkabay/cyberwatch/index.htm

* * *

This page of advice is used with permission of the author, M. E. Kabay, PhD, CISSP, Assoc. Professor, Computer Information Systems, Norwich University
Last revision 2001-12-17.

Category 14.5 Virus hoaxes

2002-05-20 **social engineering hoax meme virus warning file deletion**

Security Wire Digest 4 39

The lastest social-engineering virus hoax of May 2002 involved detailed instructions on how to remove the "virus-infected" file JDBGMGR.EXE. Unfortunately, this harmful file is the Microsoft Debugger Registrar for Java and its removal causes some Java applets to fail. Apparently the hoax was circulating in English, French, Italian, Spanish, Dutch and German versions.

Category 14.5 Virus hoaxes

2003-01-06 **virus hoaxes continue fool users anti-virus vendor information**

NIPC/DHS

January 02, ZDNet — Virus hoaxes continue to fool computer users.

Fuelled by concern over genuine threats such as Klez, Bugbear and Magistr, computer users are continuing to fall for false warnings of non-existent viruses. These hoaxes typically warn the reader not to open an e-mail with a certain subject line, or to immediately delete a particular file on their hard drive, because they contain a virus. They will also tell the reader to forward the warning to their friends and colleagues. Even though these hoaxes didn't encourage the reader to delete files from their machine, they are harmful because they waste both time and bandwidth. All the major anti-virus companies include information on such hoaxes on their Web sites.

Category 14.5 Virus hoaxes

2004-07-26 **virus hoax Bin Laden suicide al Qaeda terrorism fear uncertainty doubt FUD**

NewsScan

BIN LADEN HOAX VIRUS WARNING

E-mail purporting to contain evidence of Osama bin Laden's suicide contains a "Trojan horse" virus that could allow network vandals to take over infected computers. Naming the new scheme the Hackarmy Trojan horse, the antivirus firm Sophos says, "Thousands of messages have been posted onto Internet message boards and usenet newsgroups claiming that journalists from CNN found the terrorist leader's hanged body earlier this week." The messages point to a site where it's claimed that a file of photographs can be downloaded, but what the file really contains is a Trojan horse that can allow hackers to gain remote control of an infected computer. (The Australian 26 Jul 2004)

---

15 Fraud (not embezzlement), extortion, slamming

Category 15 *Fraud (not embezzlement), extortion, slamming*

1997-01-29 **E-mail**

RISKS; AP 18 81

Ms Adelyn Lee sued Oracle Corporation for wrongful dismissal and sexual harassment. Her evidence included an e-mail message from her boss, Craig Ramsey, to the CEO Larry Ellison confirming that Ramsey had fired Lee in accordance with Ellison's direct instructions. She settled out of court for a $100,000 payment. Subsequent events showed that in fact Ms Lee logged into her ex-boss' e-mail account the day after she was fired and forged the message. She was found guilty of perjury and falsification of evidence; she faces up to four years in prison.

Category 15 *Fraud (not embezzlement), extortion, slamming*

1997-01-30 **cellular phone fraud**

AP

Criminals altered imported cellular phones into Finland and "cloned" them by changing the electronic serial numbers — but used the same number for all the phones. When a victim of this scam reported his phone stolen, its serial number was inactivated; hundreds of phones went dead. This was the first indication of the extent of the problem. Experts predicted that the lost revenues would amount to the equivalent of tens of millions of dollars.

Category 15 *Fraud (not embezzlement), extortion, slamming*

1997-01-30 **phone fraud appropriate-use policy**

Reuters

Police in Mexico City have been placing so many calls to phone-sex lines that police stations have had their phones cut off or severely restricted.

Category 15 *Fraud (not embezzlement), extortion, slamming*

1997-02-01 **phone fraud slamming**

UPI

Heartline Communications of Houston forged consumer signatures in their "slamming" operation — the unauthorized switch of long-distance carriers. A NJ judge has ruled in favor of consumers and may slap half-million dollar fines or more on the slammer.

Category 15 *Fraud (not embezzlement), extortion, slamming*

1997-02-11 **fraud**

Reuters

The FTC warned that scam artists have been using the Internet to promote the usual round of frauds. In particular, beware of franchise operations; demand written documentation justifying claims of specific income from such operations. Job seekers should be skeptical of any scheme demanding advance payment for job placement; and be aware that there are _no_ "undisclosed" government positions.

In a related story, the British Securities and Investments Board announced a new Web site with information about Internet scams and risky investments promoted on the Net. See <http://www.sib.co.uk> for details.

Category 15 *Fraud (not embezzlement), extortion, slamming*

1997-02-24 **fraud**

UPI, AP

The FTC won a settlement from Fortuna Alliance company in Washington state, which fraudulently deposited money contributed by victims fleeced through Internet promotions of a pie-in-the-sky pyramid (or Ponzi) scheme that promised $5,000 a month and more in return for an enrollment fee of $500 — if they suckered their friends and acquaintances into "investing" in the scheme. Most of the money received instantly went into bank accounts in Antigua. The settlement included restitution of $2.8M and assurances that the business would close down. AP reported that total reimbursements could top $5M and that (A pyramid / Ponzi scheme pays early contributors fraudulent profits out the money paid by subsequent victims; when the source of funds dries up through exhaustion of the pool of gullible people in the network, the criminals abscond with the remaining funds.)

Category 15 *Fraud (not embezzlement), extortion, slamming*

1997-03-14 **phone fraud stealing dial tone**

RISKS 18 90

From Britain, a salutary case: Unexplained long-distance calls on family phone; phone company claims could not be an error. Correspondents explain how someone could steal dial tone using wireless phones, vestigial phone lines, or wiretaps. Do not accept the "computer cannot lie" syndrome.

Category 15 *Fraud (not embezzlement), extortion, slamming*

1997-04-15 **fraud e-mail**

RISKS 19 8

In April, many Microsoft Network (MSN) users received fraudulent e-mail asking for their credit card numbers to help recover from a fictitious virus attack that had supposedly wiped out billing records.

Category 15 *Fraud (not embezzlement), extortion, slamming*

1997-04-16 **bank error QA law fraud**

UPI

Frank McPherson discovered a balance of $169,000 in his bank account. He told a teller about it and was informed that the money must be his. Figuring it was a credit from the government, he promptly spent it all on useful things like a new truck, a car, some mountain bikes, a new home, a camcorder and some new clothes. Unfortunately, the teller was wrong, so McPherson ended up in court, charged with fraud. Moral: do not spend money that comes from nowhere into your bank account, regardless of tellers who breezily say the computer couldn't be wrong.

Category 15 *Fraud (not embezzlement), extortion, slamming*

1997-04-24 **fraud Internet**

EDUPAGE

According to Deloitte & Touche, criminals are defrauding European Union members of about $77B a year using Internet-based or Internet-mediated fraud.

Category 15 *Fraud (not embezzlement), extortion, slamming*

1997-04-27 **fraud Internet**

EDUPAGE

The FTC, securities regulators and attorneys-general from 24 states found 215 cases of fraudulent marketing in a single day of surfing the Web. The FTC issued stern warnings to the fraud artists and dozens of them shut down altogether. The FTC intends to continue surfing the Web, but urges consumers to be careful and demand evidence of the wild claims they encounter. In one case, someone claimed to be able to earn $100,000 a year by grooming pets; another claimed that victims of his scam would earn $240,000 a year operating 900-number phone lines.

Category 15 *Fraud (not embezzlement), extortion, slamming*

1997-05-17 **spam vandalism denial of service fraud**

RISKS 19 16

In May 1997, Jim Youll's company was subjected to repeated denial-of-service attacks, apparently because of his public anti-spam stance.

Category 15 *Fraud (not embezzlement), extortion, slamming*

1997-05-22 **credit card hacker social engineering**

AAP

An unidentified 16-year-old boy with a penchant for computing tricked several banks into giving him credit cards, which he then used to order $18,000 of goods and services via computer-based purchases. He pleaded guilty to 104 countrs of fraud and was sentenced to 12 months in prison. His defense team argued that he should receive psychiatric treatment for what they described as "an anxiety disorder and elements of an obsessive, compulsive disorder." His mother excused his behavior by saying, "If we were a wealthy family he'd be at a private school, where his talents could be directed properly." Um, what about parental direction of the child's talents? (More news in October listing, where the boy was identified as Drew Henry Madden and pleaded guilty to yet more fraud.)

Category 15 *Fraud (not embezzlement), extortion, slamming*

1997-05-25 **packet sniffer credit card fraud**

EDUPAGE

A thief who ran a packet sniffer to capture 100,000 credit card numbers from a dozen on-line commerces was arrested when he tried to sell the list to the FBI for $260,000.

Category 15 *Fraud (not embezzlement), extortion, slamming*

1997-05-26 **fraud Web ghost redirection penetration hack**

Guardian Weekly

Garth McLachlan of the Organised Crime Unit of the National Criminal Intelligence Service of the UK reported on new ways of defrauding victims on the Net. Simple methods include putting up Web sites that market fraudulent schemes; e.g., Ponzi / pyramid sales. Another scam is the reputable-looking site that offers venture capital — in return for a $10,000 advance fee for evaluation of the business proposals. Anyone gullible enough to send that much money to unknown people usually gets asked for more and more money but never gets anything in return. In another scam, criminals offer credit cards, collect detailed information from the victims, and then generate fraudulent cards or attack the victims' bank accounts directly. Another form of chicanery is to hack a competitor's Web page to change the prices of their products so they lose money when their automated sales programs accept credit card numbers; or sometimes to substitute a competitor's phone number so orders come to them instead of to the owner of the hacked Web page.

Category 15 *Fraud (not embezzlement), extortion, slamming*

1997-06-03 **identity theft fraud credit cards checks**

American Banker

Cheryl and Roger Cullen were arrested in Delaware at dawn on 1997.03.19 in the act of trying to burn evidence of an alleged crime spree that involved hundreds of false identities and check and credit-card frauds probably amounting to more than a million dollars since 1992. The case, one of the most difficult fraud investigations of recent years, demonstrates the importance of each act of verification in the banking and commerce sector. Credit-card applications, in particular, should be scrutinized with care and all details checked for veracity before cards are issued. According to the Federal reserve, check fraud alone cost society $615M in 1995, compared with $59M for physical bank robberies.

Category 15 *Fraud (not embezzlement), extortion, slamming*

1997-06-04 **fraud counterfeit electronic commerce**

Guardian Weekly, Reuter

The National Criminal Intelligence Service of the UK publicly stated that the growth in electronic commerce and specifically the coming widespread use of electronic money (e.g., the smart card systems of Mondex) will open an enormous vulnerability in the economy. Digital counterfeiting would likely be impossible to distinguish, said Gareth MacLachlan, head of the Organised Crime Unit of the NCIS; he emphasized the value of integrating full audit trails into all forms of electronic money, including electronic "cash" system that are designed at present to provide anonymous financial transactions. Dr James Backhouse of Computer Security Research Centre at the London School of Economics agreed, saying, "The biggest impact would be the loss of any audit trail. Most bank transactions leave some trail within the system and this would be lost."

Category 15 *Fraud (not embezzlement), extortion, slamming*

1997-06-08 **extortion hacking penetration banks**

Newsday

Newsday published a cover story by Matthew McAllester that started, "COMPUTER HACKERS have successfully forced financial institutions in the United States, Europe and Asia to pay millions of dollars in ransom by threatening the companies' computer networks.

"The payouts were confirmed by law enforcement officials, banking insiders and security experts interviewed over the past several weeks. When most successful, the sources said, the crimes have linked disgruntled insiders with computer experts recruited throughout the world - including the former Soviet Union, India and southeast Asia - by organized crime groups."

See <TheLibrary@newsday.com> for details.

Category 15 *Fraud (not embezzlement), extortion, slamming*

1997-06-15 **Netscape bug extortion**

EDUPAGE, Newsbytes,

Christian Orellana, a Danish computer consultant, threatened to release information to the press about a serious security weakness in Netscape Navigator unless he were paid more than the $1,000 prize offered by Netscape to encourage independent quality assurance tests. His message included the words, "I think the person most suited for handling this is somebody in charge of the company checkbook. . . . I'll leave it to you to estimate what impact that would have on Netscape stocks." His actions were almost universally reviled by professional security specialists.

Category 15 *Fraud (not embezzlement), extortion, slamming*

1997-07-03 **Internet fraud**

EDUPAGE

Canadian investment regulators announced they would cooperate with the U.S. Federal Trade Commission in prosecuting investment frauds involving supposed "Internet Shopping Malls." The project is called "Field of Schemes" and aims to educate senior citizens particularly targeted by criminals.

Category 15 *Fraud (not embezzlement), extortion, slamming*

1997-07-07 **hackers extortion blackmail infowar Web vandalism**

Electronic Telegraph

According to an investigation by Robert Uhlig, reporter for the Electronic Telegraph in Britain, criminal hackers have been trying to blackmail hundreds of corporate and government officials by threatening to post defamatory claims on corporate Web sites. According to Nick Lockett, a barrister (attorney) with special expertise in cyberlaw, "Typically, the hackers say they will put defamatory information about a senior MP or other public figure on the target company's web site and then let the MP know about the publication of the material. If the threat is ignored, they make a small change to the company's site to prove their point and force it to take them seriously. They are testing the waters at the moment. This is almost certainly a market research exercise. A big campaign of blackmail is about to start." The journalist reports that the extortion demands are in the thousands of pounds.

Category 15 *Fraud (not embezzlement), extortion, slamming*

1997-07-15 **slamming**

AP

The FTC, overwhelmed with over 16,000 complaints from enraged customers whose long-distance telephone service has been switched without their permission — a practice known as "slamming" — proposed several changes in their regulations to help victims. For example, victims would no longer pay anything at all for calls placed via the slammers' services (unlike the current rule, which pays the slammers at the rate the victims' original phone company would have charged). Other changes would force the predators to obtain explicit consent for changes and to provide easy ways to cancel unauthorized changes.

Category 15 *Fraud (not embezzlement), extortion, slamming*

1997-07-29 **bank fraud counterfeit checks audit policy**

UPI

Check fraud costs American businesses nearly $10B annually. Around 55% of all criminal cases reported to the FBI involve check fraud and counterfeiting. Much of this fraud could be prevented if organizations paid attention to reasonable commercial standards. For example, every organization showed verify its bank statements quickly, conduct periodic audits, and Institute controls over accounts payable and payroll functions.

Category 15 *Fraud (not embezzlement), extortion, slamming*

1997-08-21 **hackers credit card fraud encryption**

AP, USA Today http://www.usatoday.com/life/cyber/tech/ctb104.htm

Five teenagers in Bloomington, MN created about 25 credit-card numbers and stole thousands of dollars of electronic gear before they were caught. Sceptics suggested that one of the boys, who worked at a dry cleaners, more likely stole all the card numbers from his employer.

Category 15 *Fraud (not embezzlement), extortion, slamming*

1997-08-26 **fraud impersonation Web theft credit card ISP**

EDUPAGE, AP

Naïve AOL members responded to credible e-mail asking them to visit a Web site where they could read a letter from AOL's chairman. The members then filled out forms with their credit card numbers and other information supposedly to update AOL records. Unfortunately, the Web site was run by thieves.

Category 15 *Fraud (not embezzlement), extortion, slamming*

1997-08-29 **beeper fraud toll call**

Newsday

Scott Van Pala, a 21-year old college student in Nassau County near New York City, set up a 540-number toll line at his parents home. He was arrested in August and accused of beeping at least 4,000 beeper users at all hours of the day and night; his victims included doctors, law enforcement officers and attorneys. The victims of the scam would call the 900 number and hear a click — but be billed $0.95 per call. Others would hear only a busy signal and waste their time trying to get through. The attack lasted over 10 weeks, at which point investigators compared notes on the fraudulent billings and easily tracked the suspect down. Investigators estimated that the criminal realized $4,000 from the scam. He faced 4 years in prison.

Category 15 *Fraud (not embezzlement), extortion, slamming*

1997-09-02 **fraud Internet credit cards**

Reuters

A former graduate student at Nova Southeastern University was charged with fraudulent applications for credit cards. He allegedly applied for 174 credit cards via the Internet using the names of fellow students; however, he used the same address for all of them. Banks contacted police and no cards were issued. Maybe now we understand why he had withdrawn from graduate school before he was arrested.

Category 15 *Fraud (not embezzlement), extortion, slamming*

1997-09-10 **Internet fraud abuse consumers protection**

AP

The National Consumers League opened a new Web site to help consumers evaluate propositions circulating through the Internet. Complaints to the NCL tripled in 1997, with about 100 reports of fraud a month compared with about 35 per month in 1996. John D. McClain of AP wrote, "The league officials said the most common signs of fraud are extravagant promises of profits, guarantees of credit regardless of bad credit history, suspiciously low prices or prizes that require up-front payments." The site is <http://www.fraud.org/ifw.htm>.

Category 15 *Fraud (not embezzlement), extortion, slamming*

1997-09-28 **spam fraud law**

RISKS, EDUPAGE 19 19

In May, Craig Nowak, a clueless college student, chose a return address at random for his slimy first attempt at junk e-mail. Unfortunately for his victim, "flowers.com" is a legitimate business whose owner received 5,000 bounced messages and plenty of abuse for supposedly spamming the world. Fortunately for the anti-spam cause, the enraged florist, Tracy LaQuey Parker, launched a lawsuit for damages and was supported by the Electronic Frontier Foundation (Austin chapter) and the Texas Internet Service Providers Association. In late September, the plaintiffs won a temporary injunction against the defendant and his ISP preventing him from further use of the appropriated domain name (not that he'd have wanted to, at that point). In November, the defendant was fined $18,910 plus court costs.

Category 15 *Fraud (not embezzlement), extortion, slamming*

1997-09-30 **Internet fraud law enforcement**

AAP

The Australian Competition and Consumer Commission announced that it was joining with more than 30 other agencies worldwide to share information about consumer fraud on the Internet and to prosecute e-crooks. Consumer Affairs Minister Chris Ellison said that "Internet scams ripped off thousands of Australians each year, with promotions including fake credit card offers, tickets in phoney lotteries, useless investments, worthless phone cards and pyramid selling schemes." He added that the Commission would not release details of it targets and said, "Those involved in scams will be in for a shock."

Category 15 *Fraud (not embezzlement), extortion, slamming*

1997-10-03 **hacker credit card fraud forgery**

AAP

A 16-year-old Australian, Drew Henry Madden, of Brisbane started defrauding businesses using stolen and forged credit-card numbers just after leaving school. By 1997, he had stolen $100,000 in goods and services. In October, he pleaded guilty to 294 counts of fraud. He was given a suspended sentence. His defense attorney blamed poor security for the losses: "Defence counsel Simon Lewis said Madden started with very minor credit card fraud, but it escalated alarmingly, because the safeguards were so inadequate." Despite the youngster's unusual revenue stream, his mother appeared to have accepted his globe-trotting ways and massive purchases of lottery tickets without comment.

Category 15 *Fraud (not embezzlement), extortion, slamming*

1997-10-21 **forgery perjury chat room**

AP

In Michigan, Circuit Judge Alice Gilbert ordered a search of an unnamed woman's computer systems by defense attorneys. The woman accused 26-year old Sean A. Crockett of assaulting her in Feb 1997 after they met via an online chat room but is in turn accused of having boasted online in a "Man Haters" chat room about fabricating the accusation.

Category 15 *Fraud (not embezzlement), extortion, slamming*

1998-01-04 **satellite piracy scrambler decoder TV**

ICSA research

ICSA's underground research team reported a growing list of sites selling equipment and techniques for defeating satellite TV encryption (scrambling). According to other reports, criminals — many of them based in Canada — have been providing dishonest customers with the ability to benefit from high-capacity TV satellites without paying subscription fees. Signal theft is a federal felony, with prison terms and up to $100,000 per violation for selling illegal devices. Customers who steal TV signals can pay up to $50,000 and may go to jail for two years for the first conviction. The criminals who sell these devices and provide decryption algorithms usually manage to defeat changes within a couple of days. Ironically, the hackers who sell hacked access-cards complain about "thieves" when their own customers fail to pay them for the illegal products.

Category 15 *Fraud (not embezzlement), extortion, slamming*

1998-01-06 **information warfare spam extortion**

RISKS 19 53

The National Organization of Internet Commerce was reported to have threatened the public disclosure of one million AOL subscriber names on its Web site as a pressure tactic to force the ISP to provide a mechanism to allow them to send junk e-mail to all AOL subscribers at low cost.

Category 15 *Fraud (not embezzlement), extortion, slamming*

1998-01-22 **extortion hacker bank reward**

RISKS 19 56

A German bank, Noris Verbraucherbank, offered a DM10K reward (~U$5000) for help in getting a criminal hacker who attempted to extort DM1M by threatening to release "confidential customer information and bank access codes" according to a report in RISKS.

Category 15 *Fraud (not embezzlement), extortion, slamming*

1998-04-23 **slamming fraud phone FCC**

EDUPAGE

The Fletcher Companies engaged in systematic "slamming" — switching customers to their expensive long-distance services without permission. The FCC, responding to over 1400 complaints, fined the group of companies $5M. FCC Chairman William Kennard vowed to crack down on these fraud artists and asked consumers to check their phone bills carefully each month.

Category 15 *Fraud (not embezzlement), extortion, slamming*

1998-12-15 **fraud scam bilk investor sucker victims gullible confidence**

AP

Kevin Tauber formed WARPnet Holdings LLC and presented the company as an ISP to wealthy investors. Actually, said the SEC, he was allegedly a con-artist who bilked his victims of their investments. [This case reminds one that some observers, including Alan Greenspan of the Federal Reserve, have commented that the frenzy of investment in Internet businesses — many of which have never earned a profit — has all the characteristics of an investment bubble. Caveat emptor (or caveat investor).]

Category 15 *Fraud (not embezzlement), extortion, slamming*

1999-11-15 **fraud scam information warfare stock price manipulation securities**

The Times (London)

Investors in the USA and in the UK were warned off "pump-and-dump" frauds in which false information is used to generate interest in stocks. Typically the fraudsters buy cheap and then try to move the share price higher by posting exciting but wrong news about the company's prospects. Cases have involved losses in the millions of dollars. One of the techniques used by the criminals is to put up Web sites that resemble or even duplicate those of the real company and link to them from their own bogus sites.

Category 15 *Fraud (not embezzlement), extortion, slamming*

1999-11-16 **Internet Web fraud bogus prosecution**

Reuters

The New Jersey Attorney General charged nine people on several complaints of fraud from 1996 through 1998. Some of the scams included selling non-existent stock for $850,000, selling non-existent Beanie Babies through the eBay online auction service, and selling Viagra through the Net without a license.

15.1 Fraud

Category 15.1 *Fraud*

1997-01-08 **fraud Internet AOL Russia**

AP, EDUPAGE

AOL staff became suspicious about enormously expensive bills being run up by Russian users. Investigation revealed so much credit-card fraud, stolen user IDs and passwords and other forms of fraud that the company terminated services in 40 Russian cities. From mid-December 1996 on, the 2,000 Russian AOL subscribers must now access the service by logging on to local Russian Internet Service Providers.

Category 15.1 *Fraud*

1997-01-08 **fraud AOL AOL4FREE**

Reuters

Nicholas Ryan, a 20-year-old Yale University student, pleaded guilty to creating the AOL4FREE program that allowed an unknown number of larcenous AOL users to cheat the company of their $2.95 per hour access fee. On a single day, submitted AOL, the program was used 2,000 times for illegal access. Ryan, who called himself "Happy Hardcore," continuously modified his program to counter defensive measures taken by AOL programmers. As a result, the young man faced up to five years in federal prison and up to $250,000 in fines.

Category 15.1 *Fraud*

1997-01-08 **credit card fraud insider**

PA News

In one of the more spectacular cases of insider fraud, Elizabeth John, a manager at Harrods in London admitted having taken 1,288 receipts and confidential records from her employer's store to her flat — but insisted that she had simply forgotten to return them. The scam, involving her brother (who confessed) and others, netted 205,000 pounds of profit. One victim was so wealthy that he failed to notice that 120,000 pounds of fraudulent charges had been attributed to his Gold Mastercard. In all, 70 customers had their credit cards pillaged.

Category 15.1 *Fraud*

1997-01-23 **infowar privacy credit card confidentiality**

UPI

Missing atheist Madalyn Murray O'Hair's American Express card has been used and paid regularly since her disappearance in September 1995. O'Hair's son, Bill Murray, is asking that the Texas Rangers be assigned to the case and allowed to use the expense data in tracking the missing woman.

Category 15.1 *Fraud*

1997-08-21 **fraud bank Internet scam**

ZDNN

The European Union Bank, supposedly based in Antigua, advertised extensively on the Internet and offered 21% interest on its offshore deposits. Unfortunately for the gullible, the bank appears to have been linked to the Russian mafia; its directors disappeared with $10M in assets. Investigators report that of the 1,200 banks with Web sites in 1997, 50 offered online transactions — and 5 of those were fraudulent. Legitimate Internet bankers warn the public to be sceptical of inflated claims, just as they would in the real world.

Category 15.1 *Fraud*

1999-02-03 **Internet credit repair fraud FTC crackdown lawsuits scam**

Wired via PointCast

The FTC and 14 state Attorneys General launched aggressive lawsuits against three credit-repair agencies that taught people with bad credit histories to lie their way to a new credit history. The dishonest victims of the fraudsters paid U$22-$40 to learn techniques for fraud. According to an article for Wired written by Heidi Kriz, credit-repair fraud instructions are the ninth most popular criminality on the Web today. Quoting Cleo Manuel of the Internet Fraud Watch consumer-protection organization, the author noted that the number one Internet fraud today is online auctions. [Comment from MK: online gambling involving unverifiable results of a game or in online auctions involving unverifiable bids by possibly virtual bidders constitute a tax on low IQ.]

Category 15.1 *Fraud*

1999-02-23 **Internet fraud scam FTC online consumers survey study statistics**

AP, UPI

The National Consumers League's Internet Fraud Watch received 7,752 complaints about Internet-based fraud in 1998 compared with 1,280 in 1997. In February, the Federal Trade Commission announced it would institute a 24-hour fraud-detection service in March 1999. Internet Fraud Watch reported that the top 10 complaints were (in order of frequency): auctions, general merchandise sales, computer equipment and software, Internet services, work-at-home offers, business opportunities, marketing schemes, credit card offers, advance fee loans and employment offers.

Category 15.1 *Fraud*

1999-04-16 **fraud securities Web forgery insider trading stock**

CNN

Gary Dale Hoke was arrested by the FBI for allegedly creating a bogus Web page that simulated the Bloomberg information service and touted PairGain stock as undervalued because of an impending takeover; the false information deceived investors into bidding up the price of Pairgain stock, causing windfall gains for some stockholders and losses for others when the price fell back to normal. The accused faced fines in the $M and up to 10 years in jail for stock manipulation. The FBI tracked the perpetrator using cooperation from ISPs and access to their Internet server log files. Hoke pleaded guilty to the charges in June 1999.

Category 15.1 *Fraud*

1999-04-21 **fraud credulity irresponsible press lies massacre shooting**

AP

People with a sick sense of humor posted fraudulent ex post facto "warnings" about the Littleton, Colorado High School attack in several AOL member profiles.

Category 15.1 *Fraud*

1999-04-23 **privacy Web Internet detectives private investigators fraud**

New York Times

The FTC announced that it would crack down on private investigators using deceit to obtain confidential information. FTC charged James and Regina Rapp, who advertised on the Web that their company, Touch Tone Information, could obtain private data such as bank records and unlisted phone numbers. The Rapps admitted to instructing employees to make hundreds of phone calls under false pretences — banned by the Federal Trade Commission Act. James Rapp shut down his Web site and promised to stop lying to get information but claimed that such limitations on his practice would only hurt victims. Sneered Rapp, "If you're a dead-beat dad or a neglected spouse you don't have to worry anymore." [The New York Times did not report on Mr Rapp's explanation of why bad people could not equally well use his service for nefarious purposes.]

Category 15.1 *Fraud*

1999-04-26 **fraud scam thieves Y2K gullible victims banks PCs software**

AP

Criminals have been taking advantage of the Y2K frenzy by selling electronic snake-oil: magical programs that fix Y2K problems instantly and without effort. Others are not even bothering with the product: they sell stocks in their fraudulent corporations by claiming to have vague but wonderful products that will sell madly in the last quarter of 1999. People have been tricked into moving their bank deposits into "another" bank account as part of their bank's Y2K efforts — only to discover that the other bank account belonged to someone else who has cleared it out and disappeared.

Category 15.1 *Fraud*

1999-05-07 **privacy children commerce Internet Web law government FTC**

AP

The FTC and Liberty Financial Companies arrived at a settlement after the company misled visitors to its "Young Investor" Web site by claiming that survey data would be "kept anonymous." In fact the company gathered personal details including name and e-mail address and sent advertising to its visitors. In addition, said the FTC, the company enticed children into filling out detailed surveys by promising prizes but the company never actually selected winners for the prizes or sent out the newsletters. Company spokesperson claimed that this was "an administrative error" and hurriedly arranged to award their prizes.

Category 15.1 *Fraud*

1999-05-11 **Internet Web fraud organization e-commerce crime**

Reuters

In May, the new Internet Fraud Council started work on standards for Internet businesses to help fight fraud. They proposed a clearinghouse to share information about different types of fraud on the Net and announced that they would collaborate with law enforcement initiatives to quash fraud.

Category 15.1 *Fraud*

1999-10-12 **fraud Internet e-commerce spam study statistics survey**

CNET news.com

The incidence of fraud through online sales and auctions is increasing as the volume of these transactions increases. Troy Wolverston and Greg Sandoval interviewed several experts on computer crime for CNET news.com and found a consensus that easy anonymity is at the root of easy crime.

Category 15.1 *Fraud*

2000-01-06 **stock manipulation fraud Web**

NewsScan, New York Times
http://www.nytimes.com/library/tech/00/01/biztech/articles/06net.html

The Securities and Exchange Commission has filed a civil lawsuit against Yun Aoo Oh Park (known as "Tokyo Joe" on the Web site where he dispenses stock market advice), charging him with defrauding investors by selling his own shares in stocks that he was urging his readers to buy. First Amendment lawyer Floyd Abrams says: "The position of the S.E.C. is not ridiculous and cannot be blown away by hoisting a First Amendment banner, but the case does raise a serious First Amendment issue involving the continued availability of the Web as a place where people can speak broadly in an uninhibited manner about topics, including the stock market." (New York Times 6 Jan 2000)

Category 15.1 *Fraud*

2000-02-21 **stock manipulation pump and dump fraud Web site penetration**

RISKS 20 81

Peter G. Neumann wrote in RISKS: "A fake press release announced a merger of Aastrom Biosciences Inc. with Geron Inc., a California biopharmaceutical house. Aastrom stock fell, while Geron rose. Aastrom asserted that the message on their Website was totally bogus, and presumably the result of a penetration."

Category 15.1 *Fraud*

2000-06-09 **fraud misrepresentation accounting dissimulation lies investors scam**

NewsScan, Investor's Business Daily

Shaky bookkeeping practices account for some dot-coms' inflated revenue reports, and a proposal before the Securities and Exchange Commission would put an end to accounting loopholes that enable these companies to jigger their figures. At issue is a tendency on the part of some companies to report as gross revenue the total sales price of all transactions, regardless of whether any revenue from those transactions is retained by the company. For many Web businesses that sell other companies' products, this practice has enabled them to boost their reported earnings and lure unwary investors. "This is going to impact a wide range of companies," says an Internet analyst. "Companies that report revenue one way are going to be rubbing their hands in glee. Now they can say their competitors were reporting bogus figures all along." (Investor's Business Daily 9 Jun 2000)

Category 15.1 Fraud

2000-06-29 **fraud deceptive advertising computers retailers**

NewsScan, New York Times
http://www.nytimes.com/library/tech/00/06/biztech/articles/30free-pcs.html

Value America, Buy.com, and Office Depot, as the result of charges brought by the Federal Trade Commission that they and other retailers have been guilty of deceptive advertising of so-called "free" or low-cost personal computers, will now post real, out-of-pocket costs of computers sold with three years of Internet service. The FTC said that some consumers ended up spending $869 for a computer advertised at $269. Although agreeing to change their ads, the three companies do not admit to having done anything wrong, and a Buy.com executive said, "We feel like our customers understood the promotion, and we received no complaints from the customers about the advertisement being misleading." (Reuters/New York Times 29 Jun 2000)

Category 15.1 Fraud

2000-09-01 **fraud hoax information warfare stock manipulation securities rumors forgery**

RISKS; NewsScan;Investors.com http://www.investors.com/editorial/tech05.asp 21 02

A former employee of online press release distributor Internet Wire was arrested [on the 31st of August] and charged with securities and wire fraud in connection with the distribution of a phony press release that sent a tech company's stock price plummeting last week. Shares of Emulex, a maker of fiber-optic equipment, lost up to 60% of their value, most of it during one 15-minute freefall, after some financial news services, including Dow Jones and Bloomberg, ran stories based on the release. The bogus release claimed the company had issued a profits warning, that it was being investigated by securities regulators, and that its CEO had stepped down. The stock eventually recovered most of its value after the company denied the reports. The suspect, 23-year-old Mark Jakob, allegedly used a computer at El Camino Community College to construct and send the release, and then initiated a series of trades that netted him profits of $240,000. (AP/Investors Business Daily 1 Sep 2000)

Category 15.1 Fraud

2000-09-07 **fraud hoax information warfare stock manipulation securities rumors forgery**

NewsScan

Days after arresting the California man responsible for the Emulex hoax, U.S. Securities and Exchange Commission officials conducted its fourth major "Internet sweep," taking action against 33 companies and individuals accused of using the Internet to defraud investors in classic "pump and dump" stock scams. Enforcers cited manipulation of more than 70 microcap or penny stocks, which are more loosely regulated than Big Board shares and have long been the target of illegal trading activities. "Thinly traded microcap stocks are particularly susceptible to online manipulations," says Richard H. Walker, SEC director of enforcement. "That's why we have made this area one of our highest enforcement priorities." The individuals and companies charged on Wednesday had allegedly reaped illegal profits totaling more than $10 million. Many of the individuals had no experience in stock trading, and included a bus mechanic, a college student and a car-service driver. (Financial Times 7 Sep 2000)

Category 15.1 Fraud

2000-10-24 **fraud background check e-commerce dot-com firms investigation background**

NewsScan, Financial Times http://news.ft.com/news/industries/infotechnology

Internet executives are four times more likely to have "unsavory backgrounds" than execs from other industries, according to a study by corporate security firm Kroll Associates. Over the past six months, Kroll has carried out 70 due diligence background checks of dot-com executives and board members, and about 39% — 27 people — were found to have problems — much higher than the typical 10% that Kroll expected. Problems included: violations of Securities and Exchange Commission rules, insurance fraud, undisclosed bankruptcies, frauds committed overseas, and even links to organized crime. In one of the most extreme cases, two people that Kroll was investigating because they had made an unsolicited offer to invest in a U.S. dot-com company were later murdered. "In the course of the law enforcement investigation they found the two were connected to penny stocks promotional scams and organized crime," says Ernie Brod, executive managing director of Kroll's New York office. Most of the problems were not associated with the inexperienced management teams who frequently run dot-coms, but rather with "gray beards" brought in to add stature to the company. "I refer to these people as vampire investors," said Brod. "Maybe they put a couple of bucks in, then they lick their lips at the opportunity and suck exorbitant consulting fees out of them, or put their relatives on the payroll." (Financial Times 24 Oct 2000)

Category 15.1 *Fraud*

2001-05-24 **Internet wire fraud money laundering investigation arrests law enforcement police**

NewsScan

FBI ARRESTS DOZENS FOR INTERNET FRAUD
The Federal Bureau of Investigation has in the past ten days charged 88 individuals with Internet crimes, including wire and mail fraud and money laundering. A government prosecutor said: "Internet fraud -- whether it's in the form of securities and other investment schemes, online auction and merchandising schemes, credit card fraud and identity theft -- has become one of the fastest-growing and most pervasive forms of white-collar crime." (Bloomberg News/The Washington Post, 24 May 2001)
http://washingtonpost.com/wp-dyn/articles/A67744-2001May23.html)

Category 15.1 *Fraud*

2001-06-18 **fraud Internet Web ISP misrepresentation**

NewsScan

NET ACCESS SCAM [18 Jun 2001]
The Federal Trade Commission is suing Illinois company New Millennium Concepts for using its Web site, Rhinopoint.com, to scam 59,000 customers. The alleged scam involved taking $10 to $16 signup fees from customers promised reduced Internet access charges for agreeing to complete monthly marketing surveys. The FTC charges that the company "rarely sent the promised surveys, even more rarely reimbursed consumers for their Internet access costs, but collected initial setup fees and personal information from tens of thousands of consumers anyway." (AP/USA Today 18 Jun 2001)
http://www.usatoday.com/life/cyber/tech/2001-06-18-net-access-scam.htm

---

Category 15.1 *Fraud*

2001-07-03 **pyramid fraud Ponzi Internet victims charges**

NewsScan

ANATOMY OF AN INTERNET SCAM [3 Jul 2001]
Federal investigators have charged 53-year-old mid-westerner Donald A. English with perpetrating an Internet-based "Ponzi" scheme that bilked tens of thousands of small investors out of $50 million. In a Ponzi scheme, early investors are paid phony "profits" from the money taken from other investors who follow them, after hearing about the huge, fast profits. Since no money is really being earned, the pyramid eventually collapses, when the supply of new investors diminishes. Many of the investors in English's operation, which was called EE-Biz Ventures, were people who are elderly or sick. One of them wrote: "I need at the least a full refund of the $3,000 spent if you do not intend to pay anyone back. Remember, I have cancer and am unable to work for the next six months." (New York Times 3 Jul 2001)
http://partners.nytimes.com/2001/07/03/business/03PONZ.html

Category 15.1 *Fraud*

2001-09-14 **online fraud scam bogus charities appeals**

NewsScan

SCAM ARTISTS SHOULD NOT DISCOURAGE ONLINE RELIEF EFFORTS
Though the problem's not widespread, there have been some e-mail marketing campaigns soliciting funds for bogus relief efforts. To make online donations to the Red Cross, use one of the official partnership sites the Red Cross has established with Amazon, AOL, Yahoo, or other respected organizations. (Wall Street Journal 14 Sep 2001)
http://interactive.wsj.com/articles/SB1000433930241803420.htm (sub req'd)

Category 15.1 *Fraud*

2001-10-18 **fraud Web advertising exploitation monitoring anthrax medication**

NewsScan

ANTHRAX WEB ADS MONITORED FOR ILLEGAL CLAIMS
The National Association of Boards of Pharmacy is monitoring Web sites that promote anti-anthrax drugs or suggest stockpiling them. The group's executive director says, "Most of the ads we've seen, we feel are illegal. They are offering medication without a valid prescription. We believe they are just capitalizing on all of the anthrax and bioterrorism fears." However, the Association acknowledges that there are online pharmacies that are completely legitimate and can be used to fill valid prescriptions made by certified physicians." (Reuters/USA Today 18 Oct 2001)
http://www.usatoday.com/life/cyber/tech/2001/10/18/anthrax-web-site-claims.htm

---

Category 15.1 Fraud

2002-02-25 **online fraud credit card charges debit checking lawsuit**

NewsScan

AOL ACCUSED OF CHARGING FOR UNWANTED GOODS [25 Feb 2002]
America Online has been named in a lawsuit for allegedly charging thousands of customers for merchandise, such as books and stereos, that they did not order. The suit, which is seeking class-action status, claims that AOL "unlawfully charged and collected money for this unordered merchandise and shipping and handling charges from credit card, debit card and checking accounts." The plaintiffs are seeking unspecified damages, the refund of unauthorized payments, and the consumers' retention of the unauthorized merchandise at AOL's expense. Meanwhile, an AOL spokesman said the "allegations are without merit and we intend to vigorously contest this lawsuit in court." (AP 25 Feb 2002)
http://apnews.excite.com/article/20020226/D7HTDUH80.html

Category 15.1 Fraud

2002-04-15 **fraud scam speculation foreign currency arbitrage consumer loss**

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/3067032.htm

BETTING MONEY ON MONEY
Speculation on foreign currencies is now a sport -- a dangerous one -- that can be played by small players who use Web sites to access the world's 24-hour currency markets. But financial experts advise investors to stick to blackjack or some slower way to lose their money. Harvard economist Dani Rodrik says, "I certainly wouldn't advise this for my mother-in-law. This is an area where it's much harder for an individual investor have a good nose for, than stocks or bonds." Unlike stock-trading, currency speculation is a zero-sum game (when you win, your opponents lose, and your opponents are mega-institutions such as Deutsche Bank, who know the game better that you ever will). There are also scam artists to watch out for, and in the past two years the U.S. Commodity Futures Trading Commission put a stop to schemes that had scammed 1,000 traders out of more than $60 million. (AP/San Jose Mercury News 14 Apr 2002)

Category 15.1 Fraud

2002-04-16 **Internet fraud complaints statistics 4-1-9 Nigerian online auctions**

NewsScan

INTERNET FRAUD
The Internet Fraud Complaint Center <http://www.ifccfbi.gov>, a partnership between the FBI and the National White Collar Crime Center, says that almost 50,000 complaints were filed last year on its site. About 2 out of 5 were related to online auctions, and 1 out of 6 involved the "Nigerian Letter Fraud," where the recipient of an Internet message gets a phony offer to make a big commission for helping the message sender transfer millions of dollars illegally out of Nigeria. (New York Times 15 Apr 2002)
http://www.nytimes.com/2002/04/15/technology/15SCAM.html

Category 15.1 Fraud

2002-05-21 **Internet pharmacy prescription prosecution international**

FindLaw Download This 86

CHARGES AGAINST INTERNET PHARMACY
In recent years, busloads of Americans have crossed into Canada to buy cheaper prescription drugs with help from Canadian doctors. Now many of those customers, mostly senior citizens facing large medicine bills, make that trip by the Internet, creating a growing industry that is attracting the attention of regulators. On May 14, the Ontario College of Pharmacists filed the province's first charges against a Web site selling prescription drugs, accusing it of doing so without a license. It is the initial salvo in what could be a lengthy battle over how to regulate the Internet prescription drug industry, raising questions about whether technology has advanced faster than the governing laws and policies.

http://news.findlaw.com/ap/ht/1700/5-19-2002/20020519130003_03.html

Explore FindLaw's Health Law Resources
http://www.findlaw.com/01topics/19health/index.html

Category 15.1 *Fraud*

2002-05-23 **4-1-9 Nigerian scam variant**

NewsScan

PHONY 'SOLDIER' NEEDS YOUR HELP GIVING HIM YOUR MONEY
A scam e-mail message now circulating the Internet purports to be from a "Special Forces Commando" in Afghanistan who's found $36 million in drug money while on patrol, and who wants your help in moving the cash. Sure he does. "We will thus send you the shipment waybill, so that you can help claim this luggage on behalf of me and my colleagues. Needless to say the trust in you at this juncture is enormous. We are willing to offer you an agreeable percentage of funds." Stop laughing, and grab onto your wallet. (AP/San Jose Mercury News 23 May 2002)
http://www.siliconvalley.com/mld/siliconvalley/3319360.htm

Category 15.1 *Fraud*

2002-06-06 **fraud hacking contest penetration criminal hackers**

Security Wire Digest 4 44

*HACKING CONTEST CHALLENGED
A Korean hacking contest is under fire for skimping on the prize money, exposing private data on contestants and maybe conning them with a false server running few activated services. When hackers "kill9" and "m0rla posted" discovered that the contest target network was an Apache server running few services on a non-standard port, they decided to break into the contest sponsor's host, Korea Digital Works (KDW). Among the duo's findings were personal data on the 1,240 contestants--319 of them from the United States. The event, sponsored by several Korean IT organizations, had promised $100,000 to the first contestant to hack into the decoy server or five $10,000 to those who made the best attempts. One winner, however, claims he's only been offered $1,250 and must provide bank details to collect it. That's made contestant Bill Wong of New York wonder if the message from KDW or the contest itself was an elaborate hoax. KDW earlier said contestants from 51 countries participated in the challenge and argues it hasn't mishandled the competition.

Category 15.1 *Fraud*

2002-07-15 **fraud education consumer warnings search engine**

NewsScan

FTC 'TEASER' SITES TAKE AIM AT UNWARY CONSUMERS
The Federal Trade Commission and the Securities and Exchange Commission have teamed up to create some number of "teaser" sites that pop up among the results on search engines when users type in requests for everything from "free vacations" to "erectile dysfunction cures." The teaser sites open with a page featuring "too-good-to-be-true" offers, and then when the unsuspecting user clicks for details, the screen switches to a young man holding out his hand to say "Stop!" with the headline "You could get scammed!". FTC attorney Eric Wenger says the ads represent the agency's attempt to reach consumers before they are victims of fraud. "We want to try to reach out to them and give them information that they can use to critically evaluate offers that they are receiving. And allow them to recognize and avoid deception before falling victim to it." He says the sites are designed to educate and empower consumers, not to make them feel silly or like they've been "had." The sites also provide links to complaint forms and tips provided by the FTC at www.ftc.gov. (CNN.com 11 Jul 2002)

Category 15.1 *Fraud*

2002-09-23 **4-1-9 Nigerian advance fee fraud embezzlement**

http://www.theregister.co.uk/2002/09/23/woman_falls_for_nigerian_scam/

A 59-year-old bookkeeper for a law firm in Michigan embezzled $2.1M and gave it all to Nigerian 4-1-9 scammers in the expectation of receiving $4.5M in stolen money. No matter how much she sent, there were always new "unexpected" charges holding up delivery of the shady money. She was arrested on 13 counts of fraud and faced up to three years in jail. Writer Lester Haines of the Detroit Free Press wrote, "Luckily for her, sheer idiocy will not be a factor in sentencing."

Category 15.1 *Fraud*

2002-12-06 **e-commerce Web advertising links pop-up banner ads alerts class-action lawsuit deception deceptive business practices**

NewsScan

LAWSUIT CHALLENGES DECEPTIVE AD-LINKS
A class action lawsuit has been filed against Internet portal Bonzi.com, accusing the company of tricking users into visiting its Web site by creating pop-up banner ads disguised as system alerts or security alerts, and directing people who click on the alert messages to the Bonzi site and its ads for software and other products. San Francisco lawyer Evan Cox, who specializes in Internet law, doubts the plaintiffs will be successful: "The approach is interesting, and there my be a lot of people out there rooting for the plaintiff on an emotional level, but the complaint is probably an uphill battle on most of its courses of action." Of course, the lawyers who filed the suit are more optimistic; one of them, Darrell Scott, says: "The Internet has unfortunately become a cornucopia for deceptive business practices. Class-based civil litigation will hopefully establish that the Internet is not, as some think, a sanctuary for those who engage in deception." (InfoWorld 5 Dec 2002)
http://www.infoworld.com/articles/hn/xml/02/12/05/021205hnsuit.xml?s=IDGNS

Category 15.1 *Fraud*

2003-10-31 **4-1-9 advance-fee fraud lottery scam**

http://www.theregister.co.uk/2003/10/31/pensioner_accused_of_aus_5m/

Nick Marinellis, a 39-year-old Australian man in Sydney has been charged with operating a 4-1-9 advance-fee fraud revolving around bogus lotteries, inheritances or "business opportunities." A Saudi prince reportedly contributed A$500K in "advance fees" in one case. Total theft was estimated to be more than A$5M.

Category 15.1 *Fraud*

2003-11-19 **Nigerian 4-1-9 scam victim $400,000 gullible fool**

RISKS 23 4

Old Nigerian scam nets $400,000

Arthur J. Byrnes and Peter G. Neumann report on the continued success of Nigerian scammers.

[For those of you who wonder why you keep getting variants of the confidential scam spams asking you to help launder millions of dollars, here is one of the reasons why: There are still suckers falling for them. PGN]

The *Daytona Beach News Journal* (13 Nov 2003) reported that a local man had fallen for the Nigerian 419 e-mail scam to the tune of $400,000. Even after being informed it was a scam, he continued to send money. He had mortgaged his house and used up his life savings. [PGN-ed]

The Risk? With no spam regulations and no cooperation between national governments con-men are getting away with many people's hard earned money. Some folks think that the greedy get what they deserve, but falling for this type of scam, may also be a sign of mental illness. [Gambling is addictive behavior. Perhaps so are Nigerian-type scams. PGN]

Category 15.1 *Fraud*

2004-01-05 **fraud internet Operation Cyber Sweep online economic crime**

NewsBits; http://www.latimes.com/technology/la-tr-internet4jan04,1,4364631.story

Fraud crackdown highlights fears over booking trips on Web Internet-related crime is a large and growing problem.

More than a third of the 218,000 fraud complaints the Federal Trade Commission received in 2002 were Web-related. In October, the FBI implemented Operation Cyber Sweep, a coordinated nationwide enforcement operation designed to crack down on the leading types of online economic crime. By November, it announced the arrests or convictions of more than 125 people. Investigators discovered more than 125,000 victims, with estimated losses totaling more than $100 million. (LA Times article, free registration required)

Category 15.1 *Fraud*

2004-01-05 **bribery IBM Korea**

DHS/IAIP Update

IBM execs, S. Korea officials accused of bribery

Some 48 South Korean government officials and corporate executives, mainly from IBM ventures, have been charged with bribery in a case involving state contracts for computer parts and servers, prosecutors said Monday. Fourteen government officials were bribed a total of $240,000 (290 million won) and an IBM Korea executive received golf memberships worth $82,000 from a subcontractor, prosecutors said. IBM Korea, a unit of IBM, said it did not condone the activities and that it had fired some staff involved in the case.

Category 15.1 *Fraud*

2004-02-04 **Internet fraud law Congress prison sentences copyright violation intellectual property rights**

NewsScan

CONGRESS TARGETS ONLINE FRAUD

The Fraudulent Online Identity Sanctions Act, sponsored by U.S. Reps. Lamar Smith (R-Texas) and Howard Berman (D-Calif.), would tack as much as seven years on to prison sentences handed down to fraudsters using the Internet to bilk unsuspecting users through a Web site registered under a false name or contact information, and would also allow copyright owners to seek larger monetary damages from fraudulently registered sites that distribute copyrighted material without permission. "The Government must play a greater role in punishing those who conceal their identities online, particularly when they do so in furtherance of a serious federal criminal offense or in violation of a federally protected intellectual property right," says Smith. The proposal could hit a snag if privacy advocates lobby against it, maintaining that private information such as home addresses and phone numbers should not be made available on the public "whois" domain name databases against the registrant's wishes. "Because of the way whois is currently structured, there are a lot of reasons why users might submit false information that have nothing to do with copyright infringement," notes Michael Steffen, a policy analyst at the Center for Democracy and Technology. (Washington Post 4 Feb 2004)

Category 15.1 *Fraud*

2004-02-12 **Net-harm Internet assasination hitlist Korea murder Website**

NewsScan

MURDER IN THE INFORMATION AGE

In Korea, police have arrested a 25-year-old college senior and charged him with operating a killer-for-hire Web site and taking thousands of dollars from his customers. In one case the student allegedly received the equivalent of $8,600 from a 22-year-old woman who wanted her ex-boyfriend and his wife murdered; in another there were discussions with a boy who wanted his father and stepmother killed. None of the murder plots was carried out. (AP/USA Today 12 Feb 2004)

[MK adds: I wonder who finally complained about the poor service? Can you imagine it? "Uh, Mr Policeman, I want to complain about a murder I ordered that has not been carried out."]

Category 15.1 *Fraud*

2004-02-25 **Microsoft fraud cyber crime warning businesses under attack criminals**

DHS IAIP Daily;
http://www.computerweekly.com/articles/article.asp?liArticleID=128636&liArticleTypeID=1&liCategoryID=2&liChannelID=22&liFlavourID=1&sSearch=&nPage=1

February 25, Computer Weekly — Businesses are under attack from cyber criminals, says MS security head.

Businesses worldwide face increasing threats from cyber criminals attempting extortion and fraud because the software running their systems makes them vulnerable, said Microsoft's top security architect at the e-Crime Congress in London. Security architect and chief technology officer of Microsoft's security business unit David Aucsmith admitted that he is considered a "target" for complaints against his company's software, but he also stressed that many of the security issues could not have been foreseen. Microsoft is addressing these security issues by working closely with law enforcement authorities and changing its patching procedures. Much of the threat comes from criminals who are making a career from high-tech crimes such as hacking, extortion and fraud, he said. The time between the release of a patch and the creation of an exploit has dwindled dramatically. Hackers have the advantage of not having to test their exploits, which allows them to move faster than suppliers who must perform rigorous testing to ensure that their patches do not break users' systems.

Category 15.1 *Fraud*

2004-03-09 **fraud Internet resumes CV curriculum vitae misrepresentation lies background checks hiring**

NewsScan

RESUME FRAUD GOES HIGH-TECH

As companies ratchet up efforts to detect misrepresentations on job seekers' resumes, resume fraud is jumping to a new level, thanks to operators of Web sites that provide phony degrees and toll-free numbers for employers to call, where they're assured that a job candidate's credentials are valid. Some candidates are even paying hackers to alter class lists at universities they claim to have attended, says Charles Wardell, managing director at Korn/Ferry International. "In the past, people just lied. Now, what they are doing is they are hacking into a class of a university and putting their name on the class list." Wardell says his company has started requesting degrees and, in some cases, even grades from potential job candidates, but such documents are also easily faked, thanks to the ingenuity of Web sites such as easydiploma.com, which offers phony degrees and a verification service. "You can select the parchment paper, the insignia and the type of degree," says the head of a corporate investigation firm's background screening division. Background search firms say these increasingly sophisticated resume fraud schemes are making their jobs more difficult: "A good liar understands that you have to have some basis and facts to pull off a scam. But it's even more dangerous when employers unknowingly hire a fraud, thief or a crook," says the president of Employment Screening Resources.

Category 15.1 Fraud

2004-03-10 **4-1-9 Nigerian advance fee fraud swindler stupidity**

http://www.theregister.co.uk/2003/03/10/419_scammers_take_us_con/

The Register published the following summary of a hilarious tale of stupidity and cupidity:

>419 SCAMMERS TAKE US CON ARTIST FOR $750,000
By Lester Haines
Published Monday 10th March 2003 15:07 GMT

A businessman in Winona, Minnesota, has been taken for a cool $750,000 by Nigerian 419 scam artists, the Winona Daily News reports.

Nothing new there, you might think, but $250,000 of the cash did not actually belong to victim Carl Fratzke. Incredibly, Fratzke had pulled a scam of his own and defrauded seven friends to raise the capital. The balance came from his own savings.

Tempted, as ever, by promises of riches beyond the wildest dreams of avarice, Fratzke asked chums to invest in a scheme whereby he would buy gloves and sell them to Wal-Mart at a hefty profit. He promptly sent the cash straight to the 419 scammers.

"They sent me a facsimile of the check they were going to send me," Fratzke later testified before a presumably astounded judge. "They said: 'This is coming'."

Well, it didn't, and now Fratzke faces sentencing on 31 March on "two counts of theft by swindle and one count of theft by check". If he's lucky, the beak will hand down a stiff sentence. Jail is probably the only place he'll be safe from his friends and investors — and his own stupidity.<

Category 15.1 Fraud

2004-03-31 **fraud confidence game swindle Nigerian 4-1-9 advance-fee fraud**

http://www.boston.com/news/local/massachusetts/articles/2004/03/31/man_arrested_in_alleged_investment_scam/

John Paczkowski, writing his column "Good Morning Silicon Valley" in the Silicon Valley Mercury News, wrote the following succinct summary of a tragic tale:

>…[F]ormer Dana-Farber Cancer Institute researcher and Harvard University professor. Weldong Xu, an academic who had done stints at both hallowed institutions, was arrested yesterday and charged with bilking friends and colleagues out of some $600,000 and then investing it in a questionable Nigerian business venture from which he expected a $50 million return. Xu allegedly persuaded a total of 35 people since last July to give him money, telling them it was for researching severe acute respiratory syndrome, before handing it over to the 419ers. "I tried to tell him he had been scammed," said Detective Steve Blair. "His plan all along was this Nigerian investment."<

<http://www.mercurynews.com/mld/siliconvalley/business/columnists/gmsv/8321286.htm?1c>

Category 15.1 Fraud

2004-04-27 **UK cybercrime law review organized crime gangs hacking spam virus-writing**

DHS IAIP Daily;
http://www.cnn.com/2004/TECH/internet/04/27/crime.britain.internet.reut/index.html

April 27, Reuters — UK to review cybercrime law.

Britain is to update its lone cybercrime law. Organized gangs around the world are honing their hacking, spamming and virus-writing skills while thinly stretched police resources are struggling to cope. The legal update will be closely watched by other countries, many of whose own laws against cybercrime are considered insufficient to fight what has become one of the fastest growing global crime waves. A group of parliamentarians will hold a public debate on Thursday, April 29, to explore ways to bring the Computer Misuse Act, or CMA, into the Internet era. Working with the UK's Home Office, the aim is to have a new cybercrime bill introduced in the next six months, MP Brian White said. Police say cybercrime costs UK industry hundreds of millions, and perhaps billions, of pounds annually. Globally, the figure is staggering, law enforcement officials say. "Serious and organized crime groups, and potentially terrorists, are moving into cyberspace simply because it's easier to hide there," said Simon Moores, a computer crime expert who works with the UK government. Thin resources, few convictions The need for an updated law is most evident to prosecutors and police. The Home Office said there were just 14 convictions under the CMA in 2002, the last year statistics were tallied.

Category 15.1 Fraud

2004-04-29 **fraud data mining banking FinCEN**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/25782−1.html

April 29, Government Computer News — Financial Crimes and Enforcement Network plans to modernize Bank Secrecy Act database.

The Department of Treasury's Financial Crimes and Enforcement Network (FinCEN) plans to update its computer database next year with a new data retrieval system, along with applications that will perform deeper analysis and improve data-mining capabilities. Banks report suspicious activity and other data through FinCEN's U.S.A.P.A.T.R.I.O.T. Act Communications System, including when customers make unusually large deposits or withdrawals. Law enforcement agencies can access and download the confidential information in FinCEN's database to help uncover and track terrorist financing. Bank Secrecy Act (BSA) Direct, which is basically a data warehouse, will make the information more easily accessible and understandable to law enforcement while securing the information from unauthorized users, according to FinCEN director William Fox.BSA Direct will also alert FinCEN to irregularities in Bank Secrecy Act reports submitted by financial institutions, and will audit use of the accessed data to ensure that it is not misused, Fox said. A networking function will link different law enforcement entities that are accessing the same data to avoid overlap or conflict in investigations. FinCEN expects to have BSA Direct online in the fall next year, Fox said.

Category 15.1 Fraud

2004-05-17 **fraud online job listings identity theft credit card theft**

DHS IAIP Daily; http://www.nytimes.com/2004/05/17/technology/17ecom.html

May 17, New York Times — Fraud in online job listings.

Online job sites like Monster.com, CareerBuilder and HotJobs have given employers another way to find workers, but it turns out that crime rings are making use of the sites, too. In a recent swindle, for instance, credit card thieves found unwitting money launderers through Monster.com, then left their "employees" on the hook for thousands of dollars in debts and possible criminal liability when the fraud was discovered. Federal authorities said the recent swindle was one they had not yet seen. Molly S. McMinn, an inspector for the United States Postal Inspection Service said this type of fraud was "a new twist on an old idea" of credit card thieves from foreign countries buying merchandise from online merchants with card numbers stolen from American citizens and having the merchandise shipped to associates in the United States. McMinn said fraud rings would recruit associates by putting ads on job sites for "reshippers," who, in exchange for a fee, mail the merchandise to Ukraine, Indonesia or other countries known by online merchants as hotbeds of Internet fraud. By using middlemen based in the United States, criminals can escape detection by merchants.

Category 15.1 Fraud

2004-05-27 **ATM scam casino organized crime theft fraud**

DHS IAIP Daily; http://www.lasvegassun.com/sunbin/stories/lv−crime/2004/may/ 27/516925888.html

May 27, Las Vegas Sun — Eleven sought in ATM, casino scam.

The FBI continues to search for 11 people named in two federal racketeering indictments alleging two Romanian crime rings are using stolen credit cards and false identification to bilk hundreds of thousands of dollars from Las Vegas, NV, casinos and ATMs. The indictments allege the credit card rings sent out runners across the country to steal credit cards that were then transported to Las Vegas, where they were used with fake driver's licenses to obtain cash advances at casinos and from automated teller machines. The groups liked to prey on people at fitness centers, where credit cards were easily taken from lockers while people worked out, or from cars parked at trail heads at recreation areas, Assistant U.S. Attorney Tim Vasquez said. On Tuesday, May 25, the FBI seized computers, printers, digital cameras, lock-picking tools, laminators, credit cards, ATM components and an ATM from the Las Vegas homes of the six people arrested in Las Vegas. "We believe they used the ATM machine to practice one of their newer techniques, which was using skimming devices," Vasquez said.

Category 15.1 Fraud

2004-06-02 **Internet scam fraud John Grisham novel plot "The Brethen"**

NewsScan

INTERNET SCAM FOLLOWS PLOT OF GRISHAM NOVEL

"I think the public needs to be protected from you," U.S. District Judge Ellen B. Burns told Steven Smith, a Connecticut man who posted Internet personal ads in which he pretended to be a gay man rejected by his parents and looking for guidance from older men. When men responded to the ads Smith told them he was in jail and needed money to be released. The scam echoes the plot of a John Grisham novel called "The Brethren," in which the perpetrators of a similar scam unknowingly ensnare a presidential candidate, from whom they then attempt to extort money as he gains front-runner status.
(AP/USA Today 2 Jun 2004)

Category 15.1 Fraud

2004-06-04 **Nigerian 4-1-9 scam software Nigeria government catch banking petroleum industry**

NewsScan

NIGERIA MAY USE SOFTWARE TO NAB SCAMMERS

Nigeria plans to launch software that will search for certain keywords to help catch fraud perpetrators who send scam letters via e-mail. Nigerian official Mustafa Bello explains: "The introduction of new software, currently under discussion within the Nigerian parliament, will scan e-mails originating in Nigeria to look for keywords commonly found, especially relating to banking and the country's petroleum industry. This will then be removed from the system and even traced back to where it originated." (The Age 4 Jun 2004) Rec'd from John Lamp, Deakin U.

Category 15.1 Fraud

2004-07-29 **extortion fraud Russia British bookmaker denial-of-service threat e-mail**

NewsScan

RUSSIAN EXTORTIONISTS: EACH DID HIS BIT OF WORK

Police authorities in Russia have broken up a hacker ring that extorted money from British bookmakers by flooding online betting sites with false requests for information in "denial-of-service" attacks and then sending e-mail demanding money for stopping the attacks. Investigators said that
bookmaker companies were the most convenient prey because the attacks could be timed to major sport events. The ring consisted of well-educated people in their early 20s who had found each other on the Internet and agreed to work together in the extortion. A Russian police official said: "There was no chief organizer in plain terms, each of them did his bit of work. And they didn't consider themselves criminals." (AP 29 Jul 2004)

Category 15.1 Fraud

2004-08-26 **Internet crime identity theft hacking phishing Operation Web Snare**

DHS IAIP Daily;
http://story.news.yahoo.com/news?tmpl=story2&u=/nm/20040826/
wr_nm/crime_internet_dc

August 26, Reuters — U.S. says over 100 arrested in Internet crime sweep.

More than 100 people have been arrested in the largest global crackdown to date on identity theft, hacking and other Internet-based crimes, Attorney General John Ashcroft said on Thursday, August 26. The arrests followed a three-month investigation into a range of crimes from reselling co-workers' Social Security numbers to disabling Websites, Ashcroft said. The crackdown, dubbed "Operation Web Snare" cost some 150,000 victims more than $215 million, Ashcroft said, adding that 53 people had already been convicted. Phishing, the sending of e-mails designed to look like they are from legitimate financial institutions, and identity theft were two of the major schemes targeted. Law enforcement officials in Romania, Nigeria and Cyprus helped track down people involved in fraudulent auctions, trafficking in stolen credit card numbers and other crimes, Ashcroft said.

Category 15.1 Fraud

2004-10-05 **e-mail scam fraud US elections Czech Republic origin**

DHS IAIP Daily; http://news.bbc.co.uk/1/hi/technology/3714944.stm

October 05, BBC News (UK) — E-mail scam plays on U.S. elections.

People are being warned about a scam e-mail which uses the U.S. presidential poll to con them out of their money. A junk e-mail invites people to dial a premium rate number to express their support for President George W. Bush or Senator John Kerry. E-mail filtering firm BlackSpider estimates that almost a quarter of a million are being sent out every day. BlackSpider Technologies said it had traced some of the e-mails to a server in the Czech Republic. "This is a relatively new scam," said BlackSpider CEO, John Cheney.

Category 15.1 Fraud

2004-11-11 **bride Russia e-mail prosecution trial suspended sentence dating cybersex seduction 4-1-9 Nigerian scam**

NewsScan; http://theage.com.au/articles/2004/11/11/1100131119740.html

ONLINE BRIDE SCAM

A Russian man who netted $300,000 by faking emails from prospective brides to unsuspecting foreigners was caught by Moscow police but received only a one-year suspended sentence. Yury Lazarev, 34, an English translator from the Urals, employed women to write flowery, romantic messages signed with real names picked off web dating sites. The photographs of seductive women that accompanied the text caught the attention of some 3000 men from New Zealand, Australia, Canada, the United States and other countries. Once a prospective victim got interested and wanted to meet his potential fiancé, the fictitious woman would ask for financial help in paying for visas and airline tickets. (The Age 11 Nov 2004)

[MK notes: this is a variant of the notorious "Nigerian 4-1-9" or "advance-fee" fraud.]

Category 15.1 Fraud

2004-12-15 **US Time Warner AOL SEC Securities Exchange Commission fraud accounting civil lawsuits criminal prosecution settlement**

NewsScan; http://www.nytimes.com/2004/12/15/business/media/15media.html

U.S. AND TIME WARNER: LET'S SETTLE UP

Time Warner has agreed to settle with the government in two separate cases: the Justice Department's investigation of whether AOL's advertising deals with smaller Internet companies were used to exaggerate AOL growth, and the SEC's investigation into accounting irregularities at the company. Time Warner is expected to pay $500- 600 million to settle all civil and criminal accusations with the two agencies. (New York Times 15 Dec 2004)

Category 15.1 Fraud

2004-12-29 **hoax spam disaster warning authentication phishing**

RISKS 23 65

WARNING ABOUT WARNINGS

Shortly after the Asian Tsunami of December 2004, Geoffrey Brent warned RISKS readers about the vulnerability of unsophisticated populations to official-looking fake warnings about natural disasters. He had received junk e-mail beginning "THIS IS AN OFFICIAL WARNING! A huge 300 ft. High ocean wave is moving towards your continent. . . ." Commented Brent, "But in the wake of this week's tragedy, it reminds me that there is no end to opportunism. I'm sure we'll see that particular message recycled; spammers aside, there are several obvious reasons why somebody might find it convenient to trigger a mass evacuation. (Looting, terrorist attack on traffic choke points, etc etc…) We know what false alarms do to the effectiveness of warning schemes. Any warning system needs to incorporate authentication - which also means limiting its distribution to people who *will* check authenticity rather than taking it on trust."

Category 15.1 *Fraud*

2005-01-06 **tsunami fraud Internet relief charity scam disaster relief**

NewsScan;
http://www.nytimes.com/2005/01/06/international/worldspecial4/06fbi.html?oref
=login

BEWARE TSUNAMI INTERNET FRAUDS

The FBI has issued a warning about online frauds that try to capitalize on the recent tsunami disaster by offering to help tsunami victims or relatives for a fee. Audri Lanford of ScamBusters.org comments: "Within hours of 9/11 we had the 9/11 scams. We've seen them for every major disaster." (New York Times 6 Jan 2005)

Category 15.1 *Fraud*

2005-04-08 **fraud indicments E-Rate program NEC Justice Department**

EDUPAGE; http://online.wsj.com/article/0,,SB111292755907301701,00.html

E-RATE INDICTMENTS HANDED DOWN

Six companies and five individuals have been indicted on charges of fraud in the federal E-Rate program, which was instituted to provide funds to connect public schools and libraries to the Internet. A year ago, a subsidiary of NEC admitted defrauding the program and settled with prosecutors for $20.7 million. Those indicted this week were charged with fraud, collusion, and rigging bids. According to the Justice Department, the accused misrepresented financial terms of E-Rate projects to school administrators and colluded on pricing and terms of government contracts. The violations are said to have taken place in seven states, though all but one defendant are based in California. The individuals charged face up to five years in prison, and the indicted companies could be fined as much as $10 million. Wall Street Journal, 8 April 2005 (sub. req'd)

Category 15.1 *Fraud*

2005-05-11 **NCAA online course cheating fraud student athletes Nicholls State University Louisiana**

EDUPAGE; http://www.insidehighered.com/news/2005/05/11/nicholls

NCAA FINDS ONLINE COURSE FRAUD

An investigation of student athletes at Nicholls State University in Louisiana has revealed that students and university staff had engaged in "gross academic fraud" by fraudulently completing online courses to preserve the students' eligibility for sports. The university's registrar discovered the fraud after noticing that many student athletes were completing online courses from Brigham Young University (BYU), often with much higher grades than for classes they took at Nicholls. As it turned out, two coaches and an academic adviser were giving students answers for the courses and in some cases serving as proctors for the students' tests. The National Collegiate Athletic Association (NCAA) confirmed the fraud and imposed penalties on the school's athletic programs, but the episode has raised a red flag about the potential for similar abuse of online programs. "There appeared generally not to be sufficient monitoring either by BYU or … by Nicholls State," according to Josephine Potuto, member of the NCAA panel that conducted the investigation. A statement from the panel noted, "This case illustrates the ease with which individuals can manipulate and then breach security protocols for online correspondence courses." Inside Higher Ed, 11 May 2005

Category 15.1 *Fraud*

2005-09-08 **hurricane Katrina disaster fraud scam FBI warning Internet sites Task Force**

DHS IAIP Daily; http://www.msnbc.msn.com/id/9229950/

KATRINA NET SCAMS MULTIPLYING, FBI WARNS

There has been a significant increase in Internet sites purporting to be charities related to Hurricane Katrina. FBI assistant director Louis M. Reigel stated there were roughly 2,300 Katrina-related sites by midday Thursday. As of last week the FBI had recieved 250 complaints at its Internet complaint center about hurricane-related charities. Due to this the Justice Department has established a Hurricane Katrina Fraud Task Force that will focus on phony charities, identity theft, insurance scams and government benefit fraud.

Category 15.1 Fraud

2005-11-03 **hacker fraud botnet software computer compromise lawsuit**

DHS IAIP Daily; http://www.securityfocus.com/news/11353

MAN ACCUSED OF SELLING BOT SOFTWARE TO COMPROMISE COMPUTERS

Federal authorities have arrested an accused man of creating bot software to compromise nearly 400,000 Windows computers and then using his control of the systems to garner more than $60,000 in profits. James Aquilina, Assistant U.S. Attorney for the Central District of California and the prosecutor on the case stated, "This is the first case to charge someone for using bots for generating profits. On the one hand, he is selling bots to other people so that they can (perform) denial-of-service attacks and spam to make money. And on the other hand, he is using bots to make affiliate income." Over nearly a year, the man allegedly used automated software to infect Windows systems, advertised and sold access to the compromised PCs, and used the software to perpetrate click fraud, garnering tens of thousands of dollars in affiliate fees.

Category 15.1 Fraud

2006-01-18 **online fraud zero liability stock broker E*Trade Securities and Exchange Commission**

EDUPAGE; http://www.nytimes.com/2006/01/18/technology/18data.html 23

ONLINE BROKER TO COVER FRAUD LOSSES

Online stock broker E*Trade has announced a "zero liability" policy in which it will cover all losses resulting from online fraud. Although some other online brokerage firms said they have absorbed some or all of the costs of fraud in past incidents, E*Trade becomes the first to establish such a policy. Losses due to fraud in the online brokerage industry remain relatively small and are a fraction of losses to credit card fraud, but the number of data breaches is rising. Moreover, when people are victimized through brokerage fraud, they are harmed "to the tune of hundreds of thousands of dollars," according to Gerri Walsh, acting director of the Securities and Exchange Commission's Office of Investor Education. Officials at E*Trade said they expect other brokers will follow suit and implement similar policies, bringing the entire industry to a level similar to that of credit card companies. A federal law passed in the 1970s requires issuers of credit cards to limit customer liability to $50, but most issuers cover all losses.

Category 15.1 Fraud

2006-02-10 **hacker indictment hospital botnet attack computer fraud**

DHS IAIP Daily; http://security.ithub.com/article/DOJ+Indicts+Hacker+for+Hospital+Botnet+Attack/171336_1.aspx 23

HACKER INDICTED FOR HOSPITAL BOTNET ATTACK.

A 20-year-old California man was indicted in Seattle Friday, February 10, on charges that he used a computer "bot" network to cause computer malfunctions at Seattle's Northwest Hospital in January of 2005. Christopher Maxwell, of Vacaville, CA, was indicted by a federal grand jury on two counts of conspiracy to cause damage to a protected computer and commit computer fraud. He is alleged to have compromised computers at a number of U.S. universities for a large botnet that generated $100,000 in payments from advertising software companies, according to a statement released by the U.S. Attorney's Office for the Western District of Washington. Maxwell is alleged to have hacked computer networks at California State University, Northridge; the University of Michigan; and University of California, Los Angeles, using high-powered computers on those networks as part of an adware distribution operation.

Category 15.1 Fraud

2006-03-02 **FCC fake caller ID probe fraud Communications Act NuFone TeleSpoof**

DHS IAIP Daily; http://www.wired.com/news/technology/0,70320−0.html?tw=rss.technology 23

FCC PROBES CALLER-ID FAKERS.

Last week the Federal Communications Commission (FCC) opened an investigation into the caller-ID spoofing sites -- services that began popping up late 2004, and have since become a useful tool for private investigators, pranksters and more than a few fraud artists. A seven-page demand from the FCC's enforcement bureau sent to one such service, called TeleSpoof, says the commission is investigating whether the site is violating the federal Communications Act by failing to send accurate "originating calling party telephone number information" on interstate calls. A copy was also sent to VoIP service provider NuFone. The FCC is demanding business records from both companies, as well as the name of every customer that has used TeleSpoof, the date they used it and the number of phone calls they made.

Category 15.1 *Fraud*

2006-04-20 **technology director charges settlement E-rate program fraud Department of Justice DoJ**

EDUPAGE; http://www.internetnews.com/bus-news/article.php/3600671 23

TECHNOLOGY DIRECTOR CHARGED WITH E-RATE FRAUD

Federal charges have been brought against a technology director in South Carolina for defrauding the E-rate program, a federal program to fund technology improvements in disadvantaged schools. Cynthia K. Ayer was indicted on 12 counts of mail and wire fraud for funneling contracts worth $3.5 million to her company, Go Between Communications. According to the Department of Justice (DOJ), Ayer's actions netted her more than $450,000 of E-rate funds. Ayer faces fines of $250,000 and a lengthy prison term if convicted. The E-rate program has been riddled with accounts of fraud and abuse, and Ayer's case is just the latest in a string of prosecutions against 11 individuals and 10 companies. Thus far, settlements with some defendants have totaled $40 million in fines and restitution, and two individuals have been sentenced to prison terms.

Category 15.1 *Fraud*

2006-04-21 **charges settlement E-rate program fraud Department of Justice DoJ**

EDUPAGE; http://www.itworld.com/Man/2681/060421erate/ 23

COMPANY TO PAY $4.5 MILLION IN E-RATE FRAUD CASE

Houston-based NextiraOne has agreed to pay $4.5 million to settle charges that it defrauded the government and the Oglala Nation Educational Coalition through the federal E-rate program. The work for which NextiraOne was under investigation took place at the Pine Ridge Reservation in South Dakota. According to a complaint by the Department of Justice, NextiraOne billed the government for products and services it did not deliver; submitted fraudulent invoices; and charged inflated prices for other products. The E-rate program, designed to extend Internet access to schools and libraries that could not otherwise afford it, has come under fire for what some have described as rampant fraud. Under the settlement, NextiraOne will pay a criminal fine of $1.9 million and will return $2.6 million to the government.

15.2 Extortion

Category 15.2 *Extortion*

1999-10-15 **indictment extortion teenager threats bomb Internet**

AP via Las Vegas Sun
http://www.lasvegassun.com/sunbin/stories/text/1999/oct/15/101500270.html

Jahair Joel Navarro, an 18-year-old from New York state, was indicted in White Plains on charges of extortion. He allegedly threatened to bomb Microsoft and IBM headquarters unless each company paid him $5M. An FBI raid on the lad's apartment found no bombs but only the usual instructions on bomb-making downloaded from the Internet.

Category 15.2 *Extortion*

2000-01-12 **Web penetration extortion revenge credit-card confidentiality**

AP, NewsScan, PR releases, InternetNews, New York Times, Daily Telegraph (Australia)

A 19-year-old Russian criminal hacker calling himself Maxus broke into the Web site of CD Universe and stole the credit-card information of 300,000 of the firm's customers. According to New York Times reporter John Markoff, the criminal threatened CD Universe: "Pay me $100,000 and I'll fix your bugs and forget about your shop forever....or I'll sell your cards [customer credit data] and tell about this incident in news." When the company refused, he posted 25,000 of the accounts on a Web site (Maxus Credit Card Pipeline) starting 1999-12-25 and hosted by the Lightrealm hosting service. That company took the site down on 2000-01-09 after being informed of the criminal activity. The criminal claimed that the site was so popular with credit-card thieves that he had to set up automatic limits of one stolen number per visitor per request. Investigation shows that the stolen card numbers were in fact being used fraudulently, and so 300,000 people had to be warned to change their card numbers.

Category 15.2 *Extortion*

2000-01-15 **criminal hacker investigation extortion theft proprietary information data source code**

PA, Sunday Times (London)

In September 1999, the Sunday Times reported in an article by Jon Ungoed-Thomas and Maeve Sheehan that British banks were being attacked by criminal hackers attempting to extort money from them. The extortion demands were said to start in the millions and then run down into the hundreds of thousands of pounds. Mark Rasch is a former attorney for computer crime at the United States Department of Justice and later legal counsel for Global Integrity, the computer security company that recently spun off from SAIC. He said, "There have been a number of cases in the UK where hackers have threatened to shut down the trading floors in financial institutions. . . . The three I know of (in London) happened in the space of three months last year one after the other. . . . In one case, the trading floor was shut down and a ransom paid." The International Chamber of Commerce (ICC) confirmed it had received several reports of attempted extortion. Ungoed-Thomas and Sheehan quoted Pottengal Mukundan, ICC Director of Commercial Crime Services, as saying, "We have had cases of extortion and the matter has been investigated internally and the threat removed. . . . I don't think you will find there are many companies which admit to having a problem." Finally, the authors spoke with Edward Wilding, Director of Computer Forensics at Maxima Group; he said, "Computer extortion is not rife, but we do get called to assist in incidents where extortionists have attempted to extract money by the use of encryption and where databases of sensitive information have been stolen."

According to Padraic Flanagan of the British Press Association in mid-January 2000, UK police were investigating a dozen attempts by criminal hackers to extort funds from multinational companies in Britain.

Category 15.2 Extortion

2000-01-18 **criminal hacker penetration bank extortion credit card**

AP, Dow Jones, RISKS 20 75

In January, information came to light that VISA International had been hacked by an extortionist who demanded $10M for the return of stolen information — information that VISA spokesperson Chris McLaughlin described as worthless and posing no threat to VISA or to its customers. The extortion was being investigated by police but no arrests had been made. However, other reports suggested that the criminal hackers stole source code and could have crashed the entire system. In a follow-up on RISKS, a correspondent asked, ". . . [What source code was *stolen*? It is extremely unlikely that it was *the source code for the Visa card system* as stated! There is no such thing. Like any system, it would consist of many source libraries, each relating to different modules of the overall system. So we should be asking what source was copied? (You can hardly say it was *stolen*, as that would imply that it was taken away, leaving the rightful owner without possession of the item of stolen property, and we all know that is not what happens in such cases. In a shop like Visa, the code promotion system maintains multiple copies in the migration libraries, so erasure of the sole copy is highly unlikely)."

Category 15.2 Extortion

2000-01-25 **extortion cryptanalysis smart card counterfeit theft fraud**

NewsScan, MSNBC, ZDNet
http://www.zdnet.com/zdnn/stories/news/0,4586,2428429,00.html, Crypto-Gram
http://www.counterpane.com/crypto-gram-0002.html

French programmer Serge Humpich spent four years on the cryptanalysis of the smart-card authentication process used by the Cartes Bancaires organization and patented his analysis. When he demonstrated his technique in September 1999 by stealing 10 Paris Metro tickets using a counterfeit card, he was arrested. The man had asked the credit-card consortium to pay him the equivalent of $1.5M for his work; instead, he faced a seven-year term in prison and a maximum fine of about $750,000 for fraud and counterfeiting (although prosecutors asked for a suspended sentence of two years' probation and a fine of approximately U$10,000). He was also fired from his job because of the publicity over his case. In late February 2000, he was given a 10-month suspended sentence and fined 12,000 FF (~U$1,800).

Category 15.2 Extortion

2000-12-13 **penetration confidentiality credit card theft extortion**

NewsScan, New York Times
http://partners.nytimes.com/2000/12/13/technology/13HACK.html, MSNBC

The FBI . . . [began] searching for a network vandal who stole 55,000 credit card numbers from a private portion of the Creditcards.com Web site and published them on the Internet after the company refused to pay the intruder money in order to keep the information from being circulated. . . .." (New York Times 13 Dec 2000)

The attack began in August 2000 but the revenge posting of the numbers occurred only in December. The criminal demanded $100,000 in extortion money and also claimed on a Web site that he was trying to obtain a contract for improving network security: "Michael Butts says I need to talk to Michael Stankewitz from COO [sic]...I told him that O want to help creditcards.com, he had my price and he knew my deal," the Web page reads. "He knew what kind of information we had from their servers. I would destroy it all after the agreement was made and provide network security. Now, I didn't receive any payment from creditcards.com and I am going to make them bankrupt."

Category 15.2 Extortion

2001-03-02 **securities fraud Internet Web SEC investigation prosecution**

NewsScan

SEC REMINDS INVESTORS: THE NET CAN BE A DANGEROUS PLACE
The Security and Exchange Commission (SEC) finished its fifth nationwide Internet fraud sweep by charging 23 companies and individuals with using spam e-mail messages, electronic newsletters and message boards, and other Internet media to pump up stock prices and defraud investors. The SEC's enforcement officer called the new cases "a sobering reminder for investors that, on the Internet, there is no clearly defined border between reliable and unreliable information." (New York Times 2 Mar 2001)
http://partners.nytimes.com/2001/03/02/technology/02NET.html

Category 15.2 *Extortion*

2001-03-02 **credit card theft international blackmail extortion**

NewsScan

CREDIT CARD THEFT RING
The FBI says an organized ring of hackers based in Russia and the Ukraine has stolen more than a million credit card numbers from 40 sites in 20 states over the last few months, and attempted to blackmail the targeted businesses by threatening to embarrass them publicly. The intrusions have been made using a well-known vulnerability that existed in the Windows NT operating system. Free patches to prevent intrusion can be found at www.microsoft.com. (Washington Post 9 Mar 2001)
http://washingtonpost.com/wp-dyn/articles/A43993-2001Mar8.html

---

Category 15.2 *Extortion*

2001-03-09 **patent intellectual property extortion lawsuits threats**

NewsScan

TINY COMPANY CRITICIZED FOR 'PATENTMAIL'
A little-known company called TechSearch has found a new gimmick for making money off the Net -- it's using a 1993 patent that covers a basic process for sending files between computers to demand license payments from big-name companies, including The Gap, Walgreen, Nike, Sony, Playboy Enterprises and Sunglass Hut. Other less-willing contributors include Audible, Encyclopaedia Britannica and Spiegel, which were threatened with litigation when they refused to pay up. "We chose to settle the lawsuit rather than move forward with potentially costly litigation," says a Britannica spokeswoman. Following complaints that the patent is invalid, the U.S. Patent and Trademark Office reached an initial decision late last month to void it, but TechSearch has amassed a collection of 20-some other patents that it can use to extract payments. It's filed several lawsuits against major electronics firms based on a 1986 patent on "plug and play" technology, and has initiated litigation with several distance learning providers based on a 1989 patent that broadly covers computer-based educational techniques. TechSearch founder Anthony Brown says his methods, although aggressive, are perfectly legal, and the company's law firm says it's won $350 million in settlements in a string of jury verdicts over the last six years. Critics have labeled the company's techniques "extortionate" and "patentmail." (Wall Street Journal 9 Mar 2001)
http://interactive.wsj.com/articles/SB984094820806670333.htm (sub req'd)

Category 15.2 *Extortion*

2002-06-18 **DNS Domain Name System governance control confidentiality sequestration password cryptographic key**

FindLaw Download This 90

CULT HERO HOLDS DOMAIN HOSTAGE
The administrator of South Africa's web addresses said on Thursday he had hidden the key to the country's ".ZA" domain network abroad to prevent any government interference in access to the Internet. South Africa's parliament has given initial approval to a law that will allow the government to take control of the country's Internet address administration. But critics, including ZA domain-name administrator Mike Lawrie, say the government has no right to stage the takeover and warn it could collapse the domestic Internet structure.
http://zdnet.com.com/2100-1105-935968.html

South African Legal Resources
http://www.findlaw.com/12international/countries/za.html

Category 15.2 *Extortion*

2003-07-29 **movie piracy Malaysia extortion impersonation**

NewsScan

THE MOVIE PIRATES
An unanticipated by-product of Malaysia's campaign against the sale of illegal video discs is the rise of extortionists who impersonate law enforcement officers on surprise checks and demand 50 ringgit (US$13) for each illegal disc they find. Illegal copying of movies and computer software is pervasive in Malaysia and cheap versions of the latest Hollywood, Indian and Hong Kong films have been widely available at street stalls and in stores. (AP/San Jose Mercury News 29 Jul 2003)

Category 15.2 Extortion

2003-08-25 **steganography extortion anonymizer credit card forgery e-mail**

http://www.expatica.com/index.asp?pad=2,18,&item_id=33655

In June 2003, a high-tech extortionist in the Netherlands threatened to poison the products of the Campina food company in Utrecht unless he were paid €200,000. The steps for payment used an unusual degree of technical sophistication:

1. Campina had to open a bank account and get a credit card for it.
2. The victims deposited the payoff in the bank account.
3. They had to buy a credit card reader and scan the credit card to extract the data from the magnetic strip.
4. Using a steganography program and a picture of a red VW car sense by the criminal, the victims encoded the card data and its PIN into the picture using the steganographic key supplied with the software.
5. They then posted the modified picture in an advertisement on a automobile-exchange Web site.
6. The criminal used an anonymizing service called SURFOLA.COM to mask his identity and location while retrieving the steganographic picture from the Web site.

The victims worked with their local police, who in turn communicated with the FBI for help. The FBI were able to find the criminal's authentic e-mail address along with sound financial information from his PAYPAL.COM account. Dutch police began surveillance and were able to arrest the 45-year-old micro chip designer when he withdrew money from an ATM using the forged credit card.

Category 15.2 Extortion

2004-02-26 **data theft extortion Japan arrest customer information organized crime**

RISKS 23 22

4.6-MILLION DSL SUBSCRIBERS' DATA LEAKED IN JAPAN

Tokyo Metropolitan Police arrested three meno n suspicion of trying to extort up to 3 billion yen (U.S. $28 million) from Softbank. The suspects claimed that they obtained DVD and CD disks filled with 4.6 million Yahoo BB customer information. Two of the suspects run Yahoo BB agencies which sells DSL and IP Telephone services…. According to Softbank, the stolen data includes name, address, telephone number, and e-mail. No billing or credit card information was leaked. However, there were indications that the suspects could be linked to organized crime (the Yakuza).

Category 15.2 Extortion

2004-03-20 **extortion fraud spoofing advertising software malware arrest arraignment trial**

http://www.siliconvalley.com/mld/siliconvalley/8234511.htm

COMPUTER PROGRAMMER ARRESTED FOR EXTORTION AND MAIL FRAUD SCHEME TARGETING GOOGLE, INC.

Extracts from the press release from the US Department of Justice, March 18, 2004

The United States Attorney for the Northern District of California announced … that Michael Anthony Bradley, 32, of Oak Park, California, was arrested … [on March 17] on a criminal complaint filed in San Jose charging him with interfering with commerce by threats or violence in violation of 18 U.S.C. § 1951, and mail fraud in violation of 18 U.S.C. 1341….

According to the criminal complaint, which was unsealed in San Jose today, Mr. Bradley attempted to defraud and extort money from Google, the Internet company best known for its free search engine, by developing a software program that automates fraudulent "clicks" on "cost-per-click" advertisements utilized by Google. These fraudulent clicks, in turn, were designed to cause Google to make payments that were supposed to be made only for "clicks" made by legitimate Web surfers.

The complaint alleges that Mr. Bradley first sent an email requesting a meeting with Google concerning his software program, which he named Google Clique, in early March. In a subsequent face-to-face meeting with Google engineers on March 10, the complaint alleges that Mr. Bradley performed a demonstration of his program, and claimed that it generated false clicks that look like real Internet traffic and were untraceable. The defendant allegedly stated that he would sell it to top spammers if Google did not pay him $100,000, and that Google would lose millions.

The maximum statutory penalty for each violation of 18 U.S.C. §§ 1341 and 1951 is 20 years imprisonment and a fine of $250,000…."

Category 15.2 *Extortion*

2004-03-23 **computer crime threat Google California**

NewsScan

THREATEN GOOGLE, GET ARRESTED

Federal law enforcement officials in California have arrested a 32-year-old man who demanded $100,000 from Google Inc. and threatened to "destroy" the company by using a a software program to fake traffic on Internet ads. The man's program automated phony traffic to cost-per-click ads Google places on websites and caused Google to make payments to Web sites the man had set up. Released on $50,000 bail, he faces up to 20 years in prison and a $250,000 fine. (Bloomberg News/Los Angeles Times 23 Mar 2004)

Category 15.2 *Extortion*

2004-05-26 **organized crime fraud identity theft extortion**

DHS IAIP Daily;
http://www.theage.com.au/articles/2004/05/26/1085461818627.h tml

May 26, Australian Associated Press — Mobsters targeting Australians online.

Australians are being targeted by Eastern European organized crime families using the internet to extort and steal far from home. Delegates at the annual AusCERT Asia Pacific Internet Security Conference were warned Wednesday, May 26, that mobsters were hiring computer programmers to take their brand of criminal activity online. The deputy head of Britain's National Hi-Tech Crime Unit, Superintendent Mick Deats, said one Eastern European syndicate with interests in prostitution, drugs and gun smuggling was also earning money all over the world from internet credit card fraud, software piracy, child pornography and online extortion. "Australia is a focus of a lot of the phishing activity at the moment," Deats said. "The people we've arrested in London were sending money to the same people that are receiving money from attacks that are happening in Australia." Another tactic linked to several eastern European crime syndicates was using distributed denial of service attacks -- bombarding online businesses with a flood of requests aimed at overloading systems and shutting them down. The businesses were then told to pay $50,000 to make the attacks go away, he said.

Category 15.2 *Extortion*

2004-05-31 **extortion fraud Softbank Tokyo database right-wing extremist**

NewsScan

ARRESTS OVER SOFTBANK EXTORTION

Police have arrested two additional people on suspicion of trying to extort money from Softbank after obtaining personal data on as many as 4 million subscribers to the Internet company's broadband service. The two -- Yutaka Tomiyasu, 24, and Takuya Mori, 35 -- are accused of obtaining company passwords to hack into Softbank's database from an Internet cafe in Tokyo in January, according to a Tokyo Metropolitan Police spokesman. The two allegedly passed the information to members of a right-wing extremist group, police said. Four members of the extremist group were arrested in February for allegedly threatening to publicly release the information
unless Softbank paid them ¥1 billion to ¥2 billion ($US13 million to $US26 million). (The Australian 31 May 2004) rec'd from John Lamp, Deakin U.

Category 15.2 *Extortion*

2005-01-18 **scam fraud extortion anonymity Web**

RISKS 23 69

PAY FOR… WHAT?

In an obvious extortion scam, "unsafedriver.com" allows anonymous posters to file unsubstantiated, untraceable complaints about vehicles being driven unsafely -- free! However, to find out whether you have been accused of bad driving, you have to pay $25 for the first vehicle registration and $15 for other vehicles to be able to locate possible libel, prevent the records from being made public, or attach protests to accusations. As RISKS correspondent Dawn Cohen wrote, "This smells like a scam to me, but I'm surprised that it would be perpetuated by a source as reputable as USA Today. If it's not a scam, it's an outrage."

Category 15.2 Extortion

2005-10-05 **VNUnet encryption attack hackers data PC key Internet Explorer malware Trojan**

DHS IAIP Daily; http://www.vnunet.com/vnunet/news/2143265/web−attack−extorts −encryption

WEB ATTACK EXTORTS BY ENCRYPTION

Security experts today warned of a newly discovered attack in which hackers encrypt data on a compromised PC and demand payment for the decryption key. These attacks are happening when a user with a improperly patched version of Internet Explorer visits a webpage containing malware that downloads a Trojan.

Category 15.2 Extortion

2006-01-18 **hacker Website blackmail fraud The Dark Group extortion**

DHS IAIP Daily; http://news.ft.com/cms/s/cd05a42c−87c6−11da−8762−0000779e234 0.html 23

HACKERS BLACKMAIL WEBSITE

The FBI is investigating the hijacking of a Website that hosts micro-advertisements by hackers who demanded a ransom to restore the site. Alex Tew of Britain was sent a demand for US$50,000 by e-mail by a hacker, believed to be Russian. When he refused, the Website crashed. Tew first received a threat on January 7 from a body calling itself The Dark Group, demanding $5,000. He thought the blackmail was a hoax and took little notice. However, on Wednesday, January 18, when Tew reached his goal of earning $1 million, the hackers intensified their attack and hijacked the Website.

Category 15.2 Extortion

2006-03-13 **Cryzip Trojan zip file ransom demand ransomware social engineering tricks**

DHS IAIP Daily; http://www.eweek.com/article2/0%2C1895%2C1937408%2C00.asp 23

CRYZIP TROJAN ENCRYPTS FILES, DEMANDS RANSOM.

Virus hunters have discovered a new Trojan that encrypts files on an infected computer and then demands $300 in ransom for a decryption password. The Trojan, identified as Cryzip, uses a commercial zip library to store the victim's documents inside a password-protected zip file and leaves step-by-step instructions on how to pay the ransom to retrieve the files. It is not yet clear how the Trojan is being distributed, but security researchers say it was part of a small e-mail spam run that successfully evaded anti-virus scanners by staying below the radar. While this type of attack, known as "ransomware," is not entirely new, it points to an increasing level of sophistication among online thieves who use social engineering tactics to trick victims into installing malware, said Shane Coursen, senior technical consultant at Moscow-based anti-virus vendor Kaspersky Lab.

Category 15.2 Extortion

2006-05-26 **criminal hackers extortion privacy social networking**

Newsday < http://www.newsday.com/news/local/longisland/ny-lihack264757084may26,0,7790806.story >

MYFRIENDSPY WRITERS CHARGED WITH EXTORTION

Shaun Harrison and Saverio Mondelli were arrested and charged with attempting to extort $150,000 from MySpace.com by writing a program (MyFriendSpy) to allow "MySpace.com users to see the online identities of anyone who looked at their profiles, undermining the Web site's privacy guarantees," according to "Jeffrey McGrath, an assistant Los Angeles district attorney." Joseph Mallia, writing in Newsday, explained in his report that "Harrison, 18, of Ronkonkoma, and Mondelli, 19, of Oakdale, were arrested in Los Angeles Friday when they stumbled into a cross-country Secret Service sting operation, authorities said. They traveled to Los Angeles in the expectation that they would collect the money from MySpace.com employees, McGrath said."

15.3 Slamming

Category 15.3 *Slamming*

2000-06-07 **slamming fraud unauthorized phone service contract impersonation**

NewsScan, Washington Post http://www.washingtonpost.com/wp-dyn/articles/A10351-2000Jun6.htm

Long-distance company WorldCom Inc. . . . [agreed to pay] $3.5 million to settle an inquiry by the Federal Communications Commission into 2,900 complaints from persons charging that WorldCom telemarketers switched them away from other phone service carriers using a deceptive practice known as "slamming." WorldCom president Bernard J. Ebbers . . . [said] the slamming incidents "were perpetrated by a few sales employees who have since been terminated." (Washington Post 7 Jun 2000)

Category 15.3 *Slamming*

2003-09-29 **Internet redirect explorer bug long distance telephone dial up patch porn**

NewsScan

VANDALS DIVERTING COMPUTERS TO $5-A-MINUTE PORN SITES
Network vandals have been exploiting a security gap in Microsoft's Internet Explorer software and using it to connect their computers to $5-a-minute porn lines by sending computer users to sites that change a computer's dial-up settings, connecting it to expensive long distance telephone numbers instead of the user's ISP. The original hole in Internet Explorer was discovered last month, and Microsoft issued a software patch to fix it, there but new variations of the malicious code seem to be evading the existing patch. (Internet News 29 Sep 2003)

---

16 INFOWAR, industrial espionage, hacktivism

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-01-15 **e-mail spam vandalism racism obscenity ISP**

AP

Someone sent a "racist joke and obscenity-laced poem" to about 140,000 users of the Erol's Internet access service in Springfield, VA. Technicians labored diligently to find the criminal hacker who vandalized the system and to remove the text from the entire network.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-01-21 **infowar sabotage information warfare**

AP

Call Management, a hotel reservations firm, has an 800 number almost identical to that of Holiday Inns, 1-800-HOLIDAY. One of Call Management's numbers is 1-800-H0LIDAY, with the letter O replaced by the numeral zero. Holiday Inns won a federal court action claiming that Call Management's number was a trademark infringement; however, on appeal, the decision was reversed because Call Management did not use the number in promotions. Finally, the Supreme Court of the United States refused to hear this case of electronic mimicry.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-01-22 **infowar e-threats information warfare**

UPI, Reuters

Youngsters in grade 10 at Profile High School in Bethlehem, NH sent death threats to the White House Web site from their school computers. The messages were traced within minutes by the Secret Service and the children were suspended from school and lost their Internet privileges for the next two years.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-01-22 **infowar sabotage information warfare**

Reuters

A Belgian lunatic has terrified travelers by broadcasting false and dangerous instructions to aircraft by using a mobile radio transmitter. The impostor seems to know so much about specialized technical vocabulary that police think he may be or have been an air-traffic controller. Authorities assure the traveling public that the rogue is more a nuisance than a threat; all instructions must be repeated to the real controller, and so far the impostor's fraudulent commands have been caught and repudiated by the real controllers.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-01-28 **infowar corporate espionage information warfare**

EDUPAGE, UPI

Informix sued Oracle after 11 software engineers defected to their competitor. However, in June, Informix dropped the suit, saying that the company "has learned that Oracle and the engineers have not misappropriated or disclosed any confidential Informix information and that Informix trade secrets are adequately protected. Informix regrets any statements or allegations that the engineers misappropriated any trade secrets or disclosed them to Oracle."

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-01-31 **infowar libel information warfare**

AP

Walter Cronkite, whom polls revealed to be the most respected man in the United States in the 1980s, was appalled to discover a page of lies about him on the Web. A 28-year-old programmer, Tim Hughes, invented and posted a scurrilous story about Cronkite's becoming enraged at the author, shrieking imprecations at the couple, boasting about his own infidelity, and spitting in their spice cake at a Florida restaurant. In addition, the anti-Cronkite Web page included falsified photographs purporting to show Cronkite at a KKK meeting. Cronkite threatened to sue for libel; Hughes took the page down and weakly protested that it was all a joke.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-02-03 **Authenticity information warfare**

RISKS 18 81

Opponents of negotiation with Colombian terrorists sent fraudulent e-mail to the kidnappers after the Colombian government announced it would negotiate via e-mail.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-02-11 **infowar crypto export policy information warfare**

AP

The increasing dependence on ubiquitous computing puts the United States at risk, computer security experts testified at a meeting of the House Science Subcommittee on Technology. Dan Farmer warned, "It seems that we only react to disasters. This is really serious stuff we're talking about here." The experts strongly urged relaxing restrictions on exports of strong encryption technology.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-02-14 **pornography infowar information warfare**

PA News

A British consultancy has won a contract from the European Parliament to study all possible ways of interfering with the use of the Internet for dissemination of pornography, pedophilia, and slavery. Smith System Engineering of Surrey will work with legal, social policy and technology experts to report on the possibilities.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-03-04 **industrial espionage hacking**

RISKS 18 85

On 97.02.28, the _Dallas Morning News_ posted news on its Web site before publishing it in its paper edition the next morning. The news report claimed that Timothy McVeigh's admitted to his lawyer, Stephen Jones, that he had in fact bombed the Oklahoma City Federal Building. Jones accused the _News_ of stealing the information through a computer hack.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-03-09 **phone phreak industrial sabotage information warfare infowar**

EDUPAGE

A Swedish man was fined for harassing 911 operators in Florida. He randomly interfered with their work by stunts such as interconnecting two operators or disrupting phone calls.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-03-17 **infowar identity theft information warfare**

RISKS 18 91

RISKS published a summary of theft-of-identity cases and gave the URL of "What Can Consumers Do To Avoid Becoming Theft-of-Identity Victims?". See <http://www.pirg.org/calpirg/consumer/privacy/toi/prevent.htm>.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-03-24 **disaster recovery information warfare infowar**

RISKS 18 93

The Canadian _Globe and Mail_ newspaper (97.03.22, p. A17) reported that computerization hit choppy waters on a recent cruise:

> Splendour on the seas:
> As we learned one evening, computer problems aren't the sole domain of land lubbers. Nowadays, everything is run by the darned things — even cruise ships.
>
> By Helga Loverseed

Seems this new cruise ship is so completely computer-controlled that it can barely function at all when the computer systems fail. Provides a stunning example of what could happen under information warfare conditions and also a warning of problems that could occur with the Millennium Bug.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-04-02 **industrial espionage**

RISKS 19 2

An unnamed correspondent reported that one of his acquaintances is angry at UPS for putting a package-tracking system on-line without adequate security. He is convinced that the decline in his mail-order business is in part due to competitive intelligence: his competitors are finding out where he ships his products by cracking the checksum system that supposedly maintains confidentiality. The businessman has now attacked the UPS system by "laboriously retrieving their shipping destinations."

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-04-06 **RFI information warfare radio**

Reuters

A mysterious Venetian separatist interrupted TV broadcasts in Italy five times in three weeks. At one point, he broke into "Gone with the Wind" and launched a seven-minute declaration of independence for Venice.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-04-15 **industrial espionage information warfare**

EDUPAGE

The president and several employees of Avant! Corp. were charged in an industrial espionage case; they are alleged to have stolen computer source code from Cadence Design Systems to use in their own line of products.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-04-24 **corporate espionage intellectual property theft employees**

EDUPAGE

Symantec launched a lawsuit against McAfee Associates Inc. claiming that McAfee's PC Medic program is a direct rip-off of Symantec's CrashGuard program.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-04-28 **intellectual property theft espionage infowar**

San Jose Mercury News

Scott Thurm and David Wilson summarized recent cases of conflict over intellectual property in Silicon Valley. Stealing information has become much easier because of the thoroughgoing computerization of high-tech information. Firms are responding by beefing up all levels of security and "spiking" their source code with non-functional parts that categorically identify their code if it does get stolen and used by competitors. According to a 1995 survey by the American Society for Industrial Security (ASIS), "companies are most often victimized by people who had legitimate access to their secrets — employees, suppliers, customers, contractors and business partners. Outsiders — hackers, competitors or foreign intelligence agents — accounted for only one-fourth of the losses. . . ." Losses are variously estimated nationwide as ranging from about $25B (ASIS) to $100B (FBI).

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-05-06 **industrial espionage intellectual property employees theft**

EDUPAGE

Novell Inc. sued three of its ex-employees who formed Wolf Mountain Group for alleged theft of ideas on how to make Windows NT computers work in parallel as clusters of processors. Wolf Mountain agreed to change the name of their business, which happens to be the project code name for the clustering technology they worked on at Novell.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-05-07 **industrial espionage sabotage**

Reuters

Borland International sues Microsoft for raiding its employee and strongly implies that the shift of employer constitutes industrial espionage and sabotage. Borland accuses MS of hiring 34 Borland employees over the last 30 months by enticing them to leave with huge signing bonuses and other incentives. MS dismisses the accusations, saying that it's a free market and that nobody is forced to work for them.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-05-20 **information warfare**

EDUPAGE

Winn Schwartau, the Paul Revere of Cyberspace, speaking at a conference in Ottawa, cyberspace is increasingly a battlefield for e-spies. "Schwartau estimated the U.S. economy loses more than $100-billion annually through economic espionage, growing by 500% since 1992."

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-06-03 **information warfare**

Defense Daily 195 45

Defense Secretary William Cohen contributed to the Quadrennial Defense Review. He emphasized the U.S. DoD's commitment to defensive and offensive information warfare. "Although our current capabilities are adequate to defend against existing information operations threats, the increasing availability and decreasing costs of sophisticated technology to potential adversaries demand a robust commitment to improve our ability to operate in the face of information threats as we approach the 21st century." The report also emphasizes the importance of unprecedented cooperation between DoD, other government agencies, the business sector and the public and mentions DoD support for the President's Commission on Critical Infrastructure Protection.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-06-10 **information warfare Web hack**

http://www.iwar.org

The U.S. Dept. of Agriculture lost control of its Web site to hackers who used it to spam the Net. As a result, the site was shut down for a week, preventing release of the monthly USDA World Supply and Demand Forecast. Information warfare experts wondered if this incident were designed specifically to delay release of the information, which affects the futures market.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-06-17 **industrial espionage info warfare intellectual property**

AP, UPI

Two Taiwanese citizens were arrested after trying to bribe a Bristol-Myers Squibb Co. scientist into turning over technological secrets for the manufacture of Taxol, a drug to fight ovarian cancer. The employee reported the approaches to his employers, and with the help of the FBI the two industrial spies were arrested. Hsu Kai-Lo, said to be the leader of the plan, faced 35 years in jail; his accomplice Chester Ho faced 10 years in jail. Hsu and Ho were charged in July; their putative accomplice, Jessica Chou, was still a fugitive at that time. In April 1999, Hsu Kai-Lo pleaded guilty to one count of conspiracy to acquire a trade secret.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-06-18 **information warfare infrastructure**

Reuters

In June, Robert Marsh, head of the President's Commission on Critical Infrastructure Protection, told reporters that the United States lacks the tools to fight a possible computer assault on critical infrastructure such as telecommunications, banking and power grids and that it is only a matter of time before such attacks take place.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-06-24 **hacker database information warfare**

OTC

WarRoom Research LLC of Baltimore, MD announced The Manhattan Cyberproject, an industry-wide effort to share information about hacker activities and technologies. It planned to create a massive database supported by major companies such as IBM and Bell Atlantic and be open for business in 1998. Contact Mark Gembicki, the Project Coordinator <mcpdir@warroomresearch.com>

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-06-25 **information warfare**

Jane's Information Group 27 25

Jane's Information Group reported that Northrop Grumman's Electronic Sensors and Systems Division and Electronic and Systems Integration Division would jointly be conducting a 13-month study on recovery from information warfare attacks on behalf of the US Air Force.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-07-17 **economic espionage infowar book**

Wired

John Fialka of the Wall Street Journal published a fascinating analysis of economic espionage: _War by Other Means: Economic Espionage in America_. By John J. Fialka: US$25. W. W. Norton & Company: +1 (212) 354 5500, or on the Web. Although some commentators such as Jeff Man of Wired criticized what they described as xenophoic "Hogwash", the book includes eye-opening details of the theft of US industrial secrets by agents of foreign powers.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-07-22 **DISA information warfare**

EDUPAGE

Bob Ayers, head of the Information Warfare Division at the U.S. Defense Information System Agency, urged infosec specialists to stop thinking in terms of prevention of attack but rather to focus on delaying damage.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-08-18 **infowar espionage israel**

IWAR mailing list

Israel was again named among 23 countires engaging in industrial, economic and trade espionage in the US according to a joing CIA-FBI report published in August. Israeli officials protested that the report confused legal, open-source intelligence with espionage.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-08-28 **industrial espionage**

Reuters, AP

Harold Worden retired from Eastman Kodak in Rochester, NY after 30 years of service. He then founded a consulting firm that hired up to 60 other Kodak retirees and proceeded to try to sell information gleaned from thousands of stolen confidential documents about Kodak's top-secret acetate-manufacturing machine. The trade secrets were offered to competitors of Kodak; however, both Agfa and Konica informed Kodak and the FBI of the attempts. The FBI then set up a sting operation in which agents pretended to be Chinese nationals intent on stealing the secrets for a mythical factory in China. In August 1997, he pleaded guilty to to one count of interstate transportation of stolen property and went to jail for 15 months as well as having to pay a $30,000 fine. Kodak has also sued him in civil court for damages.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-09-04 **industrial espionage pharmaceutical infowar**

UPI

In 1994, Subu Kota and Vemui Bhaskar Reddy, both from the Boston area, were arrested for industrial espionage when they sold biotechnology secrets to a Russian-speaking undercover FBI agent. In September, the two went on trial for conspiring to sell methods for creating erythropoetin (EPO) which stimulates red-blood cell production and is worth about $2B a year in worldwide sales.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-10-01 **QA information warfare sabotage**

RISKS 19 40

According to correspondent Bryan O'Sullivan, writing in RISKS, Internet Explorer 4.0 includes several features that used to be packaged in the Windows Plus! CD add-in for Windows 95. The anti-aliasing feature works well to make large fonts look smoother on screen — except in Netscape Navigator, where the old blocky effects still reign. If this claim is confirmed, it sounds like level-two information warfare in Winn Schwartau's terminology.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-10-21 **infowar critical infrastructure**

EDUPAGE

Preliminary reports from the President's Commission on Critical Infrastructure Protection urged the administration to increase spending on R&D to defend against attacks on the nation's information infrastructure. This is one of the first official reports to recognize the vulnerability of civilian computer, communications and control systems to deliberate electronic sabotage by hostile forces. In October the final report came out and warned that the United States communications infrastructure is increasingly vulnerable to terrorist attacks.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-10-28 **industrial espionage**

EDUPAGE, TechInvestor (CMP)

In another industrial espionage case, Digital Equipment Corp. accused Intel of stealing chip designs and using them in the Pentium design. A few weeks later, predictably, Intel counter-sued DEC, demanding it return confidential information about Intel designs. In June, DEC filed a legal motion demanding that a former DEC employee now working for the enemy keep his mouth shut about Intel proprietary information. In addition, DEC asked for legal orders to force Intel to preserve all documents relevant to the case, including e-mail and accused Intel of monopolistic practices. The suit was settled out of court in October.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1997-12-01 **industrial espionage information warfare**

Security Management 41 12

Richard Withers and Steve Albrecht provided an excellent review of a case of industrial espionage, where Daniel Worthing, a maintenance worker, offered proprietary information from PPG to its competitor Owens-Corning Fiberglass in 1996. Owens-Corning officials immediately told PPG about the offer and the FBI set up a sting operation which eventually resulted in the arrest and conviction of the spy. The article provides a thorough review of counter-surveillance measures and describes how to set up an espionage-response plan if spying is discovered.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1998-01-03 **information warfare sabotage US Navy military banking**

DAILY TELEGRAPH

Representatives from major Wall Street investment firms participated in war games organized by the U. S. Naval War College in December 1997. Growing out of the report of the President's Commission on Critical Infrastructure Protection, the meeting focused on how the corporate sector could work effectively with government to improve national security in cyberspace.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1998-02-10 **information warfare espionage**

EDUPAGE, Washington Post

A story broke in January about a year-long investigation of claims that Reuters Analytics staff broke into the computers of a major competitor, Bloomberg LP. Investigators were reported to be analyzing source code at the two companies to see if Reuters stole any from Bloomberg.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1998-02-17 **industrial espionage data leakage lawsuit**

EDUPAGE

Pixar, makers of the recent animated movie, "Toy Story," filed suit for a restraining order barring persons unknown from spreading stolen information about the salaries of their 400 employees. The report was widely circulated on the Net and damaged the company's ability to hire and retain employees (because competitors could outbid Pixar easily and inexpensively).

Category 16 *INFOWAR, industrial espionage, hacktivism*

1998-03-01 **information warfare government sabotage hackers**

EDUPAGE

In March, Attorney General Janet Reno announced the formation of the National Infrastructure Protection Center (NIPC) to fight cybercrime and sabotage of the US technological infrastructure.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1998-03-19 **airport disruption interference vandalism prosecution phreak**

EDUPAGE

EDUPAGE reported: "A Massachusetts teenage computer vandal found guilty of disrupting phone service to about 600 homes and a small airport's control tower now faces two years of probation, forfeiture of his computer, 250 hours of community service, and $5,000 in restitution. The government hopes that bringing charges against the young man will send a clear warning to others…."

Category 16 *INFOWAR, industrial espionage, hacktivism*

1998-04-07 **information warfare cyberattacks threat national security**

EDUPAGE

Former Senator Sam Nunn, speaking at an information warfare conference at Georgia Tech, warned that the US was vulnerable to cyberattack. He used Winn Schwartau's notorious expression, "electronic Pearl Harbor," despite objections from the politically correct. At the same meeting, the CIA director, George Tenet, argued forcefully in favor of strong cryptanalysis tools.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1998-04-19 **penetration information warfare Pentagon**

Defense Electronics & Electronics Report, EDUPAGE

In mid-April, DoD announced that the results of their own cyberattack exercise, named "Eligible Receiver" were sufficiently alarming to warrant serious improvements in its computer security posture. According to a Washington Times report cited by EDUPAGE editors, "cyber attacks were able to access the military's command and control structure in the Pacific (and could have shut it down); the attacks also could have turned off the entire electrical power grid in the U.S."

Category 16 *INFOWAR, industrial espionage, hacktivism*

1998-07-12 **information warfare CIA espionage sabotage**

EDUPAGE

George Tenet of the CIA and Lt. Gen. Kenneth Minihan of the NSA both warned the Senate Government Affairs Committee that other nations are developing serious information warfare capabilities that could damage national security by attacks on the civilian infrastructure and on battlefield computers.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1998-07-12 **intellectual property programs industrial espionage lawsuit**

EDUPAGE

In a case that began in 1997, Cadence Design Systems accused Avant of stealing code from Cadence's Framework II software for design automation. The case finally made into the court in mid-July and accusations flowed both ways, with Avant claiming that Cadence's lawsuit was a ploy for damaging Avant's sales.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1998-07-26 **information warfare sabotage software QA quality assurance**

EDUPAGE, RISKS

RealNetworks president Rob Glaser, speaking at a hearing of the Senate Judiciary Committee, accused Microsoft of deliberately engineering their Media Player to attack and disable RealNetworks streaming audio/video software. Such an accusation is extremely difficult to prove in an environment where companies routinely release their newest software versions expecting to find additional bugs. However, in October, Wade Ripkowski reported through a message forwarded to RISKS 20.03 that Microsoft Media Player really does attack all other competitive programs. In Nov, several companies testified at the Microsoft anti-trust trial that their software had been disabled — in their opinion, deliberately — by Microsoft products. Microsoft spokespersons pooh-poohed the notion, calling the accusations "overblown rhetoric."

Category 16 *INFOWAR, industrial espionage, hacktivism*

1998-08-18 **information warfare sabotage marketing service**

EDUPAGE

Intel's marketing campaign for its Pentium II processor raised a stink in Webmasters' quarters when it became clear that Intel was offering 75% of advertising costs if advertisers made their pages complicated and graphics-heavy so as to slow down older processors — and sport a "Better with Pentium II" logo. The normal subsidy, for displaying the "Intel Inside" logo, was only 50% of the costs.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1998-09-22 **hactivism criminal hacker hactivism vandalism Web information warfare**

Wired http://www.wired.com/news/print_version/politics/story/15129.html

Niall McKay summarized a trend towards "hacktivism" among some criminal hackers worldwide in an article for Wired in September. He wrote that victims of political cyber-activism included the Web sites of a right wing party in Sweden, the Mexican government, and many others. The Boston-based criminal hacker organization "Cult of the Dead Cow" announced the formation of a new site <http://www.hacktivism.org> supporting political action through Web vandalism. The site also included links to news items about fighting censorship and repression and to the Global Internet Liberty Campaign <http://www.gilc.org/about/principles.html>.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1998-10-11 **industrial espionage information warfare spying lawsuit**

AP

Johnston Industries of Columbus, GA filed suit in Alabama against Milliken Industries of Spartansburg, SC claiming damages of $30M resulting from industrial espionage in 1995. The suit alleges that Justin Waldrep misrepresented himself as a graduate student at Georgia State University and that Rodney A. Taylor lied about being an investment banker. The two men were given royal treatment at JI plants and given confidential information about secret industrial processes. According to the statement of the tort, the two were actually employed on contract by Millken, which allegedly benfitted from the information to make competitive products. An AP news-wire story stated "NRB Industries of New York filed a suit against Milliken last year. The suit, which reads more like a novel of intrigue than a legal paper, accused Milliken of using the same two men to conduct corporate spying. But in this case, Waldrep was supposed to be a graduate student at Columbia University since NRB is in New York. Court records included an investigation contract signed by a Milliken division chief and an agreement stating, ``Milliken's identity will remain absolutely anonymous." Milliken settled that suit in January without disclosing the terms."

Category 16 *INFOWAR, industrial espionage, hacktivism*

1998-10-12 **information warfare government infrastructure vulnerability**

Congressional Record http://www.access.gpo.gov/su_docs/aces/aaces002.html

Sen. Kerrey addressed the Senate in October with a stirring call to action on information warfare preparedness.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1998-10-13 **penetration information warfare attack defense hostile**

RISKS 20 3

In a incident worthy of a Monty Python skit, criminal hackers calling themselves the "Electronic Disruption Theater" complained that the DoD had used offensive information warfare techniques (allegedly a hostile Java applet) in responding to the group's attack on DefenseLink on 9 Sep.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1998-10-18 **information warfare espionage intellectual property employee**

EDUPAGE

Walmart sued Amazon over alleged theft of proprietary information. Allegedly Amazon hired former employees and vendors who revealed the intricacies of Walmart's sophisticated customer-tracking system and purchase-prediction system.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1998-10-22 **information warfare propaganda Web vandalsim penetration**

DER STANDARD, Austria (German-language)

Hackers broke into the Indian army's Kashmir website (http://www.armyinkashmir.com) and put up propaganda supporting "all the brothers in Kashmir who suffer from the brutal suppression of the Indian army." There were serious questions about whether the hackers were independents or suported by the Pakistani secret service.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1998-10-23 **information warfare vandalism Web hacktivism**

BBC http://news.bbc.co.uk/hi/english/sci/tech/newsid_200000/200069.stm

In October, Serbian hackers attacked a Web site run by Kosovo Albanians; they also threatened to destroy NATO's official Web site. The "Black Hand" hacking group threatened the Serbian government itself in protest over President Slobodan Milosevic took action to curb the country's independent media. Historically, the Black Hand Serbian secret society was originally founded at Belgrade in May 1911 as an irridentist organization working to reunite Serbs living within the Austrian and Ottoman Empires and those in Serbia.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1998-10-27 **information warfare China censorship vandalism Web**

Wired http://www.wired.com/news/print_version/politics/story/15857.html

A criminal hacker defaced the Web site managed by Tianjin City Network of Information of Science & Technology site and which explains the areas of the WWW acceptable to the government of China. The hacker, a computer science post-graduate student in California, described his attack as "a protest against the treatment of Lin Hai, a man arrested for simply sending email to the US who now faces life in prison." The criminal hackers added links from the Chinese site to Amnesty International as well as a site called Human Rights in China. "The Chinese Communist government is ... a gang of 100-plus year old thugs and bullies who hide in seclusion," wrote Bronc Buster. "This pitiful effort of trying to change the hearts and minds of the world is a joke! "How can the United States trade millions and millions of dollars with them and give them most favored trade status when they know what is happening? Two wrongs do not lead to a right, no matter what twisted world you live in. Get informed!" the site read.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1998-11-01 **criminal hackers political activists vandalism hacktivism**

EDUPAGE

The NY Times reported that the Electronic Disturbance Theater urged political activists to engage in "electronic civil disobedience" by Web vandalism and denial of service ("virtual sit-ins") directed against "oppressors."

Category 16 *INFOWAR, industrial espionage, hacktivism*

1998-11-11 **hate e-mail racism harassment intimidation incitement**

UPI

In Oct, hateful, racist messages including crude obscene drawings and support for the KKK were posted on the Miami University (Ohio) e-mail system and screensavers at the Black Student Center were changed to include racist messages. Police investigations were continuing in mid-Nov.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1998-11-16 **criminal hacker hacktivism Web vandalism information warfare**

Forbes http://www.forbes.com/tool/html/98/nov/1116/featb.htm

In Forbes magazine for November 16, Aladm Penenberg wrote an extensive analysis of the events surrounding the breach of security in mid-May 1998 at the Bhabha nuclear research center in Bombay, India. The author interviewed the criminal hackers involved and presented a penetrating glimpse into the minds and values of the young people involved.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1998-12-01 **information warfare censorship vandalism firewall Web attack**

Wired
http://www.wired.com/news/print_version/email/member/politics/story/16545.h
tml

Criminal hackers attacked Chinese firewalls and censorware in late 1998, disabling the totalitarian government's ability to interfere with their Internet users' access to dangerous sites such as sites for the BBC, ABC, MSNBC, ZDNET, News.com, and Wired News. In addition, the restrictions had stopped acces to all the search engines and to subversive, family-oriented sites such as Parents.COM, Family.com, and Seniors.Com. The Cult of the Dead Cow also announced a special Chinese-oriented e-mail plug-in to allow e-mail access to Web sites, making it more difficult for the authorities to catch illicit Web browsing.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1998-12-15 **information warfare crime police law enforcement conference**

AP

In December, law-enforcement agents from Britain, Canada, France, Germany, Italy, Japan, the United States and Russia held a a video-link conference to discuss coordination in the fight against international crime. The linkup took place over secured (encrypted) telephone lines and was hosted by the British Home Secretary, Jack Straw. Topics included improved investigation and prosecution of international crime; extradition of suspects; jurisdictional and forensic aspects of international cyber-crime; money laundering; smuggling of illegal immigrants; corruption and blocking funds for terrorists.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1998-12-15 **information warfare vulnerability infrastructure catastrophe**

Federal Computer Week http://www.fcw.com/pubs/fcw/1998/1214/web-report-
12-15-98.html

The Center for Strategic and International Studies caused waves by criticizing the Administration for inadequate attention to information warfare directed at the U.S. infrastructure. A three-year assessment attacked the President's Commission on Critical Infrastructure Protection, saying, "The president's commission has identified only the tip of a very large iceberg. The battleground of the future will encompass the very foundations of America's knowledge-based, high-tech economy. There are now info-guerillas intent on doing major damage to the citadel of capitalism, and cybergeniuses in their late teens and early 20s are the new front-line fighters, arguably more important to the nation's defense than the men and women who fought the country's wars in the past." Perhaps in response to the growing pressure for information warfare preparedness, President Clinton included the issue briefly in his January State of the Union address.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1998-12-27 **information warfare cyberterrorism national security**

Deseret News http://deseretnews.com:80/dn/view/0,1249,30003297,00.html?

Jack Anderson and Jan Moller discovered cyberwar in December 1998 and wrote a stirring call to, um, to worry. They cited the report ("Cybercrime . . . Cyberterrorism . . . Cyberwarfare: Averting an Electronic Waterloo") from the Center for Strategic and International Studies which laid out the standard picture of infrastructure vulnerability.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1999-01-04 **information warfare strategy national security**

Federal Computer Week http://www.fcw.com/pubs/fcw/1999/0104/web-rand-01-04-98.html

The RAND Corporation issued a DoD-commissioned report, "Strategic Information Warfare Rising" in mid-1998 that fueled the growing debate within the Pentagon about the wisdom of pursuing offensive information warfare capabilities. Opponents argue that widening the sphere of warfare to include cyberattacks on critical infrastructure would only increase likelihood of successful attacks on the US. The report laid out four basic scenarios for future developments in IW; as laid out by Daniel Verton, writing in Federal Computer Week, they were the following [bullets added]:
"* U.S. supremacy in offense and defensive strategic IW.
* A club of strategic IW elites, whereby a policy of no first use of strategic IW capabilities could be established.
* Global "defensive dominance" in strategic IW, whereby a regime would be established to control the spread of strategic IW similar to biological and chemical weapons.
* Market-based diversity, whereby the damage or disruption achievable through a strategic IW attack is modest and recovery is fast."

Category 16 *INFOWAR, industrial espionage, hacktivism*

1999-01-04 **criminal hackers industrial espionage software piracy theft**

Reuters

Unemployed Russian computer programmers pose a serious threat to world computing, according to Elizabeth Piper, writing for Reuters. With 89% of all the programs in Russia being pirated, the habits are well inculcated already; however, the growing economic crisis is throwing programmers into desperation. Many are turning to hacking, including industrial espionage, to make a living.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1999-01-08 **network defense information warfare INFOWAR criminal hackers spies DoD**

UPI, OTC

The Joint Task Force - Computer Network Defense (JTC-CND) was announced on 1999-12-08 and officially launched on the 1999-01-01. The JTC-CND immediately generated controversy among politicians and industry security experts who argued that the agency should concentrate on proactive identification of vulnerabilities and measures to plug the security holes. In contrast, spokespeople for the Task Force seemed to emphasize a more reactive approach, where they would respond to cyberattack in real time. Melissa Bohan, speaking for the office of USAF Maj. Gen. John Campbell, the new head of the task force, said that detecting intrusions was a primary function; "Who may have made that intrusion is often a secondary question. In fact, 'who' it is may not even be important." By August 1999, the JTF-CND was fully operational and monitoring Pentagon networks for intrusions round the clock.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1999-01-29 **government support education infrastructure scholarships**

Science

The Clinton administration proposed a 40% increase in critical infrastructure protection and computer security — a proposed budget item of $1.464B. Some $3M of this amount was earmarked for new scholarships in computer science and security programs.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1999-02-12 **sabotage information warfare knowbot feedback fraud error**

RISKS 20 21

For unknown reasons, the BUY.COM online store Web site listed a $588 Hitachi monitor at only $164.50 — and staff failed to notice the error until two days later, by which time there were 1,600 orders for this incredible bargain. The potential cost was estimated by the company at $320,000. BUY.COM filled 200 orders and told all the rest that they were out of luck. They also posted new language on their Web site addressing the non-validity of erroneous prices.

Analysts speculated on the cause of the error. One intriguing possibility: the BUY.COM online store had a policy of underbidding any price on the Net and may possibly have used knowbots to scour the Web looking for prices of products it was selling. Speculation had it that if a competitor accidentally or deliberately posted a bad price, the unsupervised knowbot could very well poison the BUY.COM Web site database. The same technique could be used in an information warfare attack to ruin a competitor. Even worse, the same problem could occur if two companies inadvertently used the same policy of underbidding all competitors and then simultaneously launched automated processes to lower the price without human intervention.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1999-02-16 **pentagon information warfare data leakage inference Web**

AP

The Pentagon began a thorough re-evaluation of the value of its public Web sites after information warfare experts demonstrated in December 1998 that open-source information could be used to infer sensitive information such as the location of military personnel's family members. Before the purge, tactically valuable data such as aerial reconnaissance photographs showing US military installations were freely available to anyone, including terrorists.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1999-02-18 **information warfare critical infrastructure protection**

COMPUTING (UK)

Colin Barker wrote an interesting essay on the change in the British government's attitude towards information warfare. In February, the UK announced that there would be a one-day conference entitled Protecting the National Information Infrastructure. Barker attributes the change in part to the effect of the Y2K bug on non-technical politicians and bureaucrats. First, the bug brought home just how dependent modern society is on computer and networks; second, it raised doubts about the competence of the I.T. specialists who had been denying that information warfare was a serious issue.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1999-02-25 **information warfare infrastructure vulnerability government**

Computing (UK)

In February, the largest information warfare conference in Britain was organized by the UK government's information security branch, the Communications Electronics Security Group (CESG). The conference was mostly held away from the public and press, but analysts suggested that the key issue was critical infrastructure protection in the face of increasing threats from criminals, ideologues, hobbyists and agents of international antagonists — governmental and terrorist.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1999-02-28 **criminal hacking interception industrial sabotage infowar**

Reuteurs; RISKS

In late February, the Sunday Business newspaper quoted an unnamed source that claimed that criminal hackers had achieved control over a British communications satellite and were making extortion threats. The story was later discredited.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1999-03-01 **information warfare international crime fraud pornography**

Washington Post

Janet Reno, the Attorney General of the U.S., announced the formation of a center for fighting Internet-based computer crime. She also called for international cooperation and laws to fight cybercrime.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1999-03-30 **information warfare Web vandalism hacktivism denial**

BBC, news wires

Serbian hackers began a low-level campaign of harassment directed at US government and military agencies as NATO began bombing Serbia in March 1999. The "Black Hand" hacker group, possibly named after the notorious Sicilian secret society associated with the Mafia, and the "Serbian Angel" hackers threatened to damage NATO computers in retaliation for the war against the Serbs. The White house Web site was defaced by red letters reading "Hackerz wuz Here" on the 29th of March. Speculation was rife that anti-NATO activists were involved. According to a Russian newspaper, "Segodyna," on the 30th of March, unknown hackers damaged a main NATO Web server; the system was down for at least half an hour. The claim was unconfirmed by NATO sources.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1999-04-03 **information warfare Web vandalism hacktivism**

LOS ANGELES TIMES 03/04/1999 P10

The Kosovo conflict generated a flurry of hacking in what the media labeled the "First Internet War," the "First CyberWar" or the "Web War I." Serbs and Albanians and their supporters attacked each others' Web sites — and those of NATO — leaving messages such as "If you're looking for the truth, visit WWW.B92.NET," and the ever-popular and eternally misspelled, "SAMURAI RULLEZ!"

Category 16 *INFOWAR, industrial espionage, hacktivism*

1999-04-04 **information warfare survey estimates virus damage costs**

SUNDAY TIMES

A report in the Sunday Times reviewed the growing scope and cost of information warfare around the world. New e-mail-enabled viruses and new Trojans have the potential for massive damage running into the billions of dollars, according to experts such as CSI's Richard Power. James Adams, of Infrastructure Defence and author of _The Next World War: Computers are the Weapons and the Front Line is Everywhere_, said, "Hackers are a new form of terrorist. You can bring a country to its knees. It is a unique weapon. Things are getting exponentially worse."

Category 16 *INFOWAR, industrial espionage, hacktivism*

1999-04-04 **information warfare vandalism Web Internet**

Sunday Times (London), Defense Daily

The British GCHQ warned in April 1999 that Serbian hackers might see infrastructure systems as prime targets for electronic attack given the perceived difficulty of penetrating government and military computers. The US DoD stated in June 1999 that Serb hackers were definitely probing Pentagon systems but had not succeeded in penetrating any.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1999-04-06 **information warfare Web vandalism hacktivism**

OTC

As the incidence of information warfare attacks grew during the Kosovo conflict, some security firms found their business going up. Internet Security Systems of Atlanta got a contract with the US Army and the Air Force for security improvements to their Web sites.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1999-04-09 **information warfare espionage propaganda Web attack**

BBC MONITORING SERVICE: CENTRAL EUROPE & BALKANS

The government of Serbia claimed that the CIA hijacked their Web site but said in April that everything was OK now.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1999-04-19 **information warfare attacks cyberwar Netwar NATO**

mi2g PR

The mi2g security group based in London, England claimed that pro-Serbian cyberwarriors were sending virus-laden e-mail to various businesses, hospitals, and government agencies throughout NATO countries in a concerted effort to cause disruption during the Kosovo air-war launched against Serbia by NATO.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1999-04-20 **information warfare cyberwar Netwar strategy terrorists**

Wired

An interesting paper by the Rand Corporation entitled _Countering the New Terrorism_ was put on the Web free < http://www.rand.org/publications/MR/MR989/MR989.pdf >. _Countering the New Terrorism_ by I.O. Lesser, B. Hoffman, J. Arquilla, D.F. Ronfeldt, M. Zanini, & B.M. Jenkins was abstracted as follows: "The contours of terrorism are changing, and the new terrorism has more diverse sources, motivations, and tactics than the old. It is more lethal, global in reach, and characterized by network forms of organization. Terrorist sponsorship is becoming hazier and `privatized.' The August 1998 terrorist bombings of U.S. embassies in Kenya and Tanzania fit in many ways the new mold. The chapters in this book trace the evolution of international terrorism against civilian and U.S. military targets, look ahead to where terrorism is going, and assess how it might be contained. Terrorism and counterterrorism are placed in strategic perspective, including how terrorism might be applied as an asymmetric strategy by less-capable adversaries. The report builds on a existing body of RAND research on terrorism and political violence, and makes extensive use of the RAND-St. Andrews Chronology of International Terrorism."

Category 16 *INFOWAR, industrial espionage, hacktivism*

1999-05-09 **hacktivists political protest Web government China USA Belgrade embassy bombing**

ABC
http://www.abcnews.go.com/sections/world/DailyNews/kosovo_chinacyber_990509.html, Reuters

In the wake of the US bombing of the Chinese embassy in Belgrade, hactivists assaulted a number of US Web sites and launched a propaganda offensive on chat boards. Damaged Web sites included those of the US Embassy in China, the Department of Energy, the Department of the Interior, and the Department of Energy.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1999-05-24 **information warfare INFOWAR destablize government secret attack hacking**

Newsweek via Reuters

Newsweek Magazine claimed in May 1999 that the Clinton Administration had agreed to attack the Milosevic regime in Yugoslavia using information warfare techniques such as damaging the dictator's foreign bank accounts and carrying out sabotage within his country to foment dissatisfaction. The anonymous sources claimed that the CIA would be involved, but equally anonymous sources denied this assertion.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1999-06-02 **information warfare criminal hackers vandalism espionage air gap**

Washington Post

In June, the Pentagon installed firewalls between sensitive and less-sensitive components of its networks. Some observers interpreted this move as a response to highly-publicized successful attacks on DoD sites by criminal hackers in the preceding months.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1999-09-30 **information warfare strategy planning theory commercial off-the-shelf software COTS infrastructure defense cyberwar**

Defense Daily 203 64

Marvin Langston, Deputy Assistant Secretary of Defense (C3I) and the Office of the Secretary of Defense's Deputy Chief Information Officer, told a National Defense University group in September that the Pentagon needs to put more effort into defensive and offensive information technology. He also warned that the DoD's dependence on commercial off-the-shelf software (COTS) makes it impossible to achieve information superiority; the DoD, he concluded, must invest in much more research and development for its particular technological needs.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1999-10-01 **information warfare infowar criminal hacker attack penetration vandalism hacktivism law enforcement response**

Defense Information and Electronics Report

James Christy of the Defense-wide Information Assurance Program (DIAP) offered a strongly-worded attack on the notion that the US has ever been the target of information warfare. On the contrary, he argued in a presentation to the International Testing and Evaluation Symposium in Atlanta in late September, the attackers are cybercriminals, not cyberwarriors. The fundamental difficulties in responding effectively to such attacks, said Christy, are as follows:
* the military has expertise in computer crime but cannot help law enforcement agencies without a presidential directive;
* the civilian has not been able sufficiently to develop its familiarity with computer crime countermeasures;
* it is difficult to tell that cyberattacks are being carried out because most victims keep that information secret, not wanting to get involved with law enforcement investigators;
* precise attribution of blame is extremely difficult in cyberspace;
* the public doesn't know much about computer crime and therefore tends to favor privacy over cybercrime prevention and law enforcement;
* jurisdiction over cyberspace crimes is confused by competing geographical claims.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1999-10-04 **information warfare foreign penetration attempts attacks firewalls defenses**

Dow Jones International newswires, Australian AP

Richard Humphrey, Managing Director of the Australian Stock Exchange, claimed in an interview that a foreign military site attacked the Exchange in late 1998. He implied that the site was in the USA, although apparently the "foreign" military officials who were contacted denied any possibility of such an attack from a military site. Humphrey urged changes in Australian laws to make it easier to try hackers; at present the laws require that criminal hackers be apprehended in the act of hacking.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1999-11-11 **information warfare espionage criminal hacking civil lawsuit**

PR Newswire

In the first case of a lawsuit involving industrial espionage by lawyers, Moore Publishing of Wilmington, DE sued Steptoe & Johnson of Washington, DC for allegedly breaking into its computer systems more than 750 times while simultaneously using a stolen user-ID and password to penetrate the victim's network. In addition, the suit alleges a systematic cyberwar involving misinformation posted on newsgroups through a HotMail account that was eventually traced to the defendants. The suit demanded damages of at least $10M.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1999-11-17 **information warfare infrastructure vulnerability national defense**

AAP

Australian Attorney-General Daryl Williams gave a clear warning on November 17th about the necessity for infrastructure protection in the era of cyberwar. Speaking at the Security in Government Conference, he said, "Australia's security is open to compromise in ways that may be less obvious than a terrorist attack but are certainly no less significant." The Attorney-General added, "The costs of a deliberate and concerted attack on our telecommunications, energy, banking and finance or air traffic control systems would be immense in both social and financial terms. The potential sources of deliberate threats are familiar to us all: disgruntled employees or contractors, criminals, issue-motivated groups, terrorists, those engaged in commercial espionage and some foreign states. As if these are not enough, there are also new villains on the scene. The computer hacker and cyber terrorist, sometimes operating alone and equipped only with a personal computer and a modem, can inflict the kind of damage that was previously the realm of organised well-resourced groups." He urged cooperation between the government and the private sector and suggested that a vulnerability and threats database would be useful.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1999-11-17 **information warfare doctrine review survey study analysis**

Jiefangjun Bao (Beijing) translated by BBC

The Chinese military newspaper Jiefangjun Bao published an article in November emphasizing the importance of information warfare in the current military sphere. The authors, Leng Binglin, Wang Ylin and Zhao Wenxiang, made the tendentious claim that "In the Kosovo war, the Yugoslav Federation organized a `hacking' war to attack certain US, British, and NATO web sites, which forced the White House and Pentagon computer systems to cease operations, while the British Meteorological Office was paralysed and unable to provide the necessary meteorological services for NATO air attacks, and a number of NATO air attack plans even had to be cancelled." The concluded, "Experts concerned believe that net attacks have not yet been fully put to good use, because corresponding links have not been established between such attacks and combat actions, since each fights its own war. To ensure that net warfare can play the maximum role in war, it is essential to integrate it with other combat actions. Modern hi-tech warfare cannot win without the net, nor can it be won just on the net. In the future there must be coordinated land, sea, air, space, electronic, and net warfare, and the state's determination will be fully expressed in this mysterious theatre space." [The article was particularly interesting because of the ongoing cyberwar waged by Taiwan and The People's Republic in which there have been thousands of attacks on each others' Web sites.]

Category 16 *INFOWAR, industrial espionage, hacktivism*

1999-11-18 **information warfare simulation games breakdown civil unrest rebellion**

UPI

Organizers from the Institute for Security and Intelligence's Center for Technology and Terrorism, with support from the Jane's company that publishes military magazines and books, brought together US government staff and industry executives in a war-game simulation that resulted in frighteningly believable attack scenarios. Instead of the usual dumb attacks directly eliminating their targets, these cyberwarriors concentrated on causing disruption with false information and denial of service. According to Pamela Hess writing for UPI, "The terrorists, determined to bring down the money-grubbing IRS, devised a diabolical plan with alarming speed. They would hack into the IRS audit system and send out millions of audit notices to American citizens, at the same time sending out "tax due" notices and jamming all the telephone, fax and e-mail lines into and out of the organization to give already irate citizens only busy signals. Just for fun, they tapped into immigration control and State Department systems to issue visas to known terrorists to come to the United States. They created fake documents to make it appear that the organization was investigating the personal lives of members of Congress, then leaked these to the media, along with fake compromising photographs."

Category 16 *INFOWAR, industrial espionage, hacktivism*

1999-11-20 **information warfare study overview**

The Times (London)

Michael Evans, writing in The Times of London on November 20th, reported on the growing awareness of cyberwar as a real threat. Citing a number of military and law-enforcement authorities, he made a strong case for the likelihood of information warfare as a threat to developed nations.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1999-11-23 **Internet e-mail interception confidentiality industrial espionage**

UPI, San Jose Mercury News

In a settlement of one of the few documented cases of industrial espionage involving intercepted e-mail, the Alibris company paid a $250K fine for the firm it acquired in 1998. That company, Interloc, admitted intercepting and copying 4,000 e-mail messages sent to Amazon.com through its own ISP, Valinet. Prosecutors said that the e-mail was intercepted to gain a competitive advantage against Amazon in Interloc's own book business. The managers of Interloc steadfastly denied any wrongful intention but failed to explain why they copied the e-mail.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1999-11-24 **criminal hacker espionage political party bank accounts**

Reuters

The British Conservative Party complained that someone hacked into its bank accounts in an investigation (or smear) campaign around foreign donations. The Times of London denied that any of its journalists had done any such thing.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1999-11-30 **information warfare espionage hacking penetration government policy secret**

AUSTRALIAN; Newsbytes

In 1996, the Attorney General of Australia blocked distribution of a special report on information warfare techniques for the Australian Security Intelligence Organisation (ASIO). A censored version was grudgingly released under the Freedom of Information Act after demands from Electronic Frontiers Australia. However, in January, a student discovered complete copies of the restricted report in several public libraries. The report recommended measures that were later incorporated into legislation that authorized ASIO to use techniques typically associated with criminal hacking such as unauthorized penetration of systems, data modification, installation of Trojans and back doors, and computer surveillance.

Category 16 *INFOWAR, industrial espionage, hacktivism*

1999-11-30 **principles policy infrastructure protection infowar information warfare government industry association**

ITAA press release http://www.itaa.org/infosec

The Information Technology Association of America (ITAA) issued a Statement of Principles on 30 Nov 1999. ITAA's InfoSec Statement of Principles acknowledged the importance of protecting the national information infrastructure and highlighted private industry's primary authority for protecting it. The statement urged the lowest possible government regulation of critical infrastructure protection. The principles included a call for distinctions among cyber-mischief, cybercrime and cyberwar so that appropriate law enforcement agencies could take charge of specific cases with minimal jurisdictional confusion and with assurance of a clear legal basis for prosecution.

Category 16 *INFOWAR, industrial espionage, hacktivism*

2000-02-01 **industrial espionage infowar trial sentence fines**

AP, NACIC Annual Reports to Congress 1999 & 2000

In September 1997, Pin Yen Yang and his daughter Hwei Chen Yang (a.k.a. Sally Yang) were arrested with Dr Ten Hong Lee for trying to steal valuable industrial secrets from the Avery Dennison Corporation, Pasadena, California, for transfer to the Four Pillars Company in Taiwan. Dr. Lee, a Taiwan native and US citizen, had been an Avery Dennison employee since 1986 at the company's Concord, Ohio, facility. Dr. Lee allegedly received between $150,000 and $160,000 from Four Pillars/Pin Yen Yang for his involvement in the illegal transfer of Avery Dennision's proprietary manufacturing information and research data over a period of approximately eight years. Economic losses to Avery Dennison were estimated at $50-60 million. This case marked the first conviction of foreign individuals or a foreign company that went to trial under the Economic Espionage Act of 1996. The Yangs each faced a maximum penalty of 10 years in prison and $250,000 in fines. On 5 January 2000, a Youngstown, Ohio, federal judge sentenced Pen Yen Yang to two years probation along with six months of home detention for violating the 1996 Economic Espionage Act. Mr Yang's daughter was sentenced to one-year probation on the same charge. Four Pillars itself also was fined $5 million by a US District Court for accepting the pilfered secrets. In February 2000, a jury verdict in US District Court, Cleveland awarded Avery Dennison at least $40 million in damages in a civil case against Four Pillars. The judge increased the award to $80 million.

16.1 Industrial espionage

Category 16.1 *Industrial espionage*

1996-11-06 **industrial espionage voice mail ex-employee disgruntled civil suit damages criminal trial sentence**

NACIC Annual Report to Congress, 1998

Standard Duplicating Machines Corporation (Standard) was the victim of unauthorized intrusion by a disgruntled former employee into a voice-mail system. John Hebel was employed by Standard as a field sales manager from 1990 to 1992 when his employment was terminated. Hebel was subsequently hired by the US affiliate of Manufacturing Corporation of Japan (Duplo), the main competitor of Standard. Through an unsolicited phone call from a customer, Standard discovered that while employed at Duple, Hebel accessed Standard's electronic phone messaging system and used the information in Duplo's benefit to compete against Standard. On 6 November 1996, Hebel was charged with one count of violating 18 USC §1343 (Wire Fraud) and on 14 March 1997, Hebel was sentenced to two years probation. In addition, a civil suit was brought against Duplo by Standard with a final settlement closed to $1 million.

Category 16.1 *Industrial espionage*

1997-01-07 **espionage competitive intelligence information warfare**

EDUPAGE

INTERNET IS NO.1 CHOICE FOR FOREIGN SNOOPERS

A report released by the National Counterintelligence Center (NACIC) indicates that the Internet is the fastest growing method used by foreign entities to gather intelligence about U.S. companies. "All requests for information received via the Internet should be viewed with suspicion," says the report, which urges caution in replying to requests coming from foreign countries or foreign governments, particularly with regard to questions about defense-related technology. NACIC works in close coordination with the CIA, but is an autonomous agency reporting the National Security Council. (BNA Daily Report for Executives 6 Jan 97 A15)

Category 16.1 *Industrial espionage*

1997-01-09 **industrial espionage infowar information warfare**

Reuters, AP

The four-year saga of Jose Ignacio Lopez de Arriortua, General Motors' Opel Division and Volkswagen AG ended in January 1997 with an out-of-court, secret settlement. Arriortua had been accused of having stolen confidential information from his previous employer, GM Opel, when he was hired by VW.

Category 16.1 *Industrial espionage*

1998-01-23 **industrial espionage employee contractor trial plea**

NACIC Annual Report 1998

On 23 January 1998, Steven Louis Davis pled guilty to federal charges that he stole and disclosed trade secrets concerning a new shaving system developed by the Gillette Company. Davis was employed by Wright Industries, a subcontractor of Gillette Company, which had been hired to assist in the development of the new shaving system. In February and March 1997, Davis made disclosures of technical drawings to Gillette's competitors Warner-Lambert Co., Bic, and American Safety Razor Co. The disclosures were made by facsimile and electronic mail. Although the FBI is aware that Davis reached out to one foreign-owned company (Bic), it is unclear if he was successful in disseminating trade secrets overseas. Davis was arrested on 3 October 1997 and was indicted on counts of Title 18, U.S.C., Section 1343 (Wire Fraud) and Title 18 U.S.C., Section 1832 (Theft of Trade Secrets). On 17 April 1998, Davis was sentenced to two years and three months in federal prison.

Category 16.1 Industrial espionage

1998-04-14 **industrial espionage sting collusion conspiracy trial plea**

NACIC Annual Report to Congress 1998

John Fulton, a former employee of the Joy Mining Machinery, a global coal mining company that manufactures and repairs technical components for longwall shearers (equipment that mechanically shears coal from the face of an underground coal wall) approached a Joy employee in an attempt to purchase schematics for part of the longwall shearer system. Fulton was operating United Mining Cable, a Joy competitor. The Joy employee became a cooperating witness in the case. The cooperating witness made consensually monitored conversations in which Fulton offered to pay any amount of money for information pertaining to the chock interface unit of the longwall shearer. On 21 November 1997, Fulton paid the cooperating witness $1,500 for blueprints and a technical binder, both of which were Joy proprietary items. Fulton was arrested by the FBI after the exchange and was charged with unlawfully attempting to obtain trade secrets (18 USC §1832). On 14 April 1998, Fulton pled guilty to one count of theft of trade secrets and was sentenced in September 1998.

Category 16.1 Industrial espionage

2000-01-29 **industrial espionage government spies surveillance eavesdropping**

RISKS, Sunday Times (London), http://www.sunday-times.co.uk/news/pages/sti/2000/01/23/stinwenws03006.html?999 20 77

According to James Clark, writing in the Sunday Times of London, French intelligence set up at least eight listening posts focused on communications with British industries. British executives were warned to avoid discussing confidential details over unsecured phone lines, especially mobiles.

Category 16.1 Industrial espionage

2000-06-20 **industrial espionage dumpster diving trashing**

NewsScan, Washington Post http://www.washingtonpost.com/wp-dyn/articles/A22819-2000Jun19.html, New York Times http://partners.nytimes.com/library/tech/00/06/biztech/articles/29tech.html

Microsoft . . . [complained] that various organizations allied to it have been victimized by industrial espionage agents who attempted to steal documents from trash bins. The organizations include the Association for Competitive Technology in Washington, D.C., the Independent Institute in Oakland, California, and Citizens for a Sound Economy, another Wash., D.C.-based entity. Microsoft . . . [said], "We have sort of always known that our competitors have been actively engaged in trying to define us, and sort of attack us. But these revelations are particularly concerning and really show the lengths to which they're willing to go to attack Microsoft." (Washington Post 20 Jun 2000)

ORACLE DEFENDS TRASHING OF MICROSOFT
Saying he was exercising a "civic duty," Oracle chairman and founder Lawrence J. Ellison defended his company of suggestions that Oracle's behavior was "Nixonian" when it hired private detectives to scrutinize organizations that supported Microsoft's side in the antitrust suit brought against it by the government. The investigators went through trash from those organizations in attempts to find information that would show that the organizations were controlled by Microsoft. Ellison, who, like his nemesis Bill Gates at Microsoft, is a billionaire, said, "All we did was to try to take information that was hidden and bring it into the light," and added: "We will ship our garbage to [Microsoft], and they can go through it. We believe in full disclosure." "The only thing more disturbing than Oracle's behavior is their ongoing attempt to justify these actions," Microsoft said in a statement. "Mr. Ellison now appears to acknowledge that he was personally aware of and personally authorized the broad overall strategy of a covert operation against a variety of trade associations." (New York Times 29 Jun 2000)

Category 16.1 Industrial espionage

2000-07-06 **industrial espionage international investigation law enforcement surveillance interception monitoring e-mail eavesdropping**

NewsScan, Newsbytes http://www.newsbytes.com/pubNews/00/151697.html

The European Parliament has renewed its attack on the U.S.-devised Echelon satellite and eavesdropping network by forming a "temporary committee" to investigate whether the spy network was used for commercial espionage against European businesses. The parliament said the committee will also determine Echelon's legality. Echelon, which is jointly operated by the U.S., the U.K., Australia, Canada and New Zealand, is capable of intercepting phone, fax and e-mail signals around the world and is intended to gather intelligence regarding terrorist and other threats to the U.S. and its allies. (Newsbytes 6 Jul 2000)

Category 16.1 *Industrial espionage*

2000-08-06 **information warfare insider industrial espionage lawsuit intellectual property IP**

NewsScan, Washington Post http://www.washingtonpost.com/wp-dyn/articles/A46353-2000Aug6.html

Qwest . . . [sued] AT&T following an AT&T threat to take legal action to prevent an AT&T employee from leaving it to work for Qwest. AT&T . . . [said it was] concerned that the employee — a vice president of policy and law — would make use of AT&T's confidential information or trade secrets, but a Qwest executive . . . [countered]: "I think AT&T may be trying to slow the flow out of the company and show people it's not going to be easy to leave." (AP/Washington Post 6 Aug 2000)

Category 16.1 *Industrial espionage*

2001-04-17 **industrial espionage sabotage revenge credit card fraud disgruntled employee firing**

NewsScan

FIRED WORKER TO BARKSDALE: NO MORE BALOGNA

In the process of cleaning out her desk after being fired by the Barksdale Group, the high-tech investment company named after Netscape founder Jim Barksdale, a 30-year-old administrative assistant allegedly stole secrets worth $1.5 million and used a company credit card to purchase $100,000 worth of jewelry -- plus two TV sets, some leather chairs and sofas, a microwave, a cruise, cookware, several watches, three cameras, purses and a rug. A police sergeant commented: "She clearly had problems. Maybe it was being in that environment, working with all those very wealthy people, around all that money and, every lunch, having to pull out a bologna sandwich." (San Jose Mercury News 17 Apr 2001)
http://www.siliconvalley.com/docs/news/svfront/barks041701.htm

---

Category 16.1 *Industrial espionage*

2001-04-26 **industrial espionage trade secrets guilty plea court trial China**

CIND < http://www.nacic.gov/archives/nacic/news/2001/jun01.html >

Junsheng Wang of Bell Imaging Technologies pled guilty to violation of 18 USC 132(a)(2) by stealing trade secrets fom Acuson Corporation. The Counterintelligence News and Developments (CIND) report noted, "In pleading guilty, Wang admitted that prior to August 24, 2000, that he took without authorization and copied for Bell Imaging a document providing the architecture for the Sequoia ultrasound machine that contained the trade secrets of Acuson Corporation. According to Wang's plea agreement, he had been able to obtain access to the Acuson trade secret materials because his wife was employed as an engineer at that company and because she had brought that document into their home. After he had copied the document, he took it with him on business trips to the People's Republic of China, turning it over to Bell Imaging during 2000. "

Category 16.1 *Industrial espionage*

2001-05-04 **industrial espionage software theft international arrests**

NewsScan, NIPC Daily Report; http://www.usatoday.com/life/cyber/tech/2001-05-03-lucent-scientists-china.htm

Federal authorities arrested two Lucent scientists and a third man described as their business partner on May 4, charging them with stealing source code for software associated with Lucent's PathStar Access Server and sharing it with Datang Telecom Technology Co., a Beijing firm majority-owned by the Chinese government. The software is considered a "crown jewel" of the company. Chinese nationals Hai Lin and Kai Xu were regarded as "distinguished members" of Lucent's staff up until their arrests. The motivation for the theft, according to court documents, was to build a networking powerhouse akin to the "Cisco of China." The men faced charges of conspiracy to commit wire fraud, punishable by a maximum five years in prison and a $250,000 fine. (USA Today, 4 May 2001

Category 16.1 *Industrial espionage*

2001-05-29 **Echelon espionage electronic intelligence ELINT SIGINT industrial espionage international**

NewsScan

EUROPEANS SAY THEY WANT PROTECTION FROM U.S. SPY NETWORK
A new European Parliament report says that, despite U.S. denials, a U.S.-led intelligence-gathering computer network called Echelon does in fact exist, and is used primarily to intercept private and commercial communications rather than military intelligence. Other countries allegedly cooperating in Echelon include Britain, Canada, Australia and New Zealand. The EU report urges countries in that alliance to make more use of encryption software to protect the security of any business and personal communications of a sensitive nature. (AP/New York Times 29 May 2001)
http://www.nytimes.com/aponline/business/AP-EU-Echelon.html

Category 16.1 *Industrial espionage*

2001-07-05 **industrial espionage employee termination breach confidentiality investigation lawsuit**

NewsScan

LAWSUITS CHARGE EX-EMPLOYEES WITH DIVULGING COMPANY SECRETS

Data storage firm EMC has filed lawsuits against former employees it suspects of stealing company secrets and aiding its competitor, Network Appliance. "We prefer not to compete against our own technology," says an EMC spokesman, while a lawyer for Network Appliance responds that EMC's lawsuits are simply a strategy to impede the progress the company's business rivals: "The litigation started when there was a war in this industry for talent." (San Jose Mercury News 5 Jul 2001) http://www.siliconvalley.com/docs/news/svfront/039513.htm

---

Category 16.1 *Industrial espionage*

2002-04-12 **industrial espionage information warfare infowar international**

NewsScan

ADDED INDICTMENTS IN STOLEN TRADE SECRETS CASE
Three Chinese citizens, two of whom were Lucent scientists in that company's Murray Hill, N.J., headquarters have been charged with stealing secrets from four companies in addition to Lucent. They had already been indicted for stealing secrets from Lucent, but are now being charged with similar crimes against Telenetworks, NetPlane Systems, Hughes Software Systems, and Ziatech. The three New Jersey residents -- Hai Lin, Kai Xu, and Yong-Qing Cheng, all in their 30s -- are thought to have developed a joint venture with the Datang Telecom Technology Company of Beijing to sell a clone of Lucent's Path Star data and voice transmission system to Internet providers in China. (AP/New York Times 12 Apr 2002)
http://www.nytimes.com/2002/04/12/technology/12LUCE.html

Category 16.1 *Industrial espionage*

2002-09-20 **criminal hacker arrest software theft intellectual property industrial espionage infowar information warfare**

NewsScan

ARRESTS: SOFTWARE THEFT. . . .
. . . . In California's Silicon Valley, the FBI has arrested a Chinese programmer accused of trying to steal a software package used for seismic imaging of oil fields. The software was created by 3DGeo Development software company in Mountain View, California. The 32-year-old programmer, who is now in custody at the Santa Clara jail, has been in the U.S. since April as part of a contract between 3DGeo and his employer in China, the state-owned China National Petroleum Corporation. (Reuters and New York Times 19 Sep 2002)

Category 16.1 *Industrial espionage*

2003-05-08 **ericsson investigation sweden espionage spy Mansour Rokkgireh Alireza Rafiei Bejarkenari russia**

NIPC/DHS

THREE CHARGED IN ERICSSON SPY INVESTIGATION IN SWEDEN

Three Swedish employees of wireless equipment maker LM Ericsson face espionage charges, Swedish prosecutors said Thursday. Afshin Bavand is accused of handing over secret company information to a Russian intelligence agent, while Mansour Rokkgireh and Alireza Rafiei Bejarkenari are accused of helping him gather the information. "If these company secrets have been given away, it is my opinion that it may cause harm to the overall defense or to the security of the country," chief prosecutor Thomas Lindstrand told The Associated Press. But Ericsson spokesman Henry Stenson said the espionage involved the company's commercial telecommunications systems, and not its military-related work. Stockholm-based Ericsson also makes radar systems for defense programs worldwide, including for the JAS-39 Gripen fighter planes made by Sweden's Saab and Britain's BAE Systems.

Category 16.1 *Industrial espionage*

2005-01-24 **IBM Lenovo China industrial espionage national security**

NewsScan; http://news.com.com/IBM-Lenovo+deal+said+to+get+national+security+review/2100-1003_3-5547546.html

IBM'S PC BUSINESS SALE RAISES RED FLAG ON NATIONAL SECURITY

The U.S. Committee on Foreign Investments, which reviews acquisitions of U.S. businesses by foreign firms, says it's concerned that IBM's sale of its PC business to China's Lenovo Group could open the door for industrial espionage. The committee is composed of 11 U.S. government agencies, including the departments of Justice and the Treasury. The $1.75-billion deal has already passed the antitrust scrutiny of the Federal Trade Commission, which said it would not raise objections based on how the sale might affect competition in the market. The IBM-Lenovo transaction is the biggest PC industry deal since Hewlett-Packard acquired Compaq in May 2002, and would result in Lenovo becoming the third largest PC maker in the world, after Dell and HP. (CNet News.com 24 Jan 2005)

Category 16.1 *Industrial espionage*

2005-06-01 **industrial espionage Trojan horse spyware police investigation arrests harassment data theft copyright violation intellectual property social engineering keystroke logging remote control jail house arrest**

CNN; http://www.cnn.com/2005/TECH/06/01/israel.computer.breakin.ap/

TROJAN HORSE SCANDAL IN ISRAEL

Israeli author Amon Jackont was upset to find parts of the manuscript on which he was working posted on the Internet. Then someone tried to steal money from his bank account. Suspicion fell on his stepdaughter's ex-husband, Michael Haephrati.

Police discovered a keystroke logger on Jackont's computer. Turned out Haephrati had also sold spy software to clients; the Trojan was concealed in what appeared to be confidential e-mail. Once installed on the victims' computers, the software sent surveillance data to a server in London, England. Haephrati was detained by UK police and investigations were underway in Germany and Israel. Twelve people were in jail in Israel; eight others were under house arrest. Suspects included private investigators and top executives from industrial firms. Victims included Hewlett-Packard, the Ace hardware stores, and a cable-communications company.

[Abstract by MK]

EXTENSIVE INDUSTRIAL ESPIONAGE CASE IN ISRAEL

A large scale industrial espionage case unfolded in Israel…. A hacker had developed a Trojan horse application and sold it to several private eye companies -- it seems the Trojan was used for keyboard sniffing as well as file transfer. The private eyes' clients chose the the targeted victims, and the Trojan was sent there by e-mail or posted CD, masquerading as legitimate business presentation.

The collected info was transferred from the victims' computers into an FTP server site (it's not clear if this site was maintained by the private eyes or the hacker) to which access was sold to the clients in the form of one-time passwords at 2000 Euro per entry.

It seems none of the targeted systems was hardened in any way to detect such an intrusion, and the scheme was discovered only because the hacker had posted some of the illegally obtained items over the net.

[Abstract by Amos Shapir]

In RISKS 23.89, Gadi Evron contributed some follow-up information that included these comments::

>… Apart from the technical side of this attack and the extreme wide-scale of it, another interesting aspect is the use of social engineering.

In one description, I heard that a woman called a certain individual at one of the companies with a business offer, and later sent him a presentation via e-mail. When that presentation did not work, she proceeded to send him a CD, which did not work either….

This is not the first time this happened, and not the first time we've seen industrial espionage in IL, or private investigator companies developing their technological and operational capabilities. I've personally been approached about such a job twice in the past 2 years.<

Category 16.1 *Industrial espionage*

2005-06-20 **information warfare China Asia cyber-conflict economic harm costs industrial espionage**

RISKS 23 91

ASIAN HACKERS BLAMED FOR ATTACKS ON U.K., U.S. COMPUTER NETWORKS

A U.K.'s National Infrastructure Security Coordination Center (NISCC) report says unidentified hackers from Asia have been launching a wave of attacks on government and corporate computer systems in the U.S., Canada, and the U.K. in an effort to steal sensitive commercially and economically valuable information.

[Abstract by Peter G. Neumann]

Category 16.1 *Industrial espionage*

2006-01-31 **corporate industrial espionage information warfare Israeli couple held**

DHS IAIP Daily; http://today.reuters.com/news/NewsArticle.aspx?type=technolo gyNews&storyID=2006−01−31T121453Z_01_L31454049_RTRUKOC_0_US− CRIME−ISRAEL−SPYWARE.xml 23

ISRAEL HOLDS COUPLE IN CORPORATE ESPIONAGE CASE.

An Israeli couple suspected of masterminding a computer virus that set off a major industrial espionage investigation was repatriated for trial on Tuesday, January 31, under an extradition deal with Britain, police said. Michael and Ruth Haephrati were arrested in their London home last year over allegations that a Trojan horse program they had developed was bought by private investigators who helped top Israeli corporations spy on each other's computers. Israeli police spokesperson Mickey Rosenfeld said the couple flew in overnight after Britain approved their extradition. Tel Aviv Magistrate's Court ordered them placed in custody for 10 days so that they could be interrogated by police. Computer hacking carries a maximum five year jail term in Israel, which can be increased if data theft is involved. At least 18 other Israelis have been questioned in the Trojan horse case, including corporate executives. Several private investigators have been indicted on related charges. Among companies probed by police in connection with the case were Israel's top mobile phone operator, Cellcom, and two subsidiaries of phone company Bezeq Israel Telecom -- cellular operator Pelephone and the satellite television provider YES. All of the firms denied any wrongdoing.

Category 16.1 *Industrial espionage*

2006-03-15 **spyware software sale trial private investigators industrial espionage**

DHS IAIP Daily; http://www.theregister.co.uk/2006/03/15/spyware_trojan_guilty_plea/ 23

SPYWARE-FOR-HIRE COUPLE PLEAD GUILTY.

An Israeli couple faces prison after confessing to the development and sale of a spyware Trojan horse that helped private investigators snoop on their clients' business competitors. Ruth Brier-Haephrati and Michael Haephrati have entered guilty pleas to industrial espionage charges over the Trojan horse case. Ruth was charged with a litany of offenses including fraud, planting computer viruses, and conspiracy. Her husband, Michael, is charged with aiding and abetting those offenses.

Category 16.1 *Industrial espionage*

2006-03-28 **industrial espionage Trojan horse spyware police investigation arrests harassment data theft copyright violation intellectual property social engineering keystroke logging remote control jail trial conviction prison**

NEWSFACTOR < http://tinyurl.com/ouefj >

INDUSTRIAL ESPIONAGE COUPLE GETS JAIL TIME

The perpretrators of the Trojan Horse scandal that rocked Israel in May 2005 were sent to jail in March 2006. The husband-and-wife team installed Trojan horse software that functioned as keystroke loggers and transmitted confidential data for use in industrial espionage. They also had to pay about ½MU$ in restitution to their victims. Michael Haephrati, who wrote the software, went to prison for four years; Ruth Brier-Haephrati was jailed for two years for her role in selling the code to dishonest private investigators.

16.2 Industrial information systems sabotage

Category 16.2 *Industrial information systems sabotage*

1997-01-09 **Sabotage information warfare**

RISKS 18 75

The San Francisco Chronicle reported that a fired subcontractor was arrested and accused of trying to cause damage to the California Department of Information Technology. A later report indicated that the accused may have spent six hours online before being detected and crashing the system. Data had to be restored from backups. System management admitted that they had not known that the accused had been fired and therefore did not alter security after his dismissal. Another commentator added that some contracts explicitly forbid direct involvement of a contractor in facilities management duties; it would normally take weeks to send notification about a subcontractor's firing through the layers of governmental bureaucracy in such a case.

Category 16.2 *Industrial information systems sabotage*

1998-02-23 **insider attack hack logic bomb disaster downtime denial-of-service attack DoS sabotage lawsuit**

Computerworld 32 8

In July 1996, Timothy Lloyd, a network administrator and programmer at Omega Engineering, was fired. Unfortunately, Mr Lloyd had planted a logic bomb that put the network down, causing, according to Sharon Gaudin, writing in _Network World_, "more than $10 million in losses, $2 million in reprogramming costs and … 80 layoffs." Lloyd was convicted in July 2000 but two weeks later, a juror told the judge that she might have been influenced by a TV program in making her decision. The judge reversed the guilty verdict and ordered a retrial. Two years later, in March 2002, Lloyd was finally found guilty once again and sentenced to 41 months in federal prison. He maintained his innocence to the end.

Category 16.2 *Industrial information systems sabotage*

2000-01-09 **Web site hacked vandalized Trojan horse quality assurance technical support**

RISKS 20 74

Someone posted a message on the Intuit UK server that claimed to be offering an update to Quicken: "There is an upgrade available to updated [sic] your current version of Quicken 2000. Would you like to download the update now ? Don't be afraid, it is just a test : My name is Nour." RISKS Forum correspondent Stephen Page wrote, "Either test code has leaked into live service or their site has been hacked. In either case, it is a serious security breach for software which is trusted (e.g., a Trojan horse could create access to users' personal financial data)."

Category 16.2 *Industrial information systems sabotage*

2000-01-19 **criminal hacker insider sabotage Web**

Wall Street Journal

Global Health Trax Inc. reported that its old Web site was opened to unauthorized access in January, possibly because of sabotage by disgruntled employees. Although there was no evidence of penetration, detailed account information about hundreds of distributors was unprotected for several hours, including bank account and credit card numbers.

Category 16.2 *Industrial information systems sabotage*

2000-01-26 **software license copyright modification competition injunction lawsuit**

NewsScan, Los Angeles Times
http://www.latimes.com/business/20000126/t000008172.html, AP

In 1998, Sun Microsystems accused Microsoft of corrupting its implementation of Java to reduce the platform-independence of their product — a violation of Microsoft's license agreement. In January 2000, a federal court judge reinstated a suspended injunction barring Microsoft from distributing its modified version of Java to other software developers.

Category 16.2 Industrial information systems sabotage

2000-02-02 **sabotage software Trojan denial of service Internet access information warfare**

NewsScan; http://www.washingtonpost.com/wp-dyn/business/A60549-2000Feb1.html, http://www.washingtonpost.com/wp-dyn/business/A23076-2000Feb7.html

A Maryland attorney has filed a class-action suit against America Online, charging that version 5.0 of its software changes computer settings of users who try to upgrade from earlier versions and making it no longer possible for them to just click on the desktop icon of another Internet service provider to access the Internet. The attorney says that that AOL is in effect forcing the customer into behavior shaped to suit the company rather than the computer user, and complains: "The Internet is supposed to be like free speech, with open access." (Washington Post 2 Feb 2000)

[A few days later,] Three Washington-area Internet service providers have filed a class-action suit America Online charging that customers who install AOL's new version 5.0 software and choose it as the default browser find that their computer setting are changed in a way that makes it much harder to access providers that use other browsers, thereby allowing AOL to leverage its market position "to foreclose competition and gain unfair competitive advantage." Although not a party to the lawsuit, Prodigy is demanding compensation from AOL for the administrative and technical costs it incurred helping customers who found it difficult to access their Prodigy accounts after installing AOL version 5.0. An AOL executive says that lawsuits are without merit and insists: "We're not doing anything that other ISPs aren't doing." (Washington Post 8 Feb 2000)

YET ANOTHER "MONOPOLY"? AOL SUED BY SMALL ISP

[In April,] Galaxy Internet Services Inc., a small Internet service provider in Massachusetts, . . . [sued] America Online, charging that it "attempted to eliminate competition in the Internet service market" when it introduced new software (AOL 5.0) that blocks AOL subscribers from using other Internet service providers. About 8% of America Online subscribers also use some other ISP, and Galaxy is hoping to be joined it its suit by other competitors of AOL. (Reuters/San Jose Mercury News 4 Apr 2000)

Category 16.2 Industrial information systems sabotage

2000-02-10 **sabotage design quality assurance information warfare**

NewsScan, WP http://www.washingtonpost.com/wp-dyn/business/A31920-2000Feb9.html

Looking into complaints by end-users, small computer businesses and Microsoft rivals, the European Union on Wednesday launched a probe into allegations that Microsoft is bundling its new Windows 2000 operating system with other software in such a way that only its own products are fully interoperable, placing rivals at a disadvantage. Microsoft, which is still embroiled in a U.S. antitrust suit, denies the charges, claiming it has complied with EU competition law. If the EU finds the allegations to be true, it could force Microsoft to make changes to the operating system, or face fines of up to 10% of global revenues if it failed to do so. Microsoft, the world's biggest software company, earns nearly a quarter of its revenues in Europe. (Reuters/Washington Post 9 Feb 2000)

Category 16.2 Industrial information systems sabotage

2000-02-23 **Web vandalism penetration criminal hacker prosecution**

NewsScan, San Jose Mercury News http://www.sjmercury.com/svtech/news/breaking/merc/docs/080797.htm

Ikenna Iffih, a 28-year-old computer science student at Northeastern University has been charged with hacking his way into government and military computers and disrupting the operations of an Internet service provider in the state of Washington. If convicted, he will face up to 10 years in prison and a fine of $250,000. Prosecutors say that Iffih caused "substantial business loss, defacing a Web page with hacker graphics, copying personal information, or in the case of a NASA computer, effectively seizing control." (AP/San Jose Mercury News 23 Feb 2000)

Category 16.2 *Industrial information systems sabotage*

2000-04-12 **industrial espionage denial-of-service lawsuit sabotage**

dc.internet.com http://dc.internet.com/news/article/0,1934,2101_342551,00.html 20 76

In the long-running lawsuit by Moore Publishing against Washington law firm Steptoe & Johnson, LLP, United States District Judge Thomas Pennfield Jackson denied a defense motion to quash the lawsuit in mid-April. A report from <dc.internet.com> summarized the allegations as follows: "The suit claims an employee of Steptoe & Johnson used the stolen e-mail identity of a former client to launch and attempt to cloak the origins of a denial of service attack designed to overwhelm the Moore Publishing sites and server with bogus requests to prevent access by legitimate consumers and computer users." The attacks were discovered in August 1999; when the victim notified the apparent originators of the penetrations, the denial-of-service attacks began in high volume.

Category 16.2 *Industrial information systems sabotage*

2000-08-01 **sabotage intellectual property IP information warfare lawsuit**

NewsScan

Motorola . . . filed a federal lawsuit charging that its copyrights were infringed when the eBay online auction site was used to sell Motorola radio service software that allows personal computers to program two-way radios. A Motorola lawyer . . . [said], "We don't see any reason why pirates should benefit when our loyal customers are doing what they are supposed to do." (Reuters/New York Times 1 Aug 2000)

Category 16.2 *Industrial information systems sabotage*

2001-10-11 **physical damage insects hardware circuit computers microprocessor mother boards potential sabotage**

NewsScan

DEBUGGING COMPUTERS
Entomologists are warning of the growing risks of insect invasion for electronic hardware, but so far few U.S. manufacturers are taking note. "...Modern (circuit) boards of comprised of fiberglass, epoxy and copper, and we're not aware that insects are particularly (attracted to them," says a spokeswoman for circuit board manufacturer RB Design. But she may be mistaken, according to Lisa Spurlock, a spokeswoman for the Entomological Society of America. "Subterranean termites attack the plastic insulation around electric cables, gnaw on electrical wiring and cause short circuits." Manufacturers in Japan are taking the threat more seriously. Matsushita Electronic Components is mass-producing circuit boards coated with a special semi-transparent insecticidal film designed to repel cockroaches, and Panasonic says it has already installed the insect-repelling boards in tens of thousands of rice cookers and refrigerators for Japanese customers. (Wired.com 11 Oct 2001)
http://www.wired.com/news/technology/0,1282,47361,00.html

Category 16.2 *Industrial information systems sabotage*

2001-10-31 **critical infrastructure protection information warfare penetration criminal hacker court case decision penalty punishment imprisonment jail**

RISKS 21 74

According to a report on the Australian Broadcasting Corporation Web site, Vitek Boden, a computer hacker who hacked into the sewage control computer and intentionally released caused thousands of litres of raw sewage into creeks and parks on the lower Queensland Coast (and the grounds of the local Hyatt Regency), has been jailed for two years by a Maroochydore District Court jury [summarized by Peter G. Neumann in the RISKS Forum Digest].

http://www.abc.net.au/news/newslink/nat/newsnat-31oct2001-96.htm

---

Category 16.2 *Industrial information systems sabotage*

2002-06-26 **proposed legislation law statute copyright violation retaliation revenge denial-of-service attacks DOS peer-to-peer spoofing interception interdiction redirection cyberwar**

NewsScan

LEGISLATION WOULD SANCTION STUDIO HACK ATTACKS
Proposed legislation crafted by California congressman Howard Berman, whose district includes Hollywood, would provide a shield against legal liability for copyright owners, such as record labels and movie studios, that used high-tech attacks against peer-to-peer Web sites to stop them from enabling illegal file-sharing. "While P2P technology is free to innovate new and more efficient methods of distribution that further exacerbate the piracy problem, copyright owners are not equally free to craft technological responses," says Berman. "This is not fair." Included in the actions a copyright holder would be allowed to take are: interdiction, in which the copyright holder swamps a P2P file server with false requests so that downloads can't get through; redirection, in which would-be file swappers are pointed to a site that doesn't contain the files they're seeking; and spoofing, in which a corrupt or otherwise undesirable file masquerades as the song or movie file being sought by a file swapper. File-swapping companies criticized the bill, saying it opens the door for copyright holders to conduct "cyber warfare" against consumers. (CNet News.com 25 Jun 2002)
http://news.com.com/2100-1023-939333.html?tag=fd_top

Category 16.2 *Industrial information systems sabotage*

2004-02-19 **information warfare quality assurance QA Trojans bad code**

RISKS; http://seclists.org/lists/isn/2004/Feb/0011.html 23 21

MALICIOUS IT DESIGN IN SUPPORT OF THE COLD WAR

Sam Garst contributed this abstract to RISKS:

On 2 Feb 2004, *The New York Times* printed an editorial by William Safire entitled "The Farewell Dossier" describing a CIA campaign in the early 1980s that supplied Russia with deliberately flawed technology; this lead directly to the massive explosion of a Siberian gas pipeline. The CIA became aware that the KGB was purchasing technology on the black market, and endeavored to supply the KGB with technology that would pass inspection, and later fail catastrophically.

Two risks leap out at me (trying hard to separate out several moral issues):

- I may test for poor design, or poor manufacturing, but these products were designed to pass testing, and then fail. Should I start testing for malicious design (perhaps, if you're building sensitive infrastructure, this is common practice)?

- These intentional flaws could 'leak' into the legitimate product lines. Hopefully, these companies had (and still have) good software build processes and code repositories. . . .

Safire indicates the story is from a soon-to-be published book: Thomas C. Reed's _At the Abyss_

Category 16.2 *Industrial information systems sabotage*

2005-02-17 **VoIP voice over IP FCC phone company antitrust Colorado investigation denial-of-service DoS information warfare competition**

NewsScan; http://www.wsj.com/

PHONE COMPANY SUSPECTED OF BLOCKING VOIP CALLS

The FCC's investigating whether a rural phone company blocked access to the Vonage Internet-phone service, which was competing for the phone company's customers. The company has not been identified. The problem became public several days ago when Larry Lessig, a professor at Stanford Law School and an advocate of Internet freedom, mentioned Vonage's problem at an industry conference in Boulder, Colorado. Shutting off a potential competitor could violate antitrust laws barring companies that control essential facilities from refusing to give competitors the access needed to compete. (Wall Street Journal 17 Feb 2005)

Category 16.2 *Industrial information systems sabotage*

2005-05-17 **study Department Homeland Security revenge reason computer sabotage sociological psychological factors**

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml?articleID=163104819

DHS STUDY: REVENGE IS OFTEN THE REASON FOR COMPUTER SABOTAGE

Corporate insiders who sabotage computers so sensitive they risk endangering national security or the economy commonly are motivated by revenge against their bosses, according to a Department of Homeland Security (DHS) funded study released Monday, May 16. The study, conducted by the U.S. Secret Service and the U.S.-funded CERT Coordination Center at Carnegie Mellon University, examined dozens of computer-sabotage cases over six years to determine what motivates trusted insiders to attack and how their actions damage the country's most sensitive networks and data. The review described most attackers as disgruntled workers or former employees--typically working in technology departments--who were angry over disciplinary actions, missed promotions, or layoffs. The attacks included deleting vital software or data, posting pornography on an employer's Website, or crippling whole networks. The study said most saboteurs showed troubling signs before the attacks: truancy, tardiness, arguments with co-workers, or shoddy performance. Nearly all the employees took some steps to conceal their identities online as they plotted their attacks. All the attacks studied occurred between 1996 and 2002. The study said it did not examine insider attacks where employees sought to steal information to sell for profit or blackmail. Report: http://www.cert.org/archive/pdf/insidercross051105.pdf

16.3 Infrastructure protection & homeland security

Category 16.3 *Infrastructure protection & homeland security*

2000-02-17 **information warfare investigation denial-of-service government policy law enforcement legislation**

Reuters, AP

In the wake of the distributed denial-of-service attacks, US federal officials debated the appropriate responses to the high-profile interference with e-commerce. Attorney General Janet Reno said publicly on 2000-02-07 that the attacks were a "wake-up call" to improve Web security and to catch criminal hackers. However, she did not endorse proposals by FBI Director Louis Freeh to prosecute criminal hackers under US anti-racketeering statutes. She did strongly support criminal prosecution, however: "We've got to help define, by our prosecutions based on real crimes, what you can and can't do on the Internet," she said.

Category 16.3 *Infrastructure protection & homeland security*

2000-02-19 **information warfare infowar study panel conference**

UPI

At the American Association for the Advancement of Science (AAAS) meeting in Washington, DC, panelists from government and from private industry concurred that information warfare is a real threat to the United States. Speakers urged better cooperation among law enforcement officials around the world to catch the culprits responsible for attacks on systems and network; they also supported changes in international law to allow extradition of suspects. Skeptics such as Kevin Poulson scoffed that if the infrastructure were as vulnerable as infowar proponents claimed, we'd have no electricity.

Category 16.3 *Infrastructure protection & homeland security*

2000-02-24 **law enforcement federal agency infrastructure protection**

NewsScan, MSNBC http://www.msnbc.com/news/374361.asp

U.S. Attorney General Janet Reno . . . nixed a bipartisan Senate plan that would make a single federal agency responsible for securing all federal computer networks against cyber-sabotage. The proposed legislation, sponsored by Sen. Fred Thompson (R-Tenn.) and Sen. Joseph Lieberman (D-Conn.) would centralize oversight authority within the Office of Management and Budget. Without commenting directly on the plan, Reno said that fending off cyber-attackers will depend more on chips and circuits rather than who's in charge: "It is not just a matter of centralizing a particular function in a particular office, it is a matter of developing the technology to protect the technology, but to do so consistent with our constitutional rights." (APBNews.com 24 Feb 2000)

Category 16.3 *Infrastructure protection & homeland security*

2000-02-29 **infrastructure protection law enforcement government private industry Internet security**

NewsScan

Technology leaders are discouraging too much government involvement in online security. Howard Schmidt of Microsoft says that infrastructure security "does not lend itself to government management. The private sector has the knowledge and expertise to help fight against computer crimes on the infrastructures on which they operate." And Charles Giancarlo of Cisco Systems insists that "the technology industry showed that it can respond swiftly and effectively, taking steps to quickly beat back the attacks to make it harder for similar assaults to succeed in the future." But the view of Deputy U.S. Attorney General Eric Holder is that some private security will fail, and he says: "In such cases, law enforcement must be prepared and equipped to investigate and prosecute cybercriminals in order to stop their criminal activity, to punish them and to deter others who might follow in their path." (AP/USA Today 29 Feb 2000)

Category 16.3 *Infrastructure protection & homeland security*

2000-03-03 **government initiative infrastructure protection law enforcement safeguards**

NewsScan, USA Today http://www.usatoday.com/life/cyber/tech/cth501.htm

A new presidential directive [was]. . . issued requiring U.S. government agencies to assess their vulnerability to cybervandalism. Chief of Staff John Podesta will work the agencies to put together a government-wide plan, and President Clinton says, "We must do more to uphold Americans' high expectations that their right to privacy will be protected online." (Bloomberg/USA Today 3 Mar 2000)

Category 16.3 *Infrastructure protection & homeland security*

2000-04-26 **infrastructure information warfare intrusion attack real-time process control**

RISKS, http://www.techserver.com/noframes/story/0,2294,500197283-500270387-501418162-0,00.html 20 87

Steve Bellovin wrote in RISKS, "The Associated Press reports that hackers, in conjunction with an insider, penetrated computer systems belonging to Gazprom, the Russian gas monopoly. . . . What is especially interesting about this case is that they managed to take control of the system controlling the flow of gas in pipelines, according to the Russian Interior Ministry. This makes it one of the few confirmed incidents of direct cyberthreats to a country's infrastructure."

Category 16.3 *Infrastructure protection & homeland security*

2000-06-18 **air traffic control disruption failure infrastructure protection information warfare simulation**

RISKS, BBC http://news.bbc.co.uk/hi/english/uk/newsid_796000/796018.stm] 20 93

Peter G. Neumann wrote, "On 17 Jun 2000, thousands of would-be passengers were stranded when the main air-traffic control computer collapsed. The National Air Traffic Services computer was fixed later in the day, but the resulting congestion caused many people to spend the night at airports around the UK, and many flights were cancelled the next day as well. Heathrow and Gatwick were hardest hit, although other UK airports experienced severe delays. This was the second time in a week that the computer system had failed." [MK notes: consider this an information warfare simulation that supports the view that critical infrastructure protection truly is important.]

Category 16.3 *Infrastructure protection & homeland security*

2000-07-06 **critical infrastructure emergency phone service backhoe attack cable availability**

RISKS 20

Mark Richards reported on how a backhoe operator sliced through a major Bell Atlantic phone cable, cutting service not only to several thousand subscribers but also the local 911 emergency operators. The outage lasted several days.

Category 16.3 *Infrastructure protection & homeland security*

2000-07-31 **Internet connectivity topology availability infrastructure protection information warfare communications disruption**

RISKS 20

Researchers from Notre Dame University discovered that concerted attack on the most highly-connected nodes of the Internet would fragment the Net into non-communicating subsets.

Category 16.3 *Infrastructure protection & homeland security*

2000-09-25 **information warfare critical infrastructure protection book**

RISKS 21 07

The security world was rocked to its foundations when revered book reviewer Rob Slade published a favorable review of controversial writer and speaker Winn Schwartau's latest book, _Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Disruption _ [Thunder's Mouth Press, ISBN 1-56025-246-4]. Slade wrote, "s some may know, Winn Schwartau and I do not see eye-to-eye on the emphasis to be given to certain exhortations in alerting the public to matters of computer security. So when he informed me of his latest book, he noted that I might like to do the usual hatchet job on it. Unfortunately, I can't fully comply. While I may quibble with some aspects of his latest book, overall it is a good overview of the existing computer security situation, and would make a helpful introduction for new computer and Internet users. . . . While there is a heavy emphasis on the sensational, overall this book does provide the security novice with a fairly reliable picture of the current security environment. Possibilities are generally presented as such, and the analysis of relative dangers is usually good. A number of useful tips are given that can help home and small business computer users be more secure in their computer and network use. Security specialists will find little that is new here, but that is not the target audience for the book. I have frequently been asked for a recommendation for a general security introduction directed at the non-technical computer and Internet user, and, for all its flaws, I think this work may be the closest I've seen. "

Category 16.3 *Infrastructure protection & homeland security*

2000-12-08 **government policy information warfare national security**

NewsScan, USA Today http://www.usatoday.com/life/cyber/tech/cti892.htm

In August, Richard Clarke, the National Security Council's first Infrastructure Coordinator, called on industry to strengthen their own information security as a means of strengthening national security: "By protecting the IT security of your company, you can protect the security of your country." He listed several ways the US government is trying to improve information security:

* Supporting Information Sharing and Analysis Centers (ISACs), which are industry-specific groups of companies sharing information about INFOSEC;

* Possibly amending the FOIA (Freedom of Information Act) to reduce ISAC participants' fears of being forced to reveal sensitive information if they talk to government and law-enforcement officials about cybercrimes;

* Supporting INFOSEC research by spending $600M, especially in areas not immediately attractive to the private sector;

* Sharing classified information with "trusted partners."

Speaking at a computer security conference [in December], National Security Council member Richard Clarke told the audience that the next president of the U.S. should appoint (and get Congressional confirmation of) a government-wide chief information officer with authority to oversee all of the government's security. "What this presidential election year showed is that statistically improbable events can occur. It may be improbable that cyberspace can be seriously disrupted, it may be improbable that a war in cyberspace can occur, but it could happen." Clarke said that certain other nations have created information-warfare units and are "creating technology to bring down computer networks." (AP/USA Today 8 Dec 2000)

Category 16.3 *Infrastructure protection & homeland security*

2001-03-23 **infrastructure protection terrorism criminal hacking sabotage information warfare**

NewsScan

CONDOLEEZA RICE WARNS OF TERRORIST DISRUPTIONS TO THE NET
National Security Advisor Condoleeza Rice wants to heighten awareness by both private and government organizations of the threat that cyberterrorism poses to national stability: "Today, the cyber-economy is the economy. Corrupt those networks, and you disrupt this nation. It is a paradox of our times that the very technology that makes our economy so dynamic and our military forces so dominating also makes us more vulnerable... A clear willingness to show that you are prepared to confront the problem is what keeps it from happening in the first place." (USA Today 23 Mar 2001)
http://www.usatoday.com/life/cyber/tech/2001-03-23-rice-cyberterrorism.htm

---

Category 16.3 *Infrastructure protection & homeland security*

2001-05-02 **infrastructure protection information warfare e-mail Web criminal hackers defacement**

NIPC Daily Report

Hackers have knocked a Transportation Department Web site offline, leaving the department unable to post railroad decisions or use e-mail. The Surface Transportation Board's Web site was hacked on 1 May, spokesman Dennis Watson said, and federal investigators have been notified. The board is responsible for oversight of the nation's railroad industry, and sends out rulings on mergers and other railroad activities daily. The site also contains news releases, economic statistics and past decisions. It is not known whether any information on the site was altered or destroyed.responsible for the attack, or from what country it originated. Watson said technicians do not know when the site will be back online. (Source: Associated Press, 2 May)

Category 16.3 *Infrastructure protection & homeland security*

2001-06-21 **critical infrastructure protection terrorists criminal hackers**

NewsScan

COMPUTER SECURITY: A FAST-MOVING TARGET
Lawrence K. Gershwin, the top science and technology advisor to the Central Intelligence Agency has told a Congressional committee that he doesn't "feel very good about our ability to anticipate" network attacks on U.S. computers, because hackers are developing tools and techniques faster than the CIA can keep up. But so far (and probably for the next 5 to 10 years) individual terrorists do not appear to represent a major treat against the U.S. phone system or financial networks. "Terrorists really like to make sure that what they do works. They do very nicely with explosions, so we think largely they're working on that." However, without being able to "feel very good about our ability to anticipate," that sense of security could disappear at any time. (AP/San Jose Mercury News 21 Jun 2001)
http://www.siliconvalley.com/docs/news/svfront/082074.htm

Category 16.3 *Infrastructure protection & homeland security*

2001-07-17 **technology council regulation export coordination security**

NewsScan

BUSH TEAM PONDERS TECH EXPORT COUNCIL [31 Jan 2001]
The Bush administration is deliberating whether to create a federal Chief Information Officer -- a technology "czar" -- or to create a technology export council instead. The Tech Czar position has been proposed as a means to coordinate e-commerce policy at home and promote the industry abroad, but a council would focus on tech-related security issues as they apply to both the online industry and the national defense. The council would also address the thorny problems associated with aerospace and computer exports, and encryption standardization. (eWEEK 31 Jan 2001)
http://www.zdnet.com/eweek/stories/general/0,11011,2680725,00.html

COORDINATING BOARD FOR INFRASTRUCTURE PROTECTION [13 Jun 2001]
Rejecting the idea of having a single security czar, the Bush Administration is planning to create a coordinating board to manage the government's initiatives focused "critical infrastructure protection" (CIP), which guards information systems that are critical to national security. The board's chairman will report directly to the national security adviser, currently Condoleezza Rice. Paul Kurtz of the National Security Council explains: "We can't have a single government agency or single government entity handling this problem. The idea is a dispersed solution that allows coordination across agencies... We can't fight for each particular agency's needs. We can help, but we need to have each agency take responsibility for their security." (USA Today 13 Jun 2001)
http://www.usatoday.com/life/cyber/tech/fcw2.htm

BUSH TO ENLARGE CYBERSECURITY GROUP [17 Jul 2001]
The Bush Administration plans to expand the office responsible for cybersecurity, replacing a single official with a group of about 21 officials from various federal agencies, including the National Security Agency, the Central Intelligence Agency, the Federal Bureau of Investigation, and the departments of State, Defense, Justice, Energy, and Treasury. The group will report to Condoleeza Rice, the National Security Advisor. The former head of the Justice Department's computer crimes division, Mark Rasch, warns sardonically: "The bad news is, nobody will do anything about critical infrastructure protection until there's a global catastrophic failure. The good news is, there will be a global catastrophic failure." (AP/USA Today 17 Jul 2001)
http://www.usatoday.com/life/cyber/tech/2001-07-17-bush-cybersecurity.htm

---

Category 16.3 *Infrastructure protection & homeland security*

2001-09-20 **911 World Trade Center Pentagon terrorist attacks infrastructure law enforcement policy military investigation Internet Web communications**

NewsScan

PHONE CARRIERS OVERWHELMED BY PANICKED CALLERS [11 Sep 2001]
Long-distance, local and wireless carriers struggled to cope with unprecedented call volumes yesterday in the wake of the U.S. attacks. Telecom companies reported between two and 10 times the number of phone calls made on an average Tuesday, and between the hours of 9 a.m. and 12 noon many customers encountered busy signals, dead air or taped recordings saying the circuits were overloaded and to try later. Cingular Wireless reported the number of attempted calls ballooned by 400% in Washington, DC and 1,000% in its New Jersey switching center. AT&T said its network handled, on average, four million calls every five minutes, while Verizon Wireless was forced to move in portable cell antennas to boost network capacity. Meanwhile, customers of VoiceStream, which is one of the few U.S. wireless companies to use the GSM mobile standard, were able to contact friends and family using text messaging, which was unaffected by call volumes and network outages. (Financial Times 11 Sep 2001)
http://news.ft.com/news/industries/telecom

INTERNET PLAYS HUGE ROLE IN DISASTER COMMUNICATIONS [11 Sep 2001]
Various Internet chat rooms were created yesterday to provide information and discussion about the terrorist events that strained traditional communications facilities, and Web sites were inundated with traffic. Major news sites (CNN, FoxNews, MSNBC, YahooNews, and ABCNews) were slowed down, as were the sites of the airlines involved in the disaster, American Airlines and United Airlines. Statistics from Keynote Systems, which monitors Web performance, give some indication of how various sites were able to cope during the day: Nytimes.com, 9 a.m. 0% availability, 10-11 a.m. 43% availability; ABCNews.com, 9 a.m. 0% availability, 11 a.m. 5% availability; USAToday.com, 9 a.m. 18% availability (took 47 seconds to connect); MSNBC.com, 9 a.m. 22% availability (38 seconds to connect); CNN.com, 9-10 a.m. 0% availability. (CNet News.com 11 Sep 2001)
http://news.cnet.com/news/0-1005-200-7129241.html?tag=mn_hd

FBI TARGETS E-MAIL FOR CLUES [12 Sep 2001]
The FBI has served major U.S. Internet service providers with search warrants in connection with an e-mail address believed to be connected to Tuesday's terrorist attacks. "They wanted to know what we have on our network, and our logs about this [e-mail] address, if that address has flowed through our network at any time," said an executive at Earthlink. The address does not belong to Earthlink, but the company was told to expect more warrants as the investigation continues. "They said they're going to all the ISPs," he said. Earthlink said that agents did not install the Carnivore e-mail surveillance device on its servers, relying instead on Earthlink's own computer logs. Meanwhile, AOL and Yahoo officials said their companies were cooperating fully with the FBI and an MSN spokesman would only say that the company works regularly with law enforcement officials. (AP 12 Sep 2001)
http://news.excite.com/news/ap/010912/17/tech-attacks-internet-warrants

SECURITY AND PRIVACY ISSUES: THE BALANCING ACT GROWS HARDER [12 Sep 2001]
The technologists, who generally are strong privacy advocates, are struggling to decide what to do to maintain data privacy without hampering law enforcement efforts to stop terrorists. An executive of a security services company in New Jersey says: "Yesterday changed the way we live and there's a whole new dimension in the debate over privacy versus security. More people seem to be willing to compromise but no one seems to have figured out just yet what's reasonable." And a security director at an Internet service provider admits: "As much as I don't like the intrusive nature of online surveillance technology, I really want to find the guys who did this [Tuesday's terrorist attacks in New York and Washington]." But Joseph Turow, a University of Pennsylvania professor of privacy and new media insists: "The question is whether you overreact in pursuit of a handful of terrorists and in the process change the constitutional protections of millions of American citizens." (Washington Post 13 Sep 2001)
http:/www.washingtonpost.com/wp-dyn/articles/A21207-2001Sep12.html

PROTECTING THE NATION FROM CYBER ATTACKS [12 Sep 2001]
Although computer security observers have noticed no signs of unusual network activities since Tuesday's terrorist attacks, the FBI's National Infrastructure Protection Center held an emergency meeting yesterday to consider the situation. Computer security consultant Donn Parker says, "Terrorists attacked our financial and political centers Tuesday. The logical next step is to attack our computer infrastructure. That would shake Americans' daily lives." (USA Today 13 Sep 2001)
http://www.usatoday.com/life/cyber/tech/2001/09/13/cyber-attack-next.htm

BUSINESSES TURN ATTENTION TO DATA RETRIEVAL [12 Sep 2001]
In the wake of Tuesday's terrorist attack on Manhattan, businesses are scrambling to find programmers and system administrators to assist in retrieving the financial and corporate data that form the lifeblood of the information economy. Bill Miller, CTO for Storage Networks, says he has confidence the ability of financial markets to recover their data, but that the attacks go beyond the scope of his clients' disaster mitigation planning. Meanwhile, recovery efforts are hampered by the lack of a facility in which to do business. "Most of our customers are not planning on showing up downtown for another two weeks," says Sanjay Kumar, CEO of Computer Associates. "The real question is, 'Where do these people go to work?'" Last night, for

instance, CA bussed 40 network-design specialists from Atlanta to CA headquarters in Islandia, NY to assist in data recovery efforts. (Wall Street Journal 13 Sep 2001)
http://interactive.wsj.com/archive/retrieve.cgi?id=SB1000336758447443683.djm (sub req'd)

THE IMPORTANCE OF REMOTE BACKUP OF CRITICAL DATA [12 Sep 2001]
Financial companies like Morgan Stanley, devastated by the attack on the World Trade Center buildings in which they were headquartered, were still able to resume operations because they used backup software and data replication software to transfer all data through instantaneous telecommunications to equivalent computing facilities located in New Jersey. (Reuters/Yahoo News 12 Sep 2001)
http://dailynews.yahoo.com/

FBI WARNS OF POSSIBLE CYBER-ATTACKS [14 Sep 2001]
Corporate systems administrators are beefing up security on their networks in response to an FBI Terrorist Threat Advisory that calls for IT professionals to "implement appropriate security measures -- both physical and cyber." Many security firms say the nation's corporate systems have a long way to go and some firms, such as RedSiren Technologies, are providing additional security measures to their clients for free. Among the recommendations RedSiren is making to clients is to review critical logs for suspicious activity in an effort to prevent corporate computers being used for distributed-denial-of-service attacks and other malicious acts. The FBI advisory will expire Oct. 11. (ZDNet 14 Sep 2001)
http://dailynews.yahoo.com/h/zd/20010914/tc/net_admins_redouble_efforts_to_p revent_cyber-attacks_1.html

EXPERTS PREDICT CYBERATTACKS [18 Sep 2001]
Although cyberattacks were not launched after last week's terrorist events in New York and Washington, a number of security expects are expecting a wave of such attacks once the U.S. commences military action against the terrorists. John Gartner, director of Gartner's Internet security research group, says, "There is no doubt that we'll see big attacks coming. It's time to plan for that now." (Interactive Week/USA Today 18 Sep 2001) http://www.usatoday.com/life/cyber/zd/zd5.htm

DISASTER GIVES BOOST TO DATA STORAGE FIRMS [18 Sep 2001]
Data storage companies such as EMC; data back-up companies such as Veritas Software and Comdisco; and IT data center managers such as IBM and EDS are expected to see a rise in business in the coming months, as businesses scramble to safeguard their data assets. In addition, companies that provide services such as Web site hosting could see a boost from customers eager to locate critical parts of their IT systems outside of their own facilities. Although many corporations have slashed their information technology budgets for the year, even before last week's attacks the focus has been shifting away from new equipment purchases and toward data protection and management. "There has been a rebalancing of IT spending by large corporations towards data storage systems," says Veritas CEO Gary Bloom. (Financial Times 18 Sep 2001)
http://news.ft.com/news/industries/infotechnology

PEOPLE WANT NEWS, NOT SEX, IN CYBERSPACE [19 Sep 2001]
Sex, a long-time Top 10 search engine term, has dropped down to No. 17 in popularity following last week's attacks. "Popular search terms last week turned almost exclusively to disaster-related information," says a spokesman for AltaVista. In addition to sex, almost all the perennial favorites like Pamela Anderson Lee, Britney Spears and Backstreet Boys were knocked off the list. Replacing them were news-related search terms, including CNN, news, World Trade Center, BBC and Pentagon. Google and Yahoo confirmed the same pattern on their search engine sites, with Yahoo saying its traffic had surged to at least 10 times normal levels since last week, and the overwhelming number of users seeking information about the attacks. (Reuters 19 Sep 2001)
http://news.excite.com/news/r/010919/20/net-attack-internet-dc

FEDS TRACK TERRORISTS' PAPERLESS TRAIL [20 Sep 2001]
Federal agents are retracing the steps of the 19 hijackers involved in last week's attacks, who apparently used a pay-per-use public Internet terminal at a Kinko's store in Hollywood, Fla. to access online ticket sites. According to an FBI document obtained by Der Spiegel magazine, some of the hijackers even entered their frequent flier numbers as they purchased their electronic tickets. A spokesperson for Travelocity confirmed that at least two of them had used the service to book flights, but declined to say whether they had booked their seat assignments on their desired planes, as some in the media have speculated. A research librarian in Delray Beach, Fla., also confirmed that one of the 19 men named by the FBI had used a computer at her library in late August. (Wired.com 20 Sep 2001)
http://www.wired.com/news/politics/0,1283,46991,00.html

TECHNOLOGY REPLACEMENT COSTS ENORMOUS [20 Sep 2001]
Billions of dollars will be spent to replace technology destroyed in the terrorist attacks last week, and some computer manufacturers have ramped up production of PCs to a night-and-day basis to meet the need. Industry analyst Astok Kumar says: "Basically, Dell and Compaq will pick up most of the business and it will give the industry a much-needed shot in the arm." One individual involved with the reconstruction process said: "It's just staggering to me. We spent thousands of dollars just to get these bankers up and running over this weekend, and this is just temporary. It is not replacing their equipment." (New York Times 20 Sep 2001)
http://www.nytimes.com/2001/09/20/nyregion/20COMP.html

Category 16.3 *Infrastructure protection & homeland security*

2001-10-15 **GOVNET government restricted network critical infrastructure protection hardened**

NewsScan

BUSH ADMINISTRATION WANTS ITS OWN INTERNET [11 Oct 2001]
The Bush Administration, citing security concerns, has proposed a new Internet-like network be created to handle sensitive government information. The new network, dubbed GOVNET, is the brainchild of Richard Clarke, the newly appointed presidential adviser for Cyberspace Security. "Planning for this network has been going on for several months," says Clarke. The General Services Administration, which will play a key role in deploying the self-contained network, has posted a Request for Information on its Web site, calling on the high-tech industry to create potential blueprints for GOVNET. "There will be no interconnections or gateways to the Internet or other public or private networks," says the RFI, which also calls for immunity to cyber-attacks and full encryption using the standard recommended by the National Security Agency. (ZDNet News 11 Oct 2001)
http://news.excite.com/news/zd/011011/07/should-the-government

'GOVNET' WOULD BE A MISTAKE, EXPERTS SAY [15 Oct 2001]
The Bush administration's proposed "Govnet" -- an independent government computer network that is separate from the Internet -- would be costly and would fail to create a safe haven from hack attacks and viruses, according to security experts. While the concept is theoretically feasible, it would be very difficult to execute. For instance, inside government offices, employees could easily pass viruses from the public Internet to Govnet via floppy disks, unless the floppy disk drive were locked shut. And if the Govnet fiber optic cable is run through the same conduits used by the Internet, it would be susceptible to the same sorts of physical attacks. "The thought is if we can have complete control over it, it will be bulletproof," says one security expert. "But this is farfetched unless they assume there's not going to be any kind of human intervention or place where someone is going to connect in through a PC." Experts recommend that instead of creating a new network from scratch, the government should improve its security practices and use existing security technologies. One possibility would involve virtual private network technology, which enables businesses to use the Internet securely by encrypting data communications before they are sent over the public network and decrypting them at the receiving end. (Reuters/SiliconValley.com 15 Oct 2001)
http://www.siliconvalley.com/docs/news/svfront/002314.htm

Category 16.3 *Infrastructure protection & homeland security*

2002-01-17 **critical infrastructure protection terrorism**

NewsScan

FBI WARNS OF TERRORIST ATTACKS ON GOVERNMENT INFOSYSTEMS [17 Jan 2002]
The FBI's infrastructure-protection team has alerted law-enforcement officers and high-tech companies of the possibility of new terrorist attacks on or through utility, municipal, or state information systems. The warning was not specific with regard to time frame or geographic area and its urgency-level was not as high as previous general alerts issued by the government to all Americans. (AP/USA Today 17 Jan 2002)
http://www.usatoday.com/life/cyber/tech/2002/01/17/net-warning.htm

---

Category 16.3 *Infrastructure protection & homeland security*

2002-01-24 **data leakage Web infrastructure protection national security**

Security Wire Digest 4 6

A National Infrastructure Protection Center (NIPC) Advisory recommended that Web sites be edited to remove sensitve data that could be useful to terrorists and other enemies of the US.

Category 16.3 *Infrastructure protection & homeland security*

2002-01-25 **homeland security airport scanners X-ray radiation privacy**

NewsScan

I-SEE-YOU: AIRPORT SECURITY MACHINES PEEK THROUGH CLOTHING
New security devices being tested at the Orlando airport are designed to find explosives residue, hazardous materials, metal items, and are able to see through clothes; airlines whose passengers will be asked to volunteer for scanning include Delta, Virgin Atlantic, Swissair and British Airways. The body scanner is expected to be the most controversial of the five machines being tested, because it subjects a passenger to low-level X-rays that penetrate clothing. (AP/USA Today 25 Jan 2002)
http://www.usatoday.com/life/cyber/tech/2002/01/25/airport-security.htm

---

Category 16.3 *Infrastructure protection & homeland security*

2002-01-31 **critical infrastructure protection law enforcement terrorists targets Web Internet research**

NewsScan

FBI SAYS TERRORISTS HAVE USED INTERNET TO FIND NEW TARGETS
The National Infrastructure Protection Center (NIPC), which is the FBI's top cyber-security unit, says that al-Qaeda terrorists were apparently using the Internet to seek targets among American dams and water-supply systems and to acquire information about certain insecticides and pest-control products. Information obtained by the NIPC indicates that the terrorists had sought information on the supervisory control and data acquisition networks that control water supplies and wastewater facilities. (AP/USA Today 31 Jan 2002)
http://www.usatoday.com/news/attack/2002/01/31/terrorists-net.htm

---

Category 16.3 *Infrastructure protection & homeland security*

2002-03-06 **international terrorism information warfare Web communication**

NewsScan

NEW AL QAEDA ACTIVITY ON THE INTERNET
U.S. government officials say they've discovered the existence of new Web sites created by Al Qaeda. The terrorist organization has always relied heavily on the Internet for communicating among its worldwide members, and its use of public Internet cafes and kiosks has made its communications difficult to track. The group has members in as many as 60 different countries. (New York Times 6 Feb 2002)
http://partners.nytimes.com/2002/03/06/international/asia/06INQU.html

---

Category 16.3 *Infrastructure protection & homeland security*

2002-03-08 **information warfare infrastructure military communications financial systems attack subversion interference**

NewsScan; http://www.usatoday.com/life/cyber/tech/2002/03/07/cuba-cyberattack.htm

STUDYING CUBA'S ABILITY USE NET TO DISRUPT U.S.
A senior U.S. government official says that the Bush administration has begun a review of Cuba's ability to use the Internet to disrupt this country's military communications or damage other U.S. interests. Last month, White House technical advisor Richard Clarke told a congressional subcommittee that if the U.S. is attacked through cyberspace, it could respond militarily: "We reserve the right to respond in any way appropriate: through covert action, through military action, and any of the tools available to the president." (AP/USA Today 7 Mar 2002)

Category 16.3 *Infrastructure protection & homeland security*

2002-03-13 **emergency wireless communications network homeland defense infrastructure cyberterrorism**

NewsScan

CEOs PLANS NETWORK TO RESPOND TO TERRORIST ATTACK
A task force formed by the Business Roundtable, an organization of corporate chief executives, is planning a nationwide system called CEO Link, designed to allow corporations to communicate with each other in the event of a terrorist attack. The president of Business Roundtable said that the more than 40 top executives who worked on the project "are really looking to make a difference for the country. They aren't coming to the table with business agendas. They're looking at how to make the country more secure." The group is chaired by C. Michael Armstrong of AT&T, which is preparing the design of CEO Link at its own expense. The system will include a wireless phone network as well as a secure Web site. (Washington Post 13 Mar 2002)
http://washingtonpost.com/wp-dyn/articles/A16827-2002Mar12.html

---

Category 16.3 *Infrastructure protection & homeland security*

2002-03-24 **information warfare infowar cyberterrorism book review**

RISKS 21 98

Noted infowar gadfly Winn Schwartau -- the cyberterrorism prophet everyone either loves or hates -- published another novel in 2002, _Pearl Harbor Dot Com_. Peter G. Neumann's review in RISKS read in part, "[T]his book seems to make a rather compelling novel out of a surprisingly large number of security and reliability risk threats that we have discussed here over the years. The story echoes one of the fundamental problems confronting Cassandra-like risks-avoidance protagonists and agonists alike, namely, that, because we have not yet had the electronic Pearl Harbor, people in power perceive that there is little need to fix the infrastructural problems, so why bother to listen to the doom-sayers who hype up the risks? Well, in this novel, one man's massive craving for vengeance reaches major proportions, and significant effects result on critical infrastructures. In the end, the good hackers contribute notably to the outcome.

The book is somewhere within the genre of technothrillers, with a typical mix of murder, mayhem, intrigue, computer-communication surveillance, and non-explicit s*x. I enjoyed it. It is entertaining, and the convoluted plot is quite consistent, fairly tight, and to RISKS readers, each incident is technologically quite plausible -- because many of the attacks seem almost reminiscent of past RISKS cases, sometimes just scaled up a little."

Category 16.3 *Infrastructure protection & homeland security*

2002-04-03 **financial services database data mining investigation forensics terrorists**

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/2989812.htm

CAN BUSINESS DATABASES BE USED IN ANTI-TERRORIST WAR?
A group of major companies that includes American Express, Visa, JP Morgan, Fidelity Investments, and CapitalOne is studying corporate databases to determine whether they can be used to find terrorists. Such databases usually include information about a person's home and car ownership, occupation, magazine subscriptions, and so forth. A lawyer working for the group says, "We have to think about how to use information to create profiles about what a bad guy might look like. This is business folks coming together to talk about how we might think about these issues. If companies go off and do advocacy based on what they learn here, that's how business works." Privacy advocates are wary, and James X. Dempsey of the Center for Democracy and Technology says he hopes the use of corporate databases to find terrorists is not an idea that is being "oversold, or overbought." (AP/San Jose Mercury News 3 Apr 2003)

Category 16.3 *Infrastructure protection & homeland security*

2002-04-17 **globalization information warfare inforwar international vulnerability**

NewsScan

ONE-FOURTH MELLON FINANCIAL'S I.T. WORK MOVED TO INDIA
The latest financial giant to move much of its information technology work outside U.S. borders, Mellon Financial will soon be sending a quarter of its routine software maintenance chores to India. (A study by the Meta Group consulting firm indicates that an Indian programmer can be hired for one-fourteenth the rate of an American programmer.) Mellon executive Ken Herz says the company hopes to have new work for all U.S. workers affected by the company's decision, and explains: "This project emphasizes our intent to focus Mellon technology talent on growth-related projects and have routine maintenance work done offshore." (San Jose Mercury News 16 Apr 2002)
http://www.siliconvalley.com/mld/siliconvalley/3077722.htm

Category 16.3 *Infrastructure protection & homeland security*

2002-04-22 **homeland security infrastructure protection government network GovNet**

Security Wire Digest 4 31

*CLARKE: GOVNET READY FOR NEXT PHASE
Despite no money earmarked for an actual program or project, U.S. cybersecurity czar Richard Clarke told a conference audience GovNet is moving forward. An impenetrable information network exclusively for the federal government is feasible, according to a General Services Administration review based on surveys from 167 technology companies. Clarke told federal IT workers last week that it's time to determine how much it will cost to build a tamper-proof network. Possible "paths" for GovNet include improving security on existing federal networks, allowing agencies to build their own stand-alone or multi-agency networks, or utilize existing stand-alone networks and create a backup network in case there's a disaster or attack.

Category 16.3 *Infrastructure protection & homeland security*

2002-05-07 **information warfare infrastructure protection failure problems weakness vulnerability financial systems health data communications emergency**

NewsScan; http://www.usatoday.com/life/cyber/tech/2002/05/06/cyber-terror.htm

UNPREPARED FOR CYBERATTACKS?
People with knowledge of national intelligence briefings say that little has been done to protect the country against a cyberattack. Senator Jon Kyl (R-Ariz.) says: "It's a big threat, because it is easy to do and can cause great harm," and vulnerable U.S. targets are said to include the Centers for Disease Control and Prevention; FedWire, the money-movement clearing system maintained by the Federal Reserve Board; computer systems that operate water-treatment plants or that run electrical grids and dams; facilities that control the flow of information over the Internet; the nation's communications network, including telephone and 911 call centers; and air traffic control, rail and public transportation systems. Rep. Jane Harman (D-Calif.) says: "What I fear is the combination of a cyberattack coordinated with more traditional terrorism, undermining our ability to respond to an attack when lives are in danger." (USA Today 6 May 2002)

Category 16.3 *Infrastructure protection & homeland security*

2002-05-24 **homeland security cybersecurity information warfare government budget funding research expenditures critical infrastructure**

NewsScan

CYBERSECURITY GETS $1.7 BILLION BOOST IN BUDGET
The Bush Administration has included a $1.7 billion increase in cybersecurity in its proposed budget -- 68% over its current level. Last fall a congressional survey gave a grade of "F" to 17 of 24 major federal agencies for their level of security preparations. In the new budget, overall technology spending by the federal government will increase from $45 billion to $52 billion, but Department of Commerce undersecretary Ken Juster notes that 90% of the nation's critical infrastructure (e.g., transportation and communication systems and power grids) is privately owned and operated, and suggests: "The insurance and legal industries should reward companies" that make computer security "as integral a part of their business as marketing and product development." (The Record, Hackensack NJ/San Jose Mercury News 23 May 2002)
http://www.siliconvalley.com/mld/siliconvalley/3324403.htm SECURITY

Category 16.3 *Infrastructure protection & homeland security*

2002-06-27 **security flaws obscurity national security quality assurance QA**

RISKS 22 13

Brien Webb wrote an interesting analysis of Microsoft testimony:

>From a 2002/05/13 article by Caron Carlson in eweek.com:

http://www.eweek.com/article/0,3658,s%253D701%2526a%253D26875,00.asp

"A senior Microsoft Corp. executive [Jim Allchin] told a federal court last week that sharing information with competitors could damage national security and even threaten the U.S. war effort in Afghanistan. He later acknowledged that some Microsoft code was so flawed it could not be safely disclosed."

and later, directly quoting Allchin...

"Computers, including many running Windows operating systems, are used throughout the United States Department of Defense and by the armed forces of the United States in Afghanistan and elsewhere."

Microsoft proposes to withhold details of the MSMQ protocol (TCP port 1801 and UDP port 3527), the Windows File Protection API, as well as APIs for anti-piracy protection and digital rights management under the security carve-out.

I recall that the Windows NT family of operating systems was designed to meet DOD's C2 security criteria, including the Orange Book (standalone, which they passed), as well as Red Book (networking) and Blue Book (subsystems) criteria which they started working on at least 4 years ago; I don't know if they've yet passed, but I suspect not if it's so flawed that they don't want to disclose the protocol or API! See
http://msdn.microsoft.com/library/default.asp? url=/library/en- us/dnproasp2/html/windowsntsecuritysystems.asp

So, one risk of flawed software might be that you have to publicly invoke national security (read patriotism) as a last refuge from legal process.<

Category 16.3 *Infrastructure protection & homeland security*

2002-06-27 **infrastructure protection terrorism distribution control systems DCS supervisory control data acquisition SCADA 911**

NewsScan

OFFICIALS FEAR TERRORIST ATTACKS ON DCS AND SCADA SYSTEMS
For some months now the FBI has been evaluating evidence that al-Quaida terrorists located throughout the world have been trying to develop ways to use the Internet to interfere with the control of major physical systems in the U.S., such as dams, utility systems, nuclear power plants, and so forth. Those kinds of facilities are managed through digitally systems called "distributed-control systems" (DCS) and "supervisory control and data acquisition" (SCADA) systems. Systems like that were typically not designed with public access in mind, so they usually lack even rudimentary security protection. The director of the FBI's National Infrastructure Protection Center said last month: "The event I fear most is a physical attack in conjunction with a successful cyber-attack in conjunction with a successful cyber-attack on the responders' 911 system or on the power grid." (Wash Post/San Jose Mercury-News 27 Jun 2002)
http://www.siliconvalley.com/mld/siliconvalley/3554402.htm

Category 16.3 *Infrastructure protection & homeland security*

2002-07-25 **cyberterrorism information warfare infrastructure protection homeland defense**

NewsScan

THE RISKS FROM CYBERTERRORISM
Cybersecurity experts are busy lobbying Congress for protections from liability lawsuits but some analysts say the media may be over-stating the risks from terrorist cyber attacks. Marc Maiffret of eEye Digital Security says, "Terrorists are only recently starting to realize the benefits of having people within their organizations that have real hacking skills," and University of South California professor of communications Douglas Thomas adds: "Cyber-terrorism is a lot more difficult than many people assume." Even so, security expert Stanley Jarocki warns that terrorists could do a lot of damage by cracking U.S. corporate systems: "Today, some say it would be easier for a terrorist to attack a dam by hacking into its command-and-control computer network than it would be to obtain and deliver the tons of explosives needed to blow it up. Even more frightening, such destruction can be launched remotely, either from the safety of the terrorist's living room, or their hideout cave." (AP/USA Today 24 Jul 2002)
http://www.usatoday.com/tech/news/computersecurity/2002... protection_x.htm

---

Category 16.3 *Infrastructure protection & homeland security*

2002-08-22 **wireless emergency response communications network law enforcement government infrastructure protection**

NewsScan

IBM TEAMS WITH U.S. GOV'T ON WIRELESS EMERGENCY NETWORK
IBM is working with a consortium of government agencies to build a wireless emergency network that will enable police, fire and safety groups in the Washington, DC area to communicate with each other in real time via instant messaging. The Capital Wireless Integrated Network (CapWIN) -- the first such network in the nation -- will run on top of existing communications and computer systems and will be accessible via standard PCs, handhelds and cell phones. "The purpose of CapWIN is to enable these functions by leveraging existing networks and systems... The hard part is going to be to make sure that we get the user requirements defined correctly the first time," says Kent Blossom, director of safety and security systems for IBM, which will supply clustered eServers to link to installed servers and databases. The CapWIN network will enable law enforcement and emergency response groups to communicate with one another over a secure IM system, search multiple databases, and facilitate better coordination between different agencies or officers responding to an emergency. (CNet News.com 21 Aug 2002)
http://news.com.com/2100-1001-954809.html

Category 16.3 *Infrastructure protection & homeland security*

2002-09-10 **infowar information warfare cyberwar infrastructure protection homeland security**

NewsScan

WORTH THINKING ABOUT: WHY WE REALLY, REALLY NEED COMPUTERS
Resist all those temptations to smash your computer and walk away. Think of where you'd be without it. Michael White, former science editor of British GQ, writes: "Even though most of us can recall a time when digital, modem, and hard drive were not words we thought about or used often, it is difficult to imagine a world without computers. If all the computers in the world shut down tomorrow, we would not simply regress to a time before they were commonplace — there would be no return to a 1950s lifestyle — such an event would mark the end of civilization itself. For today we are totally dependent upon computers. The way electricity is delivered to our homes and our factories, the way essential commodities such as gasoline and food reach us is controlled entirely by automated computerized networks. If the world's computers were to shut down, our gas, electricity, and water supplies would soon stop; sewage systems would fail; the financial markets would collapse in disarray; communications would break down; there would be no TV, no radio; military and law-enforcement establishments thrown into confusion; hospitals could function only on a basic level. And from all this, anarchy would soon follow."

Category 16.3 *Infrastructure protection & homeland security*

2002-09-18 **cybersecurity plan homeland defense infrastructure protection infowar information warfare**

NewsScan

BUSH ADMINISTRATION PONDERS CYBERSECURITY PLAN
The Bush Administration is considering creating a technology fund, possibly "jointly financed by government and industry," that would "address those "areas that fall outside the purview of both industry and government and yet are critical to the future secure functioning of the Internet." Working papers for the national cybersecurity plan cite the development of highly secure versions of computer operating system software as something that could be paid for by the proposed fund. In addition, the draft documents discuss sweeping new obligations on companies, universities, federal agencies and home users to secure their own "portions of cyberspace." Other ideas under consideration include: improving security of wireless technologies and prohibiting their use in some cases by federal workers; beefing up protection of computer systems that help operate major utilities like water and power; coming up with a game plan for responding to cyberattacks when it's not immediately evident whether the source is a hostile government or a teenage hacker; creating an industry testing center that would ensure software updates don't undermine security measures; and contemplating the creation of a new government network that would handle communications and computing tasks during Internet outages. The White House cautioned that the ideas in the working papers are subject to change until approved by the president, and that any recommendations would still need go through traditional policy and budget processes. (AP 7 Sep 2002)
http://apnews.excite.com/article/20020907/D7LT1J980.htm

CYBERSECURITY PLAN AUTHORS SEEK FEEDBACK
The White House panel drafting recommendations on beefing up U.S. cybersecurity has decided to open it up for more comment before it is presented to President Bush in two months. "If we just come up with a government strategy and announce it without participation from the people who have to implement it, we're not going to get the level of cooperation? that we need for this," says Bush administration senior cybersecurity advisor Richard Clarke. The National Strategy to Secure Cyberspace offers nearly 60 suggestions on ways that home users, small businesses, universities, large corporations and government agencies can improve cybersecurity, including installing and using security products such as firewalls and antivirus software. However, the draft report backs away from legal action. "We're not creating regulation, not creating mandates," says Clarke. "We want to do this through market forces." (AP 18 Sep 2002)
http://apnews.excite.com/article/20020918/D7M4185O1.htm

Category 16.3 *Infrastructure protection & homeland security*

2002-10-29 **cybersecurity plan homeland defense infrastructure protection infowar information warfare**

NewsScan

HOME ISN'T WHERE THE SECURITY IS

Columnist Robert Lemos says the Bush administration's plan to ask home computer users to secure their systems as part of its "National Strategy to Secure Cyberspace" is a misguided effort. Citing the prevalence of users who still call tech support wondering why their computer won't turn on (because they've neglected to plug it in), Lemos says: "The experts are guilty of wrongheaded thinking in relying upon home users to shore up the nation's security. Frankly, that's somebody else's job. Home users are responsible for protecting their own important data. But it's a dangerous illusion to believe they will take better precautions after authorities ask them to upgrade their cyberdefenses." Lemos says the government instead should be focusing on persuading the ISPs "to protect cyberspace from home users. There are simple technologies for doing this. Source egress filtering — a technique for preventing users from sending data with a false source address, useful in denial-of-service attacks — should be the norm. Companies filter e-mail messages for any viruses and disallow several types of executable attachments; ISPs should do the same." Security expert Dorothy Denning says the only question left is, who will pay? "Once you start formalizing where we are going to put liability, the questions start coming up about who's going to pay for it. And, almost anywhere you put it, the costs are going to end up coming back to the users." (CNet News.com 29 Oct 2002)
http://news.com.com/2010-1071-963614.html

Category 16.3 *Infrastructure protection & homeland security*

2002-10-30 **cyberterrorism infowar information warfare homeland defense infrastructure protection**

NewsScan

WARNING OF SIMULTANEOUS CYBER- AND CONVENTIONAL TERRORISM
Rand Corporation's Brian Michael Jenkins told attendees at a security conference in London: "We do not have concrete evidence that terrorists are about to carry out sabotage by coming through cyberspace, but if there's one thing we know: the downside risks of ignoring it exceed the cost of preparation." Acknowledging that terrorists have in the past tended toward bombs and bloodshed, Jenkins indicated that there's an increasing potential for them to coordinate attacks of physical violence with a simultaneous attack on a computer network, and warned: "Such sabotage may become more attractive if the Internet makes it easier to facilitate." (Reuters/San Jose Mercury News 30 Oct 2002)

Category 16.3 *Infrastructure protection & homeland security*

2002-11-20 **infrastructure protection homeland defense infowar information warfare cyberterrorism government defenses**

NewsScan

HOUSE SUBCOMITTE FLUNKS U.S. ON INTERNET SECURITY
A U.S. House of Representatives Government Reform subcommittee has concluded that U.S. Internet security suffers serious problems, especially in the departments of State, Justice and Transportation. The exception to the rule is the Social Security Administration, which the head of the committee called a "shining example of sound leadership and focused attention" on computer security. The most glaring weakness at other agencies is vulnerability against insiders attempting sabotage or trying to profit personally by destroying or stealing sensitive information. And Richard Pethia of the federally funded CERT Coordination Center warned the committee: "Until customers demand products that are more secure or there are changes in the way legal and liability issues are handled, the situation is unlikely to change." (USA Today 19 Nov 2002)

Category 16.3 *Infrastructure protection & homeland security*

2002-11-22 **homeland security infowar information warfare cyberterrorism infrastructure protection**

NewsScan

BY-PRODUCT OF HOMELAND SECURITY IS BUSINESS FOR IT COMPANIES

The creation of the new 170,000-person Department of Security, which among other things will integrate the activities of 22 existing government agencies, will have enormous consequences for information technology contractors, and Harris Miller of the Information Technology Association of America predicts: "The impact is going to be quick and dramatic, and it will provide a lot of opportunities for IT companies." Just a few of those opportunities are: a $10 billion project by the Immigration and Natural Service to keep track of people entering the U.S.; the creation of an advanced research projects agency, along the lines of the Pentagon's DARPA; and a host of activities required to bring all 22 agencies up to a baseline level of security. (San Jose Mercury News 22 Nov 2002)

Category 16.3 *Infrastructure protection & homeland security*

2002-11-25 **homeland defense infrastructure protection warning system**

NewsScan

CALL FOR NEW EMERGENCY WARNING SYSTEM

An expert panel called Partnership for Public Warning comprising members from FEMA, the FBI, the NRC, and the American Red Cross is calling for creation of a high-technology warning system to be placed under the management of the new Department of Homeland Security. The group's chairman, Peter Ward, says: "Our vision is that every person at risk from natural disaster, an accident or terrorism would get a heads-up. Every piece of electronics you own — be it cell phone, a car phone, a computer a radio, a television — should have ability to give you a heads-up. It's not hard to think of many scenarios with weapons of mass destruction where, if you get to people right away and tell them to get out of harm's way, you save thousands of lives." (New York Times 24 Nov 2002)

Category 16.3 *Infrastructure protection & homeland security*

2002-11-26 **homeland defense infrastructure protection education responsibility**

NewsScan

SAFE & SOUND IN THE CYBER AGE

Stephen and Chey Cobb, security consultants, remind you that computer security is your patriotic duty:
... "Fellow citizens, now is the time to firewall your broadband connections and filter your email, lest your computer be abused by those who would attack our nation's critical infrastructure. Now is the time to do your patriotic duty and install security patches for your applications, change your passwords, and tighten up those directory permissions. If not, that computer in your den, the one on the high speed Internet connection, could become an attack platform."

Sound a little hokey? Maybe, but we'd be surprised if anyone can find a flaw in the logic or fault any of the stated facts. As far as we are concerned, and we're the ones who've been giving this speech, the large and growing number of unprotected, high-powered, always-on, broadband-connected personal computers does indeed represent a threat to the national infrastructure (note that we are both U.S. citizens, but this is by no means a uniquely American perspective — we would be holding the same truths to be self-evident if we were citizens of the United Kingdom, or Germany, or Brazil, or anywhere else that is experiencing a rapid increase in broadband connectivity).

We have had these thoughts, and said these things, for some time, but we feel compelled to reiterate them now, because our President has just signed the Homeland Security Bill, causing the biggest overhaul of the U.S. government since the National Security Act of 1947 unified the Armed Forces under a single department and created the National Security Council and Central Intelligence Agency. The Homeland Security Department is expected to have a combined workforce of more than 175,000 employees and pull together more than 20 agencies. As if that wasn't enough for one bill, the Homeland Security Act also amends a bunch of other laws and encompasses things like the creation of a new form of charitable trust to "provide for the spouses and dependents of military, CIA, FBI and other federal employees killed in the line of duty in the war on terrorism." A noble goal, but arguably extraneous to the creation a new department of government. We will have more to say about the Homeland Security Act in future columns, after we have more completely digested all 470 pages (okay, that's the double-spaced version, but still, this is not light reading).

What we want to highlight here is the starring role that computer security plays in this legislation. For a start, the bill includes a definition of information security and spells out that other C-I-A, the one that infosec people have been working at for years: Confidentiality, Integrity, and Availability. In a dramatic turn, the bill makes significant amendments to the Computer Fraud and Abuse Act of 1986. Indeed, these amendments are to be known as the "Cyber Security Enhancement Act of 2002." The "enhancements" include increased penalties for criminal hacking, up to life imprisonment "if the offender knowingly or recklessly causes or attempts to cause death" through conduct such as intentionally accessing a computer without authorization or exceeding authorized access.

What we don't see in the Homeland Security Bill, or in the $900 million appropriation for computer security research that was also passed last week, is funding for the education of network computer users and operators. These are the people, like you, and us, and generations just getting started, who are connecting their computers to the Internet. The connections are often high bandwidth (24 million Americans have broadband Internet connections at home according to Pew report this summer).

Whose job is it to tell the people who have these connections that their computer could unwittingly host a distributed denial of service attack? Who is responsible for telling computer owners to make sure they are not harboring programs that could bring down emergency service communications during a terrorist attack? When you get a Dell does it say on the box: "Dude, this thing could kill someone"? No, and we don't expect to see such a warning sticker any time soon. That is the point. With powerful technology comes a ton of responsibility. But it tends to arrive somewhat later than the technology itself.

In the meantime, securing all those computers on the network will take some serious motivation. Patriotism seems like a good place to start.

... Chey Cobb, the author of "Network Security for Dummies," is an independent consultant and former senior technical security advisor to the NRO and can be reached at chey@patriot.net. Stephen Cobb, the author of "Privacy for Business: Web Sites and Email," is Senior VP of Research and Education for ePrivacy Group and can be reached at scobb@cobb.com.

Category 16.3 *Infrastructure protection & homeland security*

2002-12-20 **national strategy cyberspace security homeland defense cyberterrorism infowar information warfare ISP Internet service providers privacy monitoring viruses infrastructure protection privacy**

NewsScan

PROPOSED NATIONAL STRATEGY TO SECURE CYBERSPACE

The President's Critical Infrastructure Protection Board is planning to propose that Internet service providers be required to help build a centralized monitoring system that could be used to protect network users from both computer viruses and terrorist attacks. The plan would be part of an Internet strategy for the new Department of Homeland Security. Some technology company executives say they fear that the system could be used to invade individual privacy but Tiffany Olson, chief of staff for the Board, says that the plan will not require gathering data that would allow monitoring at an individual user level. She says a centralized monitoring system is needed because, currently, "we don't have anybody that is able to look at the entire picture. When something is happening, we don't know it's happening until it's too late." (New York Times 20 Dec 2002)

GOVERNMENT VOWS TO RESPECT CITIZEN PRIVACY
Responding to concerns that the Internet monitoring center proposed by the government's forthcoming report "National Strategy to Secure Cyberspace," President Bush's top cyberspace adviser, Richard Clark, says that the plan contains nothing which "in any way suggests or proposes a government system that could extend to monitoring individuals' e-mails"; to the contrary, it "articulates a strong policy of protecting citizens' privacy in cyberspace." The Bush administration contemplates that any Internet monitoring operation would be run by the private sector and not the government. There is no proposal for monitoring e-mail or other data traffic of Internet users. (20 Dec 2002)

Category 16.3 *Infrastructure protection & homeland security*

2003-01-06 **Department Homeland Security IT key success federal agencies US government anti-terrorism**

NIPC/DHS

January 02, National Journal's Technology Daily — IT systems key to success of Department of Homeland Security.

Strong information technology systems will be crucial to the success of the new Department of Homeland Security, according to the General Accounting Office (GAO). The GAO report (03-260), released December 24, found that federal agencies have made progress in addressing their homeland security missions since the September 11, 2001, terrorist attacks, and that information sharing between federal agencies has increased. But GAO said federal agencies still face many challenges, such as improving their collaboration with state and local officials and with the private sector. Twenty-two existing federal agencies and offices will move into the new DHS, which also will include an Office of State and Local Coordination and a liaison official for the private sector. GAO estimated that the full transition to the new department could take five to 10 years, and recommended that the Office of Management and Budget (OMB) work with the department to implement the appropriate management systems. "Strong financial and information technology systems will also be critical to the success of [the DHS] and other organizations with homeland security missions."

Category 16.3 *Infrastructure protection & homeland security*

2003-01-07 **Department Homeland Security IT implementation worries security**

NIPC/DHS

January 06, Washington Post — Setting up IT infrastructure will help the Department of Homeland Security.

One of the challenges in creating a department from a hodgepodge of 22 federal agencies and 170,000 employees is the information technology headache. "It is not enough to shuffle redundant or overlapping programs under the new bureaucracy," Michael Scardaville, a policy analyst at the Heritage Foundation, wrote in a recent report. The department "should develop and deploy an information technology infrastructure that links and fuses intelligence and law enforcement terrorism databases." Representative of the agency's challenge will be monitoring the thousands of freighters that enter U.S. ports daily. The department wants a "smart border" program in which cargo ships heading for U.S. ports would electronically file information detailing the contents of cargo containers, crew members' names and nationalities, and what stops the ships are scheduled to make before reaching the United States. Steven I. Cooper, special assistant to the president on information technology's place in homeland security, admitted, it may be a lengthy process. "I think parts of it could probably be done fairly quickly, meaning within months instead of years," he said. "To fully put together something like that across the world is obviously going to take a longer period of time." In the meantime, short term priorities for the new department will include border and transportation security technology, such as equipment that identifies radioactivity and software that identifies non-obvious trends in databases or protects computer infrastructure from hackers.

Category 16.3 *Infrastructure protection & homeland security*

2003-01-08 **Department Homeland Security cyber terrorism combat secure cyberspace**

NIPC/DHS

January 07, Associated Press — Revised White House security initiative focuses on agencies.

An internal draft of the Bush administration's revised plan to improve cybersecurity, the National Strategy to Secure Cyberspace, is circulating among government offices and industry executives this week. In the new plan, the number of initiatives to tighten security for vital computer networks was reduced from 86 to 49. The plan no longer includes a number of voluntary proposals for America's corporations to improve security, focusing instead on suggestions for U.S. government agencies, such as a broad new study assessing risks. Among the draft's changes was the removal of an explicit recommendation for the White House to consult regularly with privacy advocates and other experts about how civil liberties might be affected by proposals to improve Internet security. The draft notes that the new Department of Homeland Security (DHS) will include a privacy officer to ensure that monitoring the Internet for attacks would balance privacy and civil liberties concerns. The draft proposes to use the DHS to launch some test attacks against civilian U.S. agencies and to improve the safety of automated systems that operate the nation's water, chemical and electrical networks. The new version also says the Defense Department can wage "cyber warfare" if the nation is attacked. It warns that although it can be difficult or even impossible to trace an attack's source, the government's response "need not be limited to criminal prosecution." The new version also puts new responsibilities on the CIA and FBI to disrupt other countries' use of computer tactics to collect intelligence on government agencies, companies and universities.

Category 16.3 *Infrastructure protection & homeland security*

2003-01-14 **war Iraq technology security battlefield PKI training biometric**

NIPC/DHS

January 13, Government Computer News — Possible war, terrorist threats shape Defense IT agenda.

The prospect of war with Iraq is defining the Defense Department's 2003 technology initiatives. U.S. soldiers on the front lines are preparing to use the latest technologies-including wireless communications and high-end cryptography tools-being tested and deployed by DOD, senior department officials said. In the coming months, DOD's technical focus will be squarely on security, boosting projects to develop antiterrorism tools, creating a DOD-wide public-key infrastructure (PKI), expanding IT training, and beginning biometric pilots.

Category 16.3 *Infrastructure protection & homeland security*

2003-02-03 **US infrastructure protection cyber terrorism threat security**

NIPC/DHS

February 02, New York Times — Departing security official highlights cyber threat.

Richard A. Clarke, the blunt, sometimes abrasive White House adviser who raised the alarm about unconventional national security threats ranging from failed states to biological and computer terrorism for more than a decade, quietly resigned as President Bush's special adviser for cyberspace security on Friday. In an interview after his last day in office, Clarke warned that although the government had made considerable progress in defending its electronic infrastructure from computer attacks, the United States faced ever greater peril, given its growing dependence on the Internet. "A sophisticated cyberattack may not result in massive deaths," he said. "But it could really hurt our economy and diminish our ability to respond to a crisis, especially if it is combined with a war, or a terrorist attack." Clarke said the attack last weekend by a computer bug known as the Sapphire worm showed the vulnerability of the United States' increasingly Internet-based economy. Though it was a relatively simple bug, he said, Sapphire, which has also been called Slammer, ravaged systems throughout the United States and overseas in just a few hours, shutting down some of the Bank of America's automated teller machines and Continental Airlines' online ticketing system, and denying access to the Internet to millions of personal computer owners. "Don't assume that the damage done by hackers in the past is predictive of the future," Clarke said. "As Sept. 11 showed, as long as our vulnerabilities are large, some enemy will exploit them in a new and hugely damaging way." Clarke said the nation is safer today than before Sept. 11 because al Qaeda's sanctuary in Afghanistan is gone and because Americans had rounded up hundreds of al Qaeda operatives abroad and tightened aviation security overseas and domestically. Clarke said he was leaving his post now because "11 years in the White House and a total of 30 in government is more than enough," and because President Bush would soon unveil a new national strategy to protect the nation's information infrastructure, which Clarke and his team had drafted.

Category 16.3 *Infrastructure protection & homeland security*

2003-02-18 **industry government plan secure cyber space anti-terrorism infrastructure**

NIPC/DHS

February 14, Government Computer News — Industry will work with government on cyberspace plan .

The White House unveiled its National Strategy to Secure Cyberspace on Friday. The plan's five priorities are: 1) A national cyberspace security response system; 2) A threat and vulnerability reduction program; 3) A security awareness and training program; 4) A plan to secure governments' cyberspace; 5) An approach to intelligence agency and international cybersecurity. The plan called for exercises to evaluate the impact of cyberattacks and pinpoint weaknesses for correction. The plan put the Justice Department and other agencies in charge of improving information sharing, investigative tools and cybercrime research. It said the General Services Administration and Department of Homeland Security will continue to cooperate on a federal software patch clearinghouse and work with the private sector on a similar clearinghouse. Federal agencies were told to tighten security measures, expand their use of security assessment tools and install applications to check continuously for unauthorized network connections. The plan said the government will also review the National Information Assurance Partnership to assess whether it is properly dealing with security flaws in commercial software. It further said the government will consider licensing or certifying private security service providers for minimum capabilities, "including the extent to which they are adequately independent." In the international arena, the plan noted that the U.S. government will not necessarily limit its response to cyberattacks to criminal prosecution and it "reserves the right to respond in an appropriate manner." That mirrors the government's pursuit of al-Quaida, which has been carried out partly by legal prosecution and partly by warfare. It called for building North America into a "cyber safe zone" with the cooperation of Canadian and Mexican public and private sectors.

Category 16.3 *Infrastructure protection & homeland security*

2003-02-18 **cyberattack homeland defense infowar information warfare government policy**

NewsScan

WHITE HOUSE OUTLINES NEW INTERNET SECURITY STRATEGY
The White House has released a new Internet security strategy focused largely on voluntary efforts by institutions in the private sector and by individual Americans. The plan suggests, without mandating, numerous steps that government agencies should take to set the example for good security procedures, and specifies that the five major priorities for action are: setting up a security response system; identifying threats and vulnerabilities; increasing awareness and training; securing critical government sites; and fostering cooperation nationwide and abroad. Acting chief White House security czar Howard Schmidt says, "This is a good start. It's a very practical and pragmatic plan and it gives us the capability to move forward in the confines of the current budget situation. There's never enough money in security, but this gives us the ability to have a dialogue with industry and set goals." (San Jose Mercury News 15 Feb 2003)

Category 16.3 *Infrastructure protection & homeland security*

2003-02-20 **cyber terrorism threat steps action States critical infrastructure protection**

NIPC/DHS

February 19, Government Computer News — States take first step toward cyberthreat sharing.

Last weekend thirteen states conducted a communications exercise that could lead to a new, multistate information sharing and analysis center (ISAC). The ISAC, which would pool cyberthreat data gathered by states, is led by William Pelgrin, director of the New York City Office of Cyber Security and Critical Infrastructure. No formal center exists yet, however. During the dry run, participating states reported to a central location any suspicious activities they monitored on the Internet over the Presidents Day weekend. "There was no malicious activity," said Mike Russo, chief information security officer in Florida's state technology office. "The exercise was about the communications and working relationships with the other states." Because sharing information about security threats and vulnerabilities is seen as essential to protect the nation's critical infrastructures, the federal government has encouraged the creation of ISACs to share information in commercial sectors such as banking, public utilities and IT. It also encourages information sharing with federal agencies. The ISACs serve as central collection points where data can be gathered and evaluated. Most such information is sanitized before distribution because of participating organizations' liability concerns.

Category 16.3 *Infrastructure protection & homeland security*

2003-02-25 **National Infrastructure Protection Center NIPC Indiana University cooperate cyber infrastructure protection security**

NIPC/DHS

February 25, National Infrastructure Protection Center — NIPC and Indiana University agree on cooperative cyber infrastructure security efforts.

In an effort to support and enhance the security and readiness of the cyber infrastructure, the National Infrastructure Protection Center (NIPC) has signed an agreement with Indiana University, operator of the Research and Education Network Information Sharing and Analysis Center (REN-ISAC). Indiana University, via the REN-ISAC, will ensure that research and education network operators receive the most current counter-terrorist threat alerts, warnings and analysis. In turn, the network operators and participating universities and research centers will be encouraged to work through the NIPC to voluntarily pass incident information. Incident information will include not only specific incidents immediately threatening participating networks, but trend information that may indicate an organized attack is in preparation or underway. "The Nation's research and education networks carry not only information critical to research but critical commercial and financial information as well. That is why information sharing between the federal government and network operators is vital in the war against terrorism," said Admiral James Plehal, Acting Director of the NIPC. "Advance knowledge of the type and nature of attacks can make a vital difference in their readiness to prevent, and mitigate the consequences of an attack," he said. Indiana University is home to a Global Network Operations Center (Global NOC) which manages several national and international high-speed networks and network links. The NIPC will transition into the Department of Homeland Security on March 1st.

Category 16.3 *Infrastructure protection & homeland security*

2003-02-28 **Department Homeland Security DHS technology barrier divide education**

NIPC/DHS

February 26, Federal Computer Week — Info sharing hobbled by lack of technology.

Agencies merging into the Homeland Security Department as well as others sharing information in the government's antiterrorism efforts are working to overcome technological barriers, but the work is going to take time, according to a panel of agency officials who spoke February 26 at an AFCEA International Inc. conference in Washington, D.C. One challenge is ensuring that information stays out of the hands of those not authorized to see it. To that end, the National Security Agency (NSA) is developing "trusted control interfaces," which the CIA is implementing, said William Dawson, chief information officer of the CIA's Department of Intelligence Communications. The interfaces' intent is to strip classified information from messages before passing them to someone of a lower security class. An early stage of the system is running at the CIA, but most of the capabilities won't be ready until September, Dawson said.

Category 16.3 *Infrastructure protection & homeland security*

2003-03-06 **Congress cyber security threat terrorism panel infrastructure civilian protection**

NIPC/DHS

March 04, News.com — Congress sets up cybersecurity panel.

The U.S. Congress on Tuesday established its first panel devoted to cybersecurity. In its first meeting, the new House Homeland Security Committee voted to create a subcommittee that will oversee the federal government's "cybersecurity, science, and research and development" efforts relating to homeland security. The office of chairman Chris Cox (R-CA) said the cybersecurity subcommittee will be in charge of the "protection of government and private networks and computer systems from domestic and foreign attack (and) prevention of injury to civilian populations and physical infrastructure caused by cyberattack." The Senate does not have a parallel effort, though its subcommittee on technology, terrorism and government information shares similar duties.

Category 16.3 *Infrastructure protection & homeland security*

2003-03-11 **Internet violence Islamic fundamentalism connection**

NIPC/DHS

March 02, Time Magazine — Investigators examine the links between Islamic fundamentalists and the Internet.

On February 26, Sami Omar al-Hussayen, a Ph.D. Candidate in computer security at the University of Idaho, was charged with violating conditions of his student visa by registering and maintaining a dozen militant websites promoting violence against U.S. interests. U.S. officials want to know more about al-Hussayen's work for the sponsor of most of these sites, the radical Islamic Assembly of North America (IANA), a Michigan-based group known as one of the most strident voices of Islam on the Web. IANA hosted the websites of two radical Saudi sheiks - Salman al-Awdah and Safar al-Hawali - both of whom are closely associated with Osama bin Laden and who provided religious justification for the September 11 attacks, according to the SITE Institute, a Washington-based terrorist-research group that monitors the Internet. Al-Hussayen's case also may provide fresh evidence that at least some of these anti-American websites are being supported by funds coming from Saudi Arabia. Al-Hussayen is accused of covertly receiving $300,000 from abroad and disbursing much of it to IANA. A Saudi-embassy spokesman in Washington said no government money has gone to IANA.

Category 16.3 *Infrastructure protection & homeland security*

2003-03-12 **US federal government secure Internet net DHS**

NIPC/DHS

March 10, eWEEK — Federal government moves to secure net.

The White House and the new Department of Homeland Security have begun in earnest the process of implementing the plan to secure the nation's critical networks. The most significant move is the development of a private, compartmentalized network that will be used by federal agencies and private-sector experts to share information during large-scale security events, government officials said at the National Information Assurance Leadership conference in Washington D.C. last week. The system is part of the newly created Cyber Warning Information Network (CWIN), a group of organizations including the National Infrastructure Protection Center, the Critical Infrastructure Assurance Office and others that have some responsibility for the security of federal systems. The private-sector Information Sharing and Analysis Centers will also be included. The CWIN, a key part of the Bush administration's National Strategy to Secure Cyberspace, will use a secure, private IP network separate from the public Internet, according to officials. As part of the plan to improve security, the CIO of each federal agency is, by statute, now accountable for the security of that agency's network.

Category 16.3 *Infrastructure protection & homeland security*

2003-03-17 **DHS infrastructure protection evaluation anti-terrorism**

NIPC/DHS

March 13, Federal Computer Week — Homeland CIO outlines priorities.

Steve Cooper, the CIO of the new Department of Homeland Security (DHS), told an industry gathering that it is essential to move quickly to build DHS' infrastructure because "state-sponsored terrorists and al Qaeda are not going to wait until we have our act together." He said he and his information technology team will complete an inventory of IT assets brought together by the merger of 22 federal agencies. It will be evaluated for "reuse, renewal, retirement or enhancement," and he expects to decide what systems to keep and what to retire by August. In the next six weeks, DHS will issue a series of requests for information about wireless and geospatial technology to help officials decide how to create the best systems.

Category 16.3 *Infrastructure protection & homeland security*

2003-03-24 **Department Homeland Security DHS security focus infrastructure protection**

NIPC/DHS

Ridge: Cybersecurity at 'heart' of department's work.

Department of Homeland Security (DHS) Secretary Tom Ridge said on Thursday that his department will work as hard to address threats to the Internet as it does to address physical threats. "We will not distinguish between physical and cyber in this new unit," Ridge told the House Homeland Security Appropriations Subcommittee in a hearing on the fiscal 2004 budget. Ridge said that he understands a cyber attack could affect every aspect of the U.S. economy and government and that preventing such an attack is "at the very heart" of his department's duties. He also said that since last month, the department has been "actively engaged" in talks about the nation's cyber infrastructure with the private sector and other groups "because they have their own list of what the vulnerabilities are." Much rests on the vulnerability assessments being done on critical infrastructures, he said. Ridge said the department's chief information officer is developing plans for a technology framework that would enable Homeland Security to share information both within and outside the department. A strategic plan to let the department's various agencies access terrorist watch lists also is being prepared, he said.

Category 16.3 *Infrastructure protection & homeland security*

2003-03-24 **security built up telecom companies East coast US anti-terrorism FCC**

NIPC/DHS

March 24, Washington Post — Telecom firms rebuild, beef up security.

Since the terrorist attacks in New York and at the Pentagon crippled communications networks along the East Coast, telecommunications companies have invested heavily to fortify their facilities. All over the country, telecommunications companies have added fiber-optic lines, increased their ability to reroute traffic and beefed up their security in response to lessons learned in the September 2001 attacks. Jeffrey M. Goldthorp, chief of network technology at the Federal Communications Commission, has been working with the nation's leading telecommunications companies for the past year. He was reluctant to discuss specifics but did point to one unnamed company that he said recently moved a huge database to a hardened underground shelter. The database will be a key resource in case the network, or any section of it, needs to be rebuilt. The FCC also recently orchestrated a series of "mutual aid" contracts between companies that allow them to work together immediately after a disaster without having to negotiate costs or other legal issues.

Category 16.3 *Infrastructure protection & homeland security*

2003-03-25 **cyber security anti-terrorism infrastructure protection**

NIPC/DHS

March 21, Government Computer News — Leadership selected for new cybersecurity panel.

Leaders have been named for the new House Homeland Security subcommittee on Cybersecurity, Science and Research and Development. Rep. Mac Thornberry (R-TX) will chair the subcommittee and the ranking minority member is Rep. Zoe Lofgren (D-CA). The Homeland Security Committee was formed to coordinate all House oversight of the Department of Homeland Security and has legislative jurisdiction over the 2002 act creating the department. The subcommittee will oversee "security of computer, telecommunications, information technology, industrial control, electric infrastructure and data systems, including science, research and development; protection of government and private networks and computer systems from domestic and foreign attack; prevention of injury and civilian populations and physical infrastructure caused by cyberattack, and relevant oversight," according to Cox's office.

Category 16.3 *Infrastructure protection & homeland security*

2003-04-04 **Department Homeland Security DHS Internet infrastructure design critical system**

NIPC/DHS

April 01, National Journal — DHS may oversee Internet infrastructure.

The Bush administration's acting cybersecurity adviser Howard Schmidt said Tuesday that homeland security and government agencies officials are working to formalize a security apparatus for the global Internet root servers, a series of computer systems that underpin the Internet's address system. After an attack on those servers and the Internet domain-name system last October, Schmidt, several agencies officials, computer-security experts and root-server operators discussed in January how they could better respond to such incidents. Their talks identified the need to develop a framework for determining when individuals and companies that operate the Internet's mission-critical domain system should report an attack or disturbance to government officials.

Category 16.3 *Infrastructure protection & homeland security*

2003-04-04 **NIST national infrastructure protection IAIP Homeland Security DHS secure cyberpsace**

NIPC/DHS

April 02, Federal Computer Week — NIST security division expands role.

The National Institute of Standards and Technology's (NIST) Computer Security Division will be playing a significant role in the Bush administration's cybersecurity strategy, according to Howard Schmidt, acting chairman of the President's Cybersecurity Board. The NIST division did not move to the new Information Analysis and Infrastructure Protection (IAIP) Directorate at the Department of Homeland Security (DHS), as originally set out in the White House's plan. Discussions are under way to determine how the organization can and will contribute to the implementation of the National Strategy to Secure Cyberspace, Schmidt said. Schmidt also is working with the recently appointed IAIP directorate leaders to make sure that all of the work being done by the President's Critical Infrastructure Protection Board — dissolved in a February executive order — is carried over into DHS.

Category 16.3 *Infrastructure protection & homeland security*

2003-04-17 **cyber attack terrorism cyberspace action war Iraq**

NIPC/DHS

April 15, Reuters — More talk, little action in war on cyber terrorism.

At a time when war in Iraq has heightened fears of terrorism, the technology industry is not moving quickly enough to guard against intrusions from hackers, identity thieves and more concerted attacks by rogue governments, computer experts said Tuesday at the RSA conference in San Francisco. Howard Schmidt, the White House cyber security adviser who is working with the technology industry to improve security, said that work to date had been strong on new ideas to improve security, but slow to execute. Despite repeated warnings of rogue nations preparing for cyber-attacks that could cripple vital computer-run U.S. infrastructure, no such attacks are known to have occurred to date. If computer systems have so far been spared a massive terrorist attack, smaller security breaches from hackers and pranksters with no political agenda occur on a daily basis. The Computer Emergency Response Team (CERT) tracked some 52,658 online security "incidents" in 2001, more than double the 21,756 reported in 2000, and way up from 9,859 in 1999. Members of the high-tech advocacy group TechNet said that while the threat of a political-based cyber terrorist attack may have been overstated, random pranksters had the ability to do much damage.

Category 16.3 *Infrastructure protection & homeland security*

2003-04-21 **US President IT security adviser resign critical infrastructure protection**

NIPC/DHS

April 18, Washington Post — President's top IT security adviser to resign.

White House cybersecurity adviser Howard Schmidt will resign from his post at the end of the month. The former chief of security at Microsoft Corp., Schmidt became chair of the President's Critical Infrastructure Protection Board in February following the departure of his predecessor, Richard Clarke. Schmidt played a key role in drafting the administration's recently released cybersecurity strategy, and has spent the last two years building ties with the private sector in a joint effort to protect the nation's most important information systems from cyber-attack. Schmidt's imminent departure would leave the administration without a high-ranking official solely in charge of cybersecurity. In January, the administration consolidated the work of five federal cybersecurity offices into the Department of Homeland Security (DHS). Full responsibility for cybersecurity matters currently rests with Robert Liscouski, a former Coca-Cola executive who was recently named assistant secretary of infrastructure protection at the DHS.

Category 16.3 *Infrastructure protection & homeland security*

2003-04-24 **Department Homeland Security cyberwar game simulation anti-terrorism**

NIPC/DHS

April 23, Government Computer News — DHS gets into the cyberwar game.

The Department of Homeland Security (DHS) is simulating cyberattacks and biological assaults to help prepare for the possibility of the real thing, deputy secretary Gordon England said. "A week ago, I participated in a war game with the Business Roundtable," England told attendees at the U.S. Chamber of Commerce's Conference on Critical Infrastructure and Homeland Security today. The Business Roundtable is an association of corporate chief executive officers that makes policy recommendations for economic growth. Part of the war game involved a cyberattack on financial institutions "that sucked money out of the financial system," England said. England endorsed the Business Roundtable's approach of periodically reviewing its members' plans for recovery from attacks and urged the Chamber of Commerce to adopt similar plans. In response to a question about the department's approach to regulation, England said, "I would like the DHS to have as few regulations as possible-our job is to coordinate the work of other federal agencies."

Category 16.3 *Infrastructure protection & homeland security*

2003-04-25 **cyber space cyberterrorism anti-terrorism threat networkks**

NIPC/DHS

April 24, New York Times — Defending the cyber realm.

Security experts have warned that cyberterrorism presents a great potential threat to the U.S., with its increasing dependence on computer networks for everything from weapons systems to hydroelectric dams to commerce. However, security technology developer Symantec says it has yet to record a single cyberterrorist attack — by its definition, one originating in a country on the State Department's terror watch list. That could be because those inclined to commit terrorist acts do not yet have the know-how to do significant damage, or perhaps because hackers and adept virus writers are not motivated to disrupt networks for a cause. But should the two groups find common ground, the result could be devastating, said Michael A. Vatis, head of the Institute for Security Technology Studies at Dartmouth College.

Category 16.3 *Infrastructure protection & homeland security*

2003-04-29 **threat cyber terrorism Internet infrastructure protection**

NIPC/DHS

April 25, London Free Press — Cyber attacks a concern?

The FBI calls cyber-terrorism a "premeditated, politically motivated attack against information, computer systems, computer programs and data which results in violence against non-combatant targets by subnational groups or clandestine agents." Some fear cyber-terrorists could shut down the Internet or substantially interfere with the use of oil, gas, power grids, telecommunications and emergency services. Others, however, say these fears are overstated as many critical systems are based on secured networks not accessible through the Internet. Terrorists and computer hackers can be a dangerous combination. There are reports that after investigations regarding several hijackings, authorities were led to believe terrorists had gained access to the architectural schematics of the planes through cyber-crime.

Category 16.3 *Infrastructure protection & homeland security*

2003-04-30 **Korea Information Communication Ministry Internet attack SQL slammer**

NIPC/DHS

April 28, The Korea Herald — Korea's MIC takes measures to prevent online attacks.

The massive Internet shutdown caused by the SQL Slammer computer virus on January 25 caused chaos for Korea's 10 million high-speed Internet users. Now, Korea's Ministry of Information and Communication (MIC) has announced that it will take an active role in promoting security countermeasures aimed at creating fast and accurate communication routes where fixing and preventing network attacks will take only a matter of minutes. The MIC plans to create an information security base, develop information security related technology and standardization, and train manpower in the sector. It will build a support center dealing with attacks and security breaches on the Internet that will run 24 hours per day. MIC is also working on introducing rights to request information and investigate the scene of the crime. Other preventative measures involve working and communicating with multiple online businesses and service providers to make sure that each complies with standards in prevention.

Category 16.3 *Infrastructure protection & homeland security*

2003-05-01 **Lucent Technologies U.S. Security Bush National Security Telecommunications Advisory Committee NSTAC Russo**

NIPC/DHS

May 01, CNET News.com — Lucent CEO tapped for U.S. security.

President Bush has enlisted Lucent Technologies' chief executive Patricia Russo as a member of the National Security Telecommunications Advisory Committee (NSTAC). The NSTAC, created in 1982 by President Reagan, provides analysis and recommendations to the president regarding policy that affects national security and emergency preparedness tied to telecommunications. The terrorist attacks on New York City and Washington D.C. on September 11, 2001, exposed the susceptibility of the nation's telecommunications networks, which suffered widespread outages. In the aftermath, the NSTAC's importance swelled in its role to make the telecommunications infrastructure more secure. Russo will be involved with a wide range of policy and technical issues related to telecommunications, infrastructure protection and homeland security.

Category 16.3 *Infrastructure protection & homeland security*

2003-05-05 **DHS Topoff2 warfare computer terrorist Ted Macklin emergency operations Dartmouth College Institute Security**

NIPC/DHS

May 05, Government Computer News — Terror attack mock-up has a cyber angle.

The Department of Homeland Security (DHS) and dozens of federal, state and local agencies will launch a simulated five-day terrorist attack on May 12 designed to include a small role for cyberwarfare, officials said Monday. The attack game, called Topoff 2, will include a small element of computer warfare, said Ted Macklin, assistant director of the Office of Domestic Preparedness (ODP). It will not focus on an emergency operations center takedown but on the ability of state and local authorities to recognize a cyberattack, he said. Seattle Mayor Greg Nickles said that participants will begin with the assumption that their computers will work, but "that could be an area they surprise us with." An ODP official who is working on Topoff 2 said DHS has contracted with Dartmouth College's Institute of Security and Technology studies to prepare a "sand table" analysis of a cyberattack, in coordination with Seattle.

Category 16.3 *Infrastructure protection & homeland security*

2003-05-09 **PITAC cybersecurity Bush President's Information Technology Advisory Committee IT homeland security**

NIPC/DHS

May 09, Federal Computer Week — PITAC nominees strong in cybersecurity.

President Bush announced May 8 that he plans to appoint 25 new members to the President's Information Technology Advisory Committee (PITAC), which offers advice on maintaining America's dominance in advanced information technologies. The panel provides information to the president, Congress and federal agencies involved in IT research and development, and helps guide the Bush administration's efforts to accelerate the development and adoption of IT policies for the nation. Its members are leading IT experts from industry and academia, many of whom have worked in or with the government. "These appointments come at a critical time for our economic security and our homeland security, particularly in the area of cybersecurity," said House Science Committee Chairman Sherwood Boehlert (R-NY).

Category 16.3 *Infrastructure protection & homeland security*

2003-05-12 **IT security Bush administration information technology OMB white house**

NIPC/DHS

May 12, National Journal — Report to recognize agencies' progress toward IT security.

President Bush's administration is readying a report that will recognize several government agencies for making tangible progress in their efforts to meet security goals for information technology, according to administration officials. The White House Office of Management and Budget (OMB) is preparing to send Congress an annual report highlighting the status of those IT initiatives, OMB analysts told members of a National Institute of Standards and Technology advisory board last Wednesday. The report will be the last IT security review by OMB before it updates its guidelines and agency reporting requirements under new IT rules created under a recent e-government law.

Category 16.3 *Infrastructure protection & homeland security*

2003-05-14 **cyber attack critical computer systems terrorism critical infrastructure**

NIPC/DHS

May 14, Silicon Valley — U.S. Still vulnerable to cyber attack.

The United States remains ill-prepared to defend against a strike on the nation's critical computer systems because of slow-moving federal research efforts, members of Congress said Wednesday. "The nation quite simply has been under-investing woefully in cyber security R&D," said Rep. Sherwood Boehlert (R-NY), chair of the House Science Committee, which brought the heads of the four agencies to Capitol Hill to testify about their efforts. The heads of the four lead agencies for cyber-security research — the directors of the science foundation, DARPA, and the National Institute of Standards and Technology, and the undersecretary for science and technology at the Department of Homeland Security — said they were making progress and beginning to work collaboratively on projects. Terrorism experts fear attacks on computer systems that operate electricity grids, phone systems or other critical infrastructure as part of a terrorist strike.

Category 16.3 *Infrastructure protection & homeland security*

2003-05-15 **cybersecurity DHS Department Homeland Security cyberspace certification research**

NIPC/DHS

May 15, Federal Computer Week — DHS setting cybersecurity priorities.

Now that responsibility for the National Strategy to Secure Cyberspace has shifted to the Department of Homeland Security (DHS), officials are developing a list of priorities for implementation within the next 180 days. Among the areas being examined are education and certification, metrics and benchmarks for the private sector, and research and development, said Andy Purdy, cybersecurity adviser for the Information Analysis and Infrastructure Protection (IAIP) Directorate at DHS. Purdy was speaking May 14 at a symposium sponsored by the Computing Technology Industry Association in Washington, D.C. DHS officials also are looking at a more comprehensive method to share security vulnerability and incident information between government and the private sector, Purdy said.

Category 16.3 *Infrastructure protection & homeland security*

2003-05-16 **Netanyahu Woolsey terror technology CIA IDPartners conference U.S.**

NIPC/DHS

May 16, Computerworld — Netanyahu and Woolsey speak out on terror and technology.

This week former Israeli Prime Minister Benjamin Netanyahu and former CIA director R. James Woolsey warned of the dangers of inaction and lack of preparedness when it comes to cyberterrorism and homeland security. "The power of the few to terrorize the many has grown by leaps and bounds...because of technology," Netanyahu said during an interview broadcast Tuesday as part of the Terror and Technology Online conference, sponsored by IDPartners LLC. He was referring to the ability of international terrorist organizations to physically destroy key cyber-based infrastructures or attack those infrastructures using the Internet. When asked what can be done to meet the threat, Netanyahu said, "through security systems and security norms that are enforced by governments." Woolsey said the networks and systems that power the U.S. economy "were put together by businesspeople...with an eye toward openness and ease of access, and were not put together with a single thought in most cases...to terrorism."

Category 16.3 *Infrastructure protection & homeland security*

2003-05-26 **critical infrastructure lawmakers cyber terror vulnerability government agencies Richard Clarke regulations police**

NIPC/DHS

May 26, The Hill — Lawmakers see cyberterror vulnerability.

Lawmakers are charging that government agencies and industry are not doing enough to protect the country's power plants, industries and financial institutions from the threat of cyberterrorism attacks. Science committee staffers have noted that 80 to 90 percent of the country's infrastructure is under private control. Staffers for the House Government Reform Technology Subcommittee are making site visits to private sector companies to assess its state of preparedness. At a subcommittee hearing in April, former White House advisor on cyber security Richard Clarke said, "I think we want to avoid regulation" and a "cyber security police." But a few weeks later, members of the National Infrastructure Advisory Committee, a White House advisory group. concluded that regulation might be the best way to get some industries to implement better cyber security, as well as physical infrastructure security. An alternative to government regulation is self-regulation through regional Information Sharing and Analysis Centers. But the threat of having competitors aware of a company's vulnerabilities has made this problematic for many organizations.

Category 16.3 *Infrastructure protection & homeland security*

2003-05-27 **homeland security webcam ordinary american monitoring from home 10$ hour**

NewsScan

HOMELAND SECURITY VIA WEBCAM

Jay Walker, who made his fortune by inventing Priceline.com, is working on a new brainstorm that addresses the timely issue of homeland security. The premise behind USHomeGuard is simple: use webcams at the 47,000 "critical infrastructure facilities" that are at risk, enabling ordinary, online Americans to help monitor the sites from their homes. If a person spots a potential terrorist — a hooded man trying to scale a power plant fence, for instance, or a panel truck parked next to a reservoir — on-site security could be alerted with the click of a mouse. Walker suggests that work-at-home monitors could be reimbursed at up to $10 an hour, paid by the government agencies and companies that need the service. "We like to think of USHomeGuard as a digital victory garden," says Walker. "It lets people be part of the solution." A spokesman for the Department of Homeland Security says federal officials have not done any "serious evaluation" of the proposal, adding that the agency isn't currently contemplating any strategies that rely on Internet surveillance. Meanwhile, law enforcement officials worry that such a system would generate too many false alarms. "People get suspicious easily, and this could quadruple our call volume," says Capt. Joe Carrillo of the San Jose Fire Department. "The idea is really good. But the timing is really bad," he added, alluding to California's current budget crisis. (AP/CNN.com 27 May 2003)

Category 16.3 *Infrastructure protection & homeland security*

2003-06-20 **democracy USAPATRIOT Act constitutional rights executive privilege homeland security counterterrorism**

NewsScan

WORTH THINKING ABOUT: HOW TO FORM A DEMOCRACY

Historian Bernard Bailyn comments on the creativity of America's Founding Fathers as shapers of the new democracy:
"The Founders of the American nation were one of the most creative groups in modern history. Some among them, especially in recent years, have been condemned for their failures and weaknesses — for their racism, sexism, compromises, and violations of principle. And indeed moral judgments are as necessary in assessing the lives of these people as of any others. But we are privileged to know and to benefit from the outcome of their efforts, which they could only hopefully imagine, and ignore their main concern: which was the possibility, indeed the probability, that their creative enterprise — not to recast the social order but to transform the political system — would fail: would collapse into chaos or autocracy. Again and again they were warned of the folly of defying the received traditions, the sheer unlikelihood that they, obscure people on the outer borderlands of European civilization, knew better than the established authorities that ruled them; that they could successfully create something freer, ultimately more enduring than what was then known in the centers of metropolitan life.
"Since we inherit and build on their achievements, we now know what the established world of the eighteenth century flatly denied but which they broke through convention to propose — that absolute power need not be indivisible but can be shared among states within a state and among branches of government, and that the sharing of power and the balancing of forces can create not anarchy but freedom.
"We know for certain what they could only experimentally and prayerfully propose — that formal, written constitutions, upheld by judicial bodies, can effectively constrain the tyrannies of both executive force and populist majorities.
"We know, because they had the imagination to perceive it, that there is a sense, mysterious as it may be, in which human rights can be seen to exist independent of privileges, gifts, and donations of the powerful, and that these rights can somehow be defined and protected by the force of law.
"We casually assume, because they were somehow able to imagine, that the exercise of power is no natural birthright but must be a gift of those who are subject to it."

Category 16.3 *Infrastructure protection & homeland security*

2003-07-15 **terrorism awareness infrastructure protection Senate education funding withheld**

NewsScan

SENATE PUTS THE SQUEEZE ON TIA FUNDING
U.S. senators deliberating over next year's defense budget have proposed eliminating all funding the Defense Department's Terrorism Information Awareness project. The TIA project, under the supervision of retired Adm. John Poindexter, seeks to develop computer software capable of scanning vast public and private databases of commercial transactions and personal data around the world to ferret out possible terrorist activities. The committee's proposal "reflects deep, deep skepticism in Congress of the Pentagon's assurances about this system," says a spokesman for the Center for Democracy and Technology. "There appears to be some spillover skepticism from Iraq where they voted to go to war and now are questioning whether that was based on clever use of words or selective use of intelligence." (AP 15 Jul 2003)

Category 16.3 *Infrastructure protection & homeland security*

2003-07-18 **surveillance privacy airplace security terrorism cameras**

NewsScan

SKY-HIGH SURVEILLANCE HITS AIRLINE INDUSTRY

Southeast Airlines is pioneering an in-flight surveillance program that will use digital videocameras installed through the cabins of its planes to record passengers' activities throughout the flight as a precaution against terrorism and other threats. The charter airline, based in Largo, Fla., says it may use face recognition software to match faces to names and personal records, and plans to store the digital data for up to 10 years. "From a security standpoint, this provides a great advantage to assure that there is a safe environment at all times," says Southeast's VP of planning. The airline says that while such security measures are not required by the FAA, it expects other airlines will adopt similar systems soon. That prediction alarms privacy advocates who especially question the need for retaining the video after the flight is over. "What's the point of keeping track of everyone when nothing happens on the flight?" asks Lee Tien, senior staff attorney for the Electronic Frontier Foundation, who points out that the video system could record conversations between passengers as well as capture the titles of passengers' reading material. (Wired.com 18 Jul 2003)

Category 16.3 *Infrastructure protection & homeland security*

2003-07-23 **cyberthreat warning Homeland Security council WMD information security protections John Gordon critical infrastructure**

NIPC/DHS

July 23, Federal Computer Week — Security adviser warns of cyberthreats.

Officials must still figure out how to fully secure the nation's critical infrastructure against cyber attacks, said General John Gordon, retired lieutenant general from the U.S. Air Force, presidential assistant and adviser to the Homeland Security Council Tuesday, July 22. Attacks over electronic networks might become a threat as great as weapons of mass destruction, he told a meeting of the National Infrastructure Advisory Council in Washington, DC. The council, which consists of a gathering of industry and government officials, is expected to issue recommendations for tougher information security protections in October. One of the council's toughest challenges is determining what should be disclosed to private industry and the public and when it should do so, officials told the council.

Category 16.3 *Infrastructure protection & homeland security*

2003-07-23 **digital control systems traditional computer networls physical infrastructure LAN WAN remote administration vulnerability risk assesment**

NIPC/DHS

July 23, Government Computer News — NDU prof: digital control systems can weaken security.

The growing integration of digital control systems with traditional computer networks is opening a new avenue of attack against the nation's physical infrastructure, John H. Saunders, a professor at the National Defense University, said Wednesday, July 23, at the GOVSEC security conference in Washington. Controls for operating utilities, buildings and campuses are being turned over to cost-effective digital systems with remote access capabilities. Proprietary protocols and single-purpose firmware have offered a degree of security for these systems. But standardizing on a few protocols is increasing the risk. Digital control systems also are being connected to LANs, WANs and the Internet for remote administration. Government administrators can do little about the level of security at utilities, but they can increase security within their own buildings, Saunders said. Building engineers need to focus on security the way systems administrators do, by performing systems inventories and vulnerability and risk assessments, and by implementing policy, he said.

Category 16.3 *Infrastructure protection & homeland security*

2003-07-26 **terrorism Ciso funding grants Treasury Department**

NewsScan

THE SECOND-ORDER COSTS OF TERRORISM
Cisco and other high-tech companies are faced now with the problem of monitoring charitable contributions made on behalf of their employees, to make sure the money isn't being sent to terrorist organizations. Taylor Griffin of the U.S. Treasury Department says: "It's the reality of a post-Sept. 11th world. Glossy brochures say they are funding orphans and people in need. But money is actually going to fund suicide bombings that kill innocents." But Janne Gallagher of the Council on Foundations complains that "adding a lot of other questions to due diligence increases the cost of making each grant," and Brian Lehnen of the Village Enerprise Fund, which has provided more than 100,000 small grants and loans to East African business startups, asks hypothetically: "Let's say one of them decides to be a terrorist... Suddenly, we support terrorism. It's on the minds of foundations and other deep-pocket organizations that fund groups overseas and don't know what they are liable for." (San Jose Mercury News 26 Jul 2003)

Category 16.3 *Infrastructure protection & homeland security*

2003-07-31 **Homeland Security Windows PC buffer overflow exploit vulnerability tool**

NewsScan

GOVERNMENT SOUNDS THE ALARM ON HACK ATTACKS
The U.S. Department of Homeland Security warns that in recent days computer hackers have successfully tested new tools that exploit a vulnerability known as "buffer overflows" in order to gain control of Windows PCs via the Internet. The vulnerability was discovered by Polish researchers who call themselves the "Last State of Delirium Research Group" and Microsoft has posted a patch on its Web site that individual PC owners can install to safeguard their machines. Experts warn that the attack tools, once perfected, could be used to disrupt Internet traffic by clogging data networks, or could allow crackers to delete or steal sensitive files. However, a senior security manager at Symantec says hackers haven't yet worked out all the glitches in these tools. "It is a little early. The exploit needs to be perfected. The effort applied to the exploit is certainly increased, but we're not sure if that's indicative of when we might see a widespread threat. People certainly need to be aware of this." Meanwhile, Internet Security Systems, which operates an early warning network for the technology industry, has raised its alert level to the second notch, indicating "increased vigilance" is warranted. "Everybody is predicting a widespread event, going from zero to 60 very quickly," says Internet Security Systems engineering director Dan Ingevaldson, who rates the probability of a major attack as "closer to imminent than probable." (AP/CNN.com 31 Jul 2003)

Category 16.3 *Infrastructure protection & homeland security*

2003-08-25 **virus network Sobig organized crime fraud**

NewsScan

ORGANIZED CRIME BEHIND SOBIG MESS?
Antivirus specialist Peter Simpson warns that the Sobig.F virus is the latest in a series of attempts on the part of organized crime to shift some of their illicit activities online. "Sobig smashed all the records in terms of pure numbers, but that's not nearly the whole story. This is the sixth in a series of controlled experiments. This isn't about some kiddy writing viruses in his bedroom — this is really a very sophisticated example of organized crime," says Simpson, a manager at Clearswift's ThreatLab. Simpson explained that the purpose of a virus such as Sobig isn't to cause damage, but to gain control of the machine in order to access information such as financial details for the purpose of fraud. It also comes in handy for disguising the source of spam by hijacking the victim's machine and identity. "The real question here has to be about the motives of the virus writer. This isn't just about writing a virus that will spread rapidly and break records; the motives here are very different and are clearly criminal. It's all about the hidden agenda." (ZDNet/Silicon.com 25 Aug 2003)

Category 16.3 *Infrastructure protection & homeland security*

2003-09-15 **homeland security cybersecurity incident response awareness federal agency strategy**

http://www.fcw.com/fcw/articles/2003/0915/web-cyber-09-15-03.asp

YORAN TO LEAD U.S. CYBER SECURITY
The Department of Homeland Security has announced that Amit Yoran will head the recently created National Cyber Security Division. Yoran currently serves as vice president of managed security services at Symantec Corp. The National Cyber Security Division comprises the Federal Computer Incident Response Center, the National Infrastructure Protection Center, and the Critical Infrastructure Assurance Office. It is responsible for awareness of and preparation for cybersecurity, including coordinating warnings and responses to cyber threats. The division, which was created in June, has been working on such issues since its inception. A spokesperson from the division said that having someone in charge will allow the division to pursue projects included in the National Strategy to Secure Cyberspace. [Federal Computer Week, 15 September 2003]

Category 16.3 *Infrastructure protection & homeland security*

2003-09-23 **MTA security systems computer hackers New York Metropolitan Transportation Authority firewalls website Intrusion Detection System IDS computer employees encryption software**

NIPC/DHS

September 23, Associated Press — MTA upgrading its security system against computer hackers.

The New York Metropolitan Transportation Authority said it would strengthen its defenses against computer viruses and theft now that officials have said its computer system could be attacked. The agency has already installed "Critical Tier I" computer firewalls at its headquarters. Documents say the firewalls will protect access to the MTA's network and its website. An "Intrusion Detection System" has also been placed in MTA computers and employees have been offered encryption software. An additional firewall and other virus protectors will be installed later. The agency is also expected to approve $5.25 million in upgrades for the security of regional bridges and tunnel facilities.

Category 16.3 *Infrastructure protection & homeland security*

2003-10-02 **foreign worker hi-tech Homeland Security track H-1B**

NewsScan

HOMELAND SECURITY SEEKS BETTER TRACKING SYSTEM FOR H1-B WORKERS

A report by the General Accounting Office (GAO), the investigative arm of Congress, says that the Homeland Security Department needs to keep track of when foreign high-tech workers with H-1B visas enter and leave the country, and to develop rules limiting the length of time workers who lose their jobs are allowed to remain in the country. According to the GAO, "much of the information needed to effectively oversee the H-1B visa program is not available." The Homeland Security Department agreed with the recommendations and is in the process of changing the systems used to track the foreign workers. (AP/San Jose Mercury News 2 Oct 2003)

Category 16.3 *Infrastructure protection & homeland security*

2003-11-03 **infrastructure protection recommendation US FCC**

NIPC/DHS

October 30, FCC — Media Security and Reliability Council to review infrastructure security recommendations.

Recommendations to ensure the continued operation and security of media infrastructure will be presented to leaders from the broadcast, cable and satellite industries at the biannual Media Security and Reliability Council (MSRC) meeting Thursday, November 6. MSRC is a Federal Advisory Committee that reports to FCC Chairman Michael K. Powell. Chairman Powell formed MSRC following the events of September 11, 2001, in order to study, develop and report on best practices designed to assure the optimal reliability, robustness and security of the broadcast and multichannel video programming distribution industries. The Communications Infrastructure Security, Access and Restoration Working Group will present detailed best practices recommendations relating to physical security, including prevention and restoration matters. The council members have until November 26 to vote on the recommendations.

Category 16.3 *Infrastructure protection & homeland security*

2003-11-06 **cyber security cyberspace plan halt Congress FBI report incident**

NIPC/DHS

November 04, Washington Post — Congressman puts cybersecurity plan on hold.

A congressional plan to require publicly traded companies to get computer security audits will be put on hold while technology businesses try to come up with a proposal of their own. Rep. Adam Putnam, R-FL, chairman of a House technology subcommittee, said he will postpone plans to introduce his bill and wait about 90 days to see what kind of alternative the business community proposes. There are no similar bills in the Senate. Businesses often keep cybercrime incidents under wraps and are generally unwilling to publicize any computer security measures, even with law enforcement. According to an April study by the Computer Security Institute and the FBI, just 30 percent of companies that experienced cyberattacks last year reported such incidents to authorities. The business community is also generally opposed to government-sponsored requirements on cybersecurity, whether from Congress or the White House.

Category 16.3 *Infrastructure protection & homeland security*

2003-11-26 **terrorism evaluation US government simulation ISTS Dartmouth DHS**

NIPC/DHS

November 24, Associated Press — Government evaluates simulated terrorist attacks.

Experts inside government and the Institute for Security Technology Studies at Dartmouth College are still formally evaluating results of a simulated terrorist attack carried out by the Department of Homeland Security (DHS) over five days in October. The "Livewire" exercise simulated physical and computer attacks on banks, power companies and the oil and gas industry, among others. "There were some gaps," said Amit Yoran, the chief of the agency's National Cyber-Security Division. "The information flow between various sectors was not as smooth as we would perhaps have liked." Yoran said the mock attacks during the exercise tried to broadly disrupt services and communications across major industrial sectors, enough to make consumers to lose economic confidence. It modeled bombings at communications facilities outside Washington and cyberattacks aimed at companies and other networks. Yoran said the exercise affirmed that troublesome interdependencies exist throughout the nation's most important systems. A broad power outage could also bring down key telephone or computer networks, disrupting repair efforts.

Category 16.3 *Infrastructure protection & homeland security*

2003-12-04 **national security policy review homeland security**

http://www.news.gc.ca/cfmx/CCP/view/en/index.cfm?articleid=73469&%20

SOLICITOR GENERAL DISCUSSES CANADA'S NATIONAL SECURITY POLICY

The Solicitor General of Canada, Wayne Easter, stated that it was time for a substantive review of Canada's national security policy. Easter noted that such a review would need to examine how the Canadian national security system interacts with the U.S. Department of Homeland Security. Additionally, Easter said that it was time to consider the creation of a centralized Canadian national security agency which could also assist in co-coordinating the work of the provinces and territories in times of crisis. He emphasized that keeping the border open for commerce and closed to criminals and terrorists was a priority.

Category 16.3 *Infrastructure protection & homeland security*

2003-12-05 **technology companies secure cyberspace Department Homeland Security DHS urge infrastructure protection**

NIPC/DHS

December 05, Mercury News (CA) — Tech firms urged: secure cyberspace.

Department of Homeland Security (DHS) Secretary Tom Ridge warned Wednesday, December 4, that terrorists who "know a few lines of code can wreak as much havoc as a handful of bombs." It is important that "we share information, work together and close any gaps and weaknesses that terrorists would otherwise seek to exploit," Ridge told an audience of about 350 business leaders and technology experts attending the National Cyber Security Summit in Santa Clara, CA. "It only takes one vulnerable system to start a chain reaction that can lead to a devastating result," Ridge added. Robert Liscouski, the DHS's assistant secretary for infrastructure protection, made clear there would be consequences if the corporations that control 85 percent of the nation's critical infrastructure chose not to cooperate. The DHS wants businesses to provide information about cyber attacks so it can identify major threats to computer networks that control everything from water supplies and power lines to banking and emergency medical services. DHS officials say they need such data to create an early warning system. The full text of Secretary Ridge's remarks are available on the DHS Website: http://www.dhs.gov/dhspublic/interapp/speech/speech_0151.xml

---

Category 16.3 *Infrastructure protection & homeland security*

2003-12-05 **information security cyber chief security officer council**

NIPC/DHS

December 04, Federal Computer Week — Fed cybersecurity chiefs get a council.

Information security has become important enough to warrant a federal Chief Security Officers Council to work with similar groups of government executives, the man in charge of national cybersecurity said this week. There is already a CIO Council, a CFO Council and a Chief Human Capital Officers Council, but security is so complicated now that Amit Yoran, director of the Department of Homeland Security's National Cyber Security Division, decided to initiate a council focused specifically on that one issue. "The CIOs have a lot on their plate and under [the Federal Information Security Act] every agency must have a security official...and this allows them to collaborate and discuss issues," Yoran said. The new CSO Council will work closely with the CIO Council, but having a separate forum where chief security officers can get together and discuss problems, tactics and best practices should make improvement easier, Yoran said.

Category 16.3 *Infrastructure protection & homeland security*

2003-12-11 **US government agencies cybersecurity secure critical information systems fail test**

NIPC/DHS

December 09, Government Executive — Agencies get failing grades on cybersecurity.

Federal efforts to secure critical computer systems and sensitive information are improving, but more than half of all agencies are still doing very poorly at the task, lawmakers said Tuesday, December 9. Overall, the federal government received a grade of D for cybersecurity, up from a grade of F a year earlier, according to the 2003 Federal Computer Security Scorecard released Tuesday. The scorecard, which is compiled by the House Government Reform subcommittee, is based on information reported by each agency and federal inspectors general to Congress and the Office of Management and Budget. Senator Susan Collins (R-ME), who chairs the Senate Governmental Affairs Committee, urged agencies to take immediate action to improve cybersecurity. "The administration has reason to believe that cyberattacks could be part of terrorists' game plans," she said. "We cannot afford to be caught off guard."

Category 16.3 *Infrastructure protection & homeland security*

2003-12-30 **new year security metal detectors New York's Times Square**

NewsScan

HIGH-TECH SECURITY FOR NEW YEAR'S EVE

On New Year's Eve, about 240 metal detectors will be used to screen the crowds of people who come to watch the ball drop in New York's Times Square, and radar-equipped Black Hawk helicopters and Citation jets will patrol the skies over the city. New York Mayor Bloomberg says: "You're going to see a lot of cops there and there will be a lot more cops that you don't see." In addition to Homeland Security air patrols, the Police Department's eight helicopters will be in the air, including one with a powerful video camera. (New York Times 30 Dec 2003)

Category 16.3 *Infrastructure protection & homeland security*

2004-01-08 **US government IT security efforts department**

NIPC/DHS; http://www.eweek.com/article2/0,4149,1426312,00.asp

January 05, eweek.com — Agencies beef up IT security.

The Department of Justice (DOJ), one of a handful of agencies that received a failing grade on last month's report card on IT security delivered by a congressional subcommittee, is at the forefront of the movement. The DOJ has made a number of changes, including the establishment of a department-wide IT security staff that answers directly to the CIO, according to DOJ officials. That group, in turn, has set about organizing a security council within the department, they said. The council comprises the top security officials from each of Justice's dozens of component organizations, and is now responsible for implementing and overseeing all the security programs in the department. So far, the results have been encouraging, department officials said. Another agency, the Environmental Protection Agency has created an automated security evaluation and remediation application capable of testing the security posture of each machine and monitoring the remediation process for any problems found. The Department of Transportation recently implemented a comprehensive vulnerability assessment and remediation package that performs continuous scans, instead of the traditional monthly or quarterly assessments.

Category 16.3 *Infrastructure protection & homeland security*

2004-01-09 **Homeland Security terrorism anti-terrorism flight cancellation airline plane fear uncertainty doubt FUD**

RISKS 23 13

BRUCE SCHNEIER ON ORANGE ALERT IN SALON (FROM DAVE FARBER'S IP)

Contributor Cory Doctorow supplies a Bruce Schneier article on flight cancellations and US anti-terrorism efforts. In this article entitled "Homeland Insecurity," Schneier analyzes the event of 15 flight cancellations in the US in January 2004. Schneier points out that all 15 of these flight cancellations had turned out to be false alarms. He says that security is a tradeoff between its costs and benefits, and stresses that cancelling flights because of not-so-credible threats will be too expensive in the long run. But Schneier appreciates that intellegence is difficult, and involves painstaking data analysis. "The crucial bits of data," he observes, "are just random clues among thousands of other random clues, almost all of which turn out to be false or misleading or irrelevant." He says that, in fact, working with too much data can be problematic. Schneier adds that throwing more computers into data analysis will not help because "[F]inding the real plot among all the false leads requires human intelligence." He concludes that the 15 airline cancellations reflected old problems with US intelligence--"too much bureaucracy and not enough coordination."

Category 16.3 *Infrastructure protection & homeland security*

2004-01-18 **quality assurance vendor liability Department Homeland Security DHS software products support anti-terrorism by fostering effective technology SAFETY quality anti-terrorism technology QATT**

RISKS 23 14

DHS PROTECTS VENDORS OF ANTI-TERRORISM TECHNOLOGIES FROM LIABILITY

Jay Wylie is concerned that Support Anti-terrorism byFostering Effective Technologies (SAFETY) Act of 2002 will lead to worse software-product quality. SAFETY "protects vendors of anti-terrorism products that have been vetted by the Department of Homeland Security and designated as QATT (Qualified Ani-Terrorism Technology) from liabilities that arise from any failings of the anti-terrorism technology," writes Wylie. An article about SAFETY, by Roland L. Trope, appeared in IEEE Spectrum in January 2004. Jay Wylie is dissappointed that this publication by a society of professional engineers "is more concerned about vendors being aware of the protection from liability than questioning whether such protection is appropriate."

Category 16.3 *Infrastructure protection & homeland security*

2004-01-20 **eyeglass lie detector law enforcement airport security anti-terrorism Homeland Security**

RISKS; http://www.eetimes.com/story/OEG20040116S0050 23 14

LIE-DETECTOR GLASSES, 90% ACCURATE?

Steve Holzworth refers us to a story in eetimes.com on a new lie-detector technology that may come to be used for airport security soon. This lie detector measures the frequency range of voice patterns to report with 89% accuracy if someone is lying. The lie detector is so small that it can fit in the eyeglasses of law enforcement officers. When an airport security screener asks a passenger, "Do you plan on hijacking this plane?", the lie detector will flash green, yellow, or red to the security screener to indicate true, uncertain, or false passenger responses. Given the success rate of this lie-detector, Steve Holzworth remarks, "Oh, excellent! I only have a 1 in 10 chance of being falsely accused." In a follow-up article, contributor Ron Bean says that this lie-detector technology "sounds like it's detecting people's emotional "hot buttons", rather than lies per se." He thinks a good actor could defeat this lie-detector. He concludes by asking, "What's the rate for false positives vs false negatives?" for this lie-detector. Contributor Peter B. Ladkin attempts to answer that in his follow-up article. Ladkin says the 89% accuracy of the lie detector says nothing about the technology's usefulness. Ladkin calls false positives and false negatives Type 1 and Type 2 errors respectively. He writes that in order to understand the problem, one needed "reliable information about the background rate of lying" of the population. Ladkin considers three cases with the given 1 in 10 success rate. In the first case, the background rate of lying is 1 in 10; therefore the passenger is never falsely accused of lying. In the second case, all errors are of Type 1; so the passenger "has a 1 in 10 chance of being falsely accused." In the third case, "[E]rrors are evenly split between Type 1 and Type 2, and the background rate of lying is 1 in 2." Now, an innocent passenger and an actual hijacker have a 1 in a 20 chance of failing and passing the test respectively. Ladkin thinks this technology is "impossible in serious use." He concludes, "…the company spokesman is Bsing,
as are most people who claim to have measured the accuracy of lie-"detector" apparatus."

Category 16.3 *Infrastructure protection & homeland security*

2004-01-28 **Homeland Security government centralized alert system**

NewsScan

HOMELAND SECURITY DEPARTMENT TO GIVE CYBER ALERTS

The cyber security division of the Department of Homeland Security is creating a new, centralized system for alerting the country to network threats by providing a clearinghouse of information on hacking, viruses, worms and other forms of cyber terrorism. Cyber security director Amit Yoran explains: "We are focused on making the threats and recommended actions easier for all computer users to understand, prioritize and act upon. The vendor community is focused on sales as well as on protecting their clients. Coming from the U.S. government, the focus [of the new centralized system] is solely on the public interest." (Washington Post 28 Jan 2004)

Category 16.3 *Infrastructure protection & homeland security*

2004-01-30 **IT security funding attention US government**

NIPC/DHS; http://www.gcn.com/vol1_no1/daily−updates/24775−1.html

January 28, Government Computer News — Davis, Putnam ratcheting up IT security oversight.

Two key lawmakers are pressing agencies to correct longstanding IT security problems. Tom Davis, chairman of the House Government Reform Committee, on Tuesday, January 27, said his committee will hold a hearing this spring on at least two contracts that failed to take the Federal Information Security Management Act into account. Adam Putnam, chairman of the Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, said he sent a letter to agency secretaries requesting a meeting with their CIOs to discuss their IT security action plans. Putnam said the letters are part of an effort to increase awareness of agency IT security problems. Putnam said his staff already has met with six CIOs and will meet with the CIO Council in March to discuss agency IT security plans, milestones and his subcommittee's expectations. He added his staff also will meet with the appropriations committee staff members to discuss the importance of funding IT security. "We've had some very positive discussions with the CIOs so far," Putnam said.

Category 16.3 *Infrastructure protection & homeland security*

2004-03-22 **security crisis co-ordination center National Cyber Partnership Homeland Security**

NIPC/DHS

March 18, Federal Computer Week — Security groups call for crisis coordination center.

Two national task forces organized by the National Cyber Security Partnership on Thursday, March 18, called for a public awareness campaign, an early warning contact network and a national crisis coordination center to improve the nation's responses to cyber vulnerabilities, threats and incidents. Establishing a national crisis coordination center by 2006 most likely would require legislation or an executive order. Guy Copeland, who led the Early Warning Task Force, said the center would coordinate threat analyses, warnings, research and responses for critical infrastructure-sector experts and federal, state and local officials. The early warning contact network, to be set up as early as December, would be a multichannel network housed and administered by the Department of Homeland Security's U.S. Computer Emergency Readiness Team. Communication would occur primarily via the Internet, although task force leaders recommended having a backup means of communicating if the Internet goes down. Reaching home users will be accomplished largely through the cooperation of Internet service providers who would keep their customers informed of cybersecurity threats and attacks, task force leaders said. 2004-03-30 16.3 March 30, SearchSecurity.com — SCADA security hearing begins today. Last summer's massive blackout in the Northeast demonstrated the vulnerability of our nation's most critical networks. It also set in motion an inquiry that today, March 30, brings together legislators and IT experts to discuss how to better secure these networks from further disaster. Supervisory Control and Data Acquisition (SCADA) systems, associated with power plants and other mission-critical networks, especially need stronger protection. "Historically, there is a false sense of security related to SCADA systems. Some administrators have been comforted by the thought that these systems are specialized and often deployed in a 'closed' network utilizing proprietary protocols," explains Andre Yee, president and CEO of a network security vendor. One problem with securing SCADA is the unique nature of the systems. Most operate in real time and can't afford to be offline for lengthy upgrades or security installations, for fear of a degradation of performance. Another problem, Yee notes, is with newer SCADA systems incorporating more Web accessibility, which poses myriad problems when using the Internet, a public conduit susceptible to attack. They also leverage Unix and Windows systems, which puts networks at risk, particularly given the number of vulnerabilities that can be exploited.

Category 16.3 *Infrastructure protection & homeland security*

2004-03-26 **security education coding programming Department Homeland Security**

DHS IAIP Daily;

March 25, Federal Computer Week — Security needs better education for programmers.

Dealing with Internet computer worms and viruses requires a long-term education effort aimed at programmers while they are still in college, a Department of Homeland Security (DHS) executive said Thursday, March 25. Lawrence Hale, deputy director of the DHS' U.S. Computer Emergency Readiness Team, said, "the things that are costing us the most pain are preventable." Programmers can be taught to avoid creating buffer overflows and other well-known vulnerabilities found in commercial software, said Hale, speaking at the FOSE conference on government technology in Washington, DC. It could be years before the results of education show up in software that is being sold, but the effort is needed more than ever because the problem is getting worse, officials said. Hale said an increasing number of cyberattacks are done for profit. "Worms are turning machines into mail servers," he said. "Your machines are being used to spam." In addition to working with universities to promote secure programming practices, DHS is working with researchers at Lucent Technologies' Bell Labs and other organizations on new tools that could detect the precursors of network attacks, Hale said.

Category 16.3 *Infrastructure protection & homeland security*

2004-03-30 **identification authentication airport security lawsuit**

NewsScan

ADVOCATE LOSES SUIT AGAINST AIRLINE ID REQUIREMENT

John Gilmore, a privacy advocate with the Electronic Frontier Foundation, has lost a federal lawsuit he'd filed after he'd been denied entry to a Southwest Airlines flight for refusing to show identification prior to boarding. Judge Susan Illston ruled that that a request for a passenger's identification does not violate that passenger's Fourth Amendment rights, and rejected Gilmore's claims that the somewhat vague regulations violated due process. But Gilmore could still find good news in the dismissal of his lawsuit: "Judge Illston confirmed I do have standing to challenge but said, 'You're in the wrong court.' I need to go to the court of appeals. I will continue working on the issue. This isn't the end." (AP/San Jose Mercury News 30 Mar 2004)

Category 16.3 *Infrastructure protection & homeland security*

2004-03-30 **SCADA security hearing power failure blackout Northeast critical infrastructure protection**

DHS IAIP Daily; http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci957331,00.html

March 30, SearchSecurity.com — SCADA security hearing begins today.

Last summer's massive blackout in the Northeast demonstrated the vulnerability of our nation's most critical networks. It also set in motion an inquiry that today, March 30, brings together legislators and IT experts to discuss how to better secure these networks from further disaster. Supervisory Control and Data Acquisition (SCADA) systems, associated with power plants and other mission-critical networks, especially need stronger protection. "Historically, there is a false sense of security related to SCADA systems. Some administrators have been comforted by the thought that these systems are specialized and often deployed in a 'closed' network utilizing proprietary protocols," explains Andre Yee, president and CEO of a network security vendor. One problem with securing SCADA is the unique nature of the systems. Most operate in real time and can't afford to be offline for lengthy upgrades or security installations, for fear of a degradation of performance. Another problem, Yee notes, is with newer SCADA systems incorporating more Web accessibility, which poses myriad problems when using the Internet, a public conduit susceptible to attack. They also leverage Unix and Windows systems, which puts networks at risk, particularly given the number of vulnerabilities that can be exploited.

Category 16.3 *Infrastructure protection & homeland security*

2004-03-31 **critical infrastructure protection challenges efforts report**

NIPC/DHS; http://www.gao.gov/highlights/d04354high.pdf

March 15, General Accounting Office — GAO-04-354: Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems (Report).

Computerized control systems perform vital functions across many of our nation's critical infrastructures. For example, in natural gas distribution, they can monitor and control the pressure and flow of gas through pipelines. In October 1997, the President's Commission on Critical Infrastructure Protection emphasized the increasing vulnerability of control systems to cyber attacks. The House Committee on Government Reform and its Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census asked GAO to report on potential cyber vulnerabilities, focusing on (1) significant cybersecurity risks associated with control systems (2) potential and reported cyber attacks against these systems (3) key challenges to securing control systems and (4) efforts to strengthen the cybersecurity of control systems. GAO recommends that the Secretary of the Department of Homeland Security (DHS) develop and implement a strategy for coordinating with the private sector and other government agencies to improve control system security, including an approach for coordinating the various ongoing efforts to secure control systems. DHS concurred with GAO's recommendation. Highlights: http://www.gao.gov/highlights/d04354high.pdf

---

Category 16.3 *Infrastructure protection & homeland security*

2004-04-01 **Transporation Security Administration TSA RFID tags airplane boarding terrorism anti-terrorism**

NewsScan

TSA EYES RFID BOARDING PASSES

The Transportation Security Administration is looking into the possibility of using RFID-tagged airline boarding passes that would enable passenger tracking in airports -- a proposal that has raised the hackles of some privacy advocates. TSA says it would use the special boarding passes in conjunction with its "registered traveler" program, which would permit frequent fliers to provide detailed personal information, corroborated by a background check. The RFID passes would allow these registered travelers to speed through "special lanes" during the boarding process. The TSA has already started work to deploy RFID boarding passes in some countries in Africa under the Federal Aviation Administration's Safe Skies for Africa Initiative. But Katherine Albrecht, who worked against the use of RFID tags on retail goods, says this new proposal is a "nightmare scenario," which uses technology to invade people's privacy. "Are they going to track how long I spend in the ladies room?" she asks. (Computerworld 1 Apr 2004)

Category 16.3 *Infrastructure protection & homeland security*

2004-04-09 **fraud passport scanners identification authentication**

NewsScan

AUSTRALIA DEPLOYS FRAUD-DETECTING PASSPORT SCANNERS

Australia has installed 400 iA-thenticate document readers from Imaging Automation in its airports in the hope of authenticating the passports of every person entering the country. The shoebox-sized device uses multiple light sources to examine hundreds of security features on travel documents. Many of the features, such as the composition of the ink used, are invisible to the naked eye. The iA-thenticate system ranges from $5,000 to $15,000 per unit and is being used or tested by a number of countries, including Canada, Hungary, Sweden, Finland and Nigeria. Imaging Automation is marketing the system to the U.S. Department of Homeland Security, which is facing delays in deployment fingerprint and facial biometric systems for passport-authentication. (AP 9 Apr 2004)

Category 16.3 *Infrastructure protection & homeland security*

2004-04-21 **Department Homeland Security coordination infrastructure protection**

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml?articleID=18902167

April 19, InformationWeek — DHS needs public-private cooperation.

Speaking at the Information Security Decisions conference in New York on Monday, April 19, Amit Yoran, director of the Department of Homeland Security's National Cyber Security Division, noted the challenges associated with this need for public-sector agencies and private-sector companies to coordinate their knowledge of cyberthreats and physical threats, as well as infrastructure vulnerabilities. DHS estimates that private-sector companies run 85% of the services required to ensure national security, public health and safety, and economic stability. Yet private-sector executives are reluctant to provide critical infrastructure information about their companies' operations for fear of their vulnerabilities becoming a matter of public record. Software quality is also a key issue for cybersecurity--particularly because most software users aren't security experts. Developers must address the most obvious problems. "Ninety-five percent of software bugs are caused by the same 19 programming flaws," Yoran said. And software quality will only become more difficult to police as more and more is developed by foreign nationals both offshore and within the United States, Yoran said. Companies will have to be on guard against backdoors potentially written into software that could allow access to their systems.

Category 16.3 *Infrastructure protection & homeland security*

2004-04-25 **security clearinghouse Federal government ISACS secure network operations center SOC DHS**

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1572951,00.asp

April 25, eWEEK — Feds making plans for security clearinghouse.

The federal government is developing plans for a secure network operations center (SOC) for all security information flowing to and from the government. The SOC would be a clearinghouse that gathers and analyzes data from the private sector, mainly the Information Sharing and Analysis Centers (ISACS) in several major vertical industries. The SOC would be run jointly by personnel from the DHS and a civilian contractor that would help build the facility. DHS officials said that even though there are less formal information-sharing efforts between government and private industry, there still is a need for a more structured program. "We're trying to operationalize the public/private partnership," said Amit Yoran, director of the National Cyber Security Division at DHS, last week. "The private sector genuinely wants to make progress on this. I think, as we get more considerate of the private sector in terms of the FOIA [Freedom of Information Act] exemption, things will come along." Officials said they hope to have plans for the SOC finalized soon and intend to fund the initiative out of the current fiscal year's budget, which runs out September 30.

Category 16.3 *Infrastructure protection & homeland security*

2004-04-27 **Islamic webmaster free speech trial prosecution civil liberties USAPATRIOT antiterrorism law**

http://www.nytimes.com/2004/04/27/national/27BOIS.html?ex=1084089284&ei=1&en=bd65293d3d6b1e62

The U.S.A.P.A.T.R.I.O.T. (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) Act makes it a crime to provide "expert guidance or assistance" to groups deemed terrorist. As a result, 34-year-old Sami Omar al-Hussayen of Saudi Arabia, a PhD candidate in computer science at the University of Idaho, was charged with three counts of conspiracy to support terrorism and 11 counts of visa and immigration fraud for being the Webmaster for several Islamic organizations, some of which had Web links to other sites where people praised suicide bombers in Chechnya and in Israel. He was charged with providing "computer advice and assistance, communications facilities, and financial instruments and services that assisted in the creation and maintenance of Internet Web sites and other Internet medium intended to recruit and raise funds for violent jihad, particularly in Palestine and Chechnya."

Defense lawyers denied that Mr. Hussayen sympathizes with extremist views; prosecutors claim that he is a secret terrorist. Civil liberties advocates argue that the law is so broad that "Somebody who fixes a fax machine that is owned by a group that may advocate terrorism could be liable," according to Prof. David Cole of the Georgetown University school of law. Judge Audrey B. Collins of the Federal District Court in Los Angeles wrote in another case dealing with the U.S.A.P.A.T.R.I.O.T. Act that "a woman who buys cookies at a bake sale outside her grocery store to support displaced Kurdish refugees to find new homes could be held liable" if the sale were sponsored by a group that were designated terrorist by the government.

Civil liberties activists also point out that the defendants activities as Webmaster and dealing entirely with ideas and statements are supposed to be protected by the First Amendment of the US Constitution.

Category 16.3 *Infrastructure protection & homeland security*

2004-04-27 **Homeland Security NSA team up cybersecurity COAEIAE**

DHS IAIP Daily; http://fcw.com/fcw/articles/2004/0426/web−nsa−04−27−04.asp

April 27, Federal Computer Week — DHS, NSA team on cybersecurity.

On April 22, officials from National Security Agency (NSA) and the Department of Homeland Security (DHS) announced the formation of the National Centers of Academic Excellence in Information Assurance Education. It stems from NSA's Centers of Academic Excellence in Information Assurance Education Program, which started in 1998 and recognizes 50 universities in 26 states. The National Strategy to Secure Cyberspace, issued in 2002 by the Bush administration, directs the government to foster training and education programs that support computer security needs and responsibilities, and improve existing information assurance programs. Earlier this month, NSA officials announced they would hire 1,500 people by September and 1,500 employees each year for the next five years. Agency jobs include information technology and acquisition positions in addition to traditional code-making and code-breaking roles, according to an April 7 statement.

Category 16.3 *Infrastructure protection & homeland security*

2004-04-28 **PATRIOT act ACLU civil liberties constitution privacy terrorism anti-terrorism US government**

NewsScan

[U.S.A.P.A.T.R.I.O.T.]… ACT RULES MUFFLE DISSENT

The secrecy provisions of the ...[U.S.A.P.A.T.R.I.O.T.] Act have prevented the American Civil Liberties Union from publicizing a lawsuit it filed three weeks ago challenging the FBI's methods of obtaining many business records. The ACLU was recently allowed to release a redacted version of the lawsuit following extended negotiations with the Justice Department. "It is remarkable that a gag provision in the U.S.A.P.A.T.R.I.O.T. Act kept the public in the dark about the mere fact that a constitutional challenge had been filed in court," says ACLU associate legal director Ann Beeson. "President Bush can talk about extending the life of the U.S.A.P.A.T.R.I.O.T. Act, but the ACLU is gagged from discussing details of our challenge to it." The crux of the ACLU's case concerns a section of the Act that allows the FBI to request financial records, telephone and e-mail logs, and other documents from businesses without a warrant or judicial approval. Such requests are known as "national security letters," and the FBI has issued scores of such letters since late 2001. The ACLU complaint says that using national security letters to force Internet service providers to turn over names, screen names, e-mail addresses and other customer information without proper notice to customers raises questions about the constitutionality of the ...[U.S.A.P.A.T.R.I.O.T.] Act's legal underpinnings. (Washington Post 29 Apr 2004)

Category 16.3 *Infrastructure protection & homeland security*

2004-05-03 **wireless federal government Homeland Security**

DHS IAIP Daily; http://www.fcw.com/fcw/articles/2004/0503/pol−wireless−05−03 −04.asp

May 03, Federal Computer Week — Agencies team to develop integrated wireless network.

The Integrated Wireless Network (IWN) will provide a common wireless infrastructure to support the departments of Homeland Security, Justice, and Treasury, and officials expect to release their requirements this summer. Bringing three diverse departments together can be challenging, said Mike Duffy, Justice's deputy chief information officer for e-government, citing as an example the number of people needed to approve a memorandum of understanding. But the three agencies' leaders see the benefits and are committed to the project, he said. "The architecture analysis we conducted show there are substantial savings to be had both in cost and spectrum use by consolidating the three departments' resources," Duffy said. The new network will replace the aging wireless systems in many of the departments' components and will be designed to serve more than 80,000 law enforcement and homeland security users at 2,500 radio sites. The statement of objectives for IWN will be released in June or July and will outline the expectations and constraints of the project, officials said. Although the project will initially focus on voice capabilities, it will soon require wireless data capabilities, officials said. Also, the standards-based system must work with state and 10 local law enforcement systems.

Category 16.3 *Infrastructure protection & homeland security*

2004-05-03 **first responder communications network Homeland Security incident management**

DHS IAIP Daily; http://home.businesswire.com/portal/site/google/index.jsp?ndmViewId=news_view&newsId=20040503005637&newsLang=en

May 03, Business Wire — Responder network to be installed in Kansas agencies.

A $993,500 grant from the U.S. Department of Justice was awarded to the University of Kansas to install a Homeland One First Responder Network across the state of Kansas. The Kansas Law Enforcement Training Center and the Kansas Fire and Rescue Training Institute, both units of University of Kansas Continuing Education, will administer the grant. The grant calls for Homeland One First Responder Training and Communications Network to be installed at 319 Kansas law enforcement and fire services agencies across the state. "The University of Kansas has been a recognized leader in providing law enforcement and fire service training for more than 60 years," said JoAnn Smith, vice provost for university outreach and dean of Continuing Education at the University of Kansas. Homeland One's training modules are modeled on National Interagency Incident Management Systems and based on the Department of Homeland Security's Office for Domestic Preparedness (ODP) First Responder Training Guidelines and Standardized Emergency Management System (SEMS) standards.

Category 16.3 *Infrastructure protection & homeland security*

2004-05-04 **Virginia Information Technologies Agencies VITA template business continuity planning**

DHS IAIP Daily; http://www.gcn.com/23_10/homeland−security/25813−1.html

May 04, Government Computer News — Virginia uses software template to standardize its agencies' COOPs.

The Virginia Information Technologies Agency (VITA) is providing state and local government agencies with training and a template for establishing standard continuity of operations plans (COOPs). Paul Lubic, VITA's associate director for policy, practice and architecture, said his agency recently bought software to promote the adoption of best practices. "We see a value in using the template so the continuity of operations plans will be in a standard format, which will enhance the management of those plans at the governor's office level," Lubic said. "Having them all look the same will let us quickly navigate to get the information we need in case of an emergency." The software includes an online template that lets agencies create their plans and store them in a central repository. "To answer the questions, the agencies must have an understanding of their business and the processes that are critical to their mission," Lubic said. The system also can notify government workers in the event of a disaster via wireless e-mail devices.

Category 16.3 *Infrastructure protection & homeland security*

2004-05-04 **business continuity planning disaster recovery federal government**

DHS IAIP Daily; http://www.gcn.com/23_10/homeland−security/25793−1.html

May 04, Government Computer News — Agencies take notice of continuity planning.

Next week, more than 2,500 federal employees from 45 agencies will test how prepared the government is to stay open if disaster strikes. The Homeland Security Department's Emergency Preparedness and Response Directorate, which still uses the acronym FEMA, will run Exercise Forward Challenge to see how far along agencies are in developing and implementing continuity of operations plans, or COOPs. During the exercise, employees will go to alternate work sites outside Washington and then try to hook up to their networks, access e-mail and data files, communicate with other federal officials and perform their usual tasks. "This is a full-scale operation designed to test interdependencies and essential functions," FEMA undersecretary Michael Brown said. "Agencies will find out if their plans 9 work, and it will give them a wake-up call to fix any problems." Brown last month told lawmakers he is confident that agencies are prepared. Linda Koontz, director for information management issues for the General Accounting Office, expressed less optimism. She told the committee that she would not guarantee that agencies would continue to operate at full capacity if a catastrophe hit the Washington area.

Category 16.3 *Infrastructure protection & homeland security*

2004-05-13 **business continuity of operations planning coop federal government Homeland Security DHS**

DHS IAIP Daily; http://www.dhs.gov/dhspublic/display?content=3554

May 13, Department of Homeland Security — Federal Government tests continuity of 8 operations plans.

The Department of Homeland Security (DHS) and more than 40 other agencies are testing their continuity of operations (COOP) plans during Forward Challenge 04 (FC 04), a two day exercise May 12-13. The exercise is a full-scale, scenario-based event in which Federal departments and agencies are implementing COOP plans, deploying pre-designated personnel and leadership at alternate sites away from the National Capital Region and performing essential functions at those locations. In order to ensure Federal departments and agencies are prepared to continue essential operations during any type of threat or emergency, DHS maintains an active program of planning, testing, training and evaluation of the Federal Executive Branch COOP program. Forward Challenge 04 tests the federal government's readiness to respond and ability to resume critical operations during an emergency situation. "This is the first-time that the Federal government has conducted a government-wide test of its continuity of operations plans," said DHS Secretary Tom Ridge.

Category 16.3 *Infrastructure protection & homeland security*

2004-05-14 **Homeland Security Data Analysis NVAC Federal Government**

DHS IAIP Daily; http://fcw.com/fcw/articles/2004/0510/web−dhsvis−05−13−04.as p

May 14, Federal Computer Week — DHS funds data center.

The Department of Homeland Security (DHS) has created a center to develop new methods and tools that would manage, analyze and graphically represent vast and diverse amounts of data to discover and predict potential terrorist activities. The Department of Energy's Pacific Northwest National Laboratory (PNNL), located in Richland, WA, will receive $2.5 million this year for the new National Visual Analytics Center (NVAC) that will work on projects related to analyzing data that includes text, measurements, images and video. It's expected that NVAC will establish four or five regional visual analytics centers next year as funding becomes available. NVAC's core responsibilities include research and development, education, technology evaluation and implementation and integration and coordination of research programs across government agencies. It will not collect data but develop tools for new ways to evaluate information currently being used by counter-terrorism analysts. It will also work with university researchers to develop future visual analytics technology.

Category 16.3 Infrastructure protection & homeland security

2004-05-14 **Homeland Security states Websites communication training events calendar**

DHS IAIP Daily; http://www.govtech.net/news/news.php?id=90248

May 14, Government Technology — Oklahoma's redesigned Homeland Security Website.

Oklahoma's Office of Homeland Security recently launched an enhanced Website with several new interactive services that facilitate communication between the eight Oklahoma regional councils, its members and training officers. The Web site allows the public to see who is working on homeland security initiatives in their area while providing a secure electronic avenue for authorized users to communicate with officials and other select representatives. After successful login, authorized users can post messages and documents to regional bulletin boards. The training events calendar is accessible to the public and published on the Office of Homeland Security Web site. "The new Website is an excellent way for our office to communicate with the public and with responders, each of whom is essential to homeland security efforts," said Kerry Pettingill, director of the Oklahoma Office of Homeland Security.

Category 16.3 Infrastructure protection & homeland security

2004-05-17 **Homeland Security DHS SPIRIT, Resource Sharing**

DHS IAIP Daily; http://fcw.com/fcw/articles/2004/0517/news−dhs−05−17−04.asp

May 17, Federal Computer Week — DHS regroups on SPIRIT; IT services pact delayed again.

The Department of Homeland Security (DHS) officials have decided to reassess their proposed five-year, $5 billion information technology services program, delaying the release of the final request for proposals for at least another month. The Security, Planning and Integrated Resources for Information Technology (SPIRIT) program, which would cover nearly all IT services for DHS, was scheduled to be released this week. SPIRIT started as the Coast Guard Information Technology Services Solution in November 2002, but two months later officials decided it would be a departmentwide program valued at $10 billion for 10 years. Since last summer, however, promises to release an RFP have failed to materialize at least six times.

Category 16.3 Infrastructure protection & homeland security

2004-05-18 **Homeland Security DHS customs data analysis**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/homeland−security/25913−1.html

May 18, Government Computer News — Auditors warn of delays, overruns in Customs system.

The Department of Homeland Security's (DHS) massive new system for processing import-export data faces continuing cost and scheduling problems, the General Accounting Office (GAO) said on Tuesday, May 18. Customs and Border Protection, a DHS agency, last year inherited the Automated Commercial Environment project from the Customs Service. Since then, cost and scheduling problems have multiplied, GAO reported. ACE releases 1 and 2 cost $109.4 million instead of the planned $86.1 million, while releases 3 and 4 ballooned from $146.4 million to $192.4 million, GAO said. GAO said the customs agency coped by borrowing resources from forthcoming releases and overlapping activities to catch up with its schedule. Department officials said they agree with the auditors' conclusions and are working to correct the problems. The report is available at http://www.gao.gov/new.items/d04719.pdf

---

Category 16.3 Infrastructure protection & homeland security

2004-05-18 **trial internet terrorism Islamic Assembly North America Michigan**

NewsScan

TRIAL OF MAN ACCUSED OF USING INTERNET FOR TERRORISM

In the terrorism trial of a University of Idaho computer science graduate student Sami Omar Al-Hussayen, a 34-year-old Saudi national, prosecutors say that they've proven a conspiracy between the defendant and the Michigan-based Islamic Assembly of North America to use the Internet to foster terrorism, and that they should therefore be allowed to show jurors Web postings about the Assembly that are not specifically related to Al-Hussayen. In rebuttal, Defense attorney David Nevin argues that his client is charged with promoting terrorism just because some Internet sites he helped maintain carried objectionable material: "We're circling around and around and making our way toward the issue of the First Amendment that has been floating around here from the start." Besides being accused of terrorist activities, Al-Hussayen is also accused of visa fraud and making false statements to cover up his association with the Assembly. (AP/USA Today 18 May 2004)

Category 16.3 *Infrastructure protection & homeland security*

2004-05-19 **security overreactions technology and society**

DHS IAIP Daily; http://www.fox11az.com/news/state/stories/KMSB−20040519 −famb p−bombscare.1d988929f.html

May 19, FOX11AZ (Tucson, AZ) — Bomb scare grounds America West plane.

An MP3 player wrapped around a soda can sparked a bomb scare at Phoenix Sky Harbor International Airport Wednesday morning, May 19, said an official with the Transportation Security Administration. Nearly 120 passengers on board the America West plane were evacuated Wednesday. The can was found in the cabin of America West Airlines flight 44 from Phoenix to Washington, DC. The bomb squad was called in and a bomb-sniffing dog was taken aboard the plane. All 117 passengers were safely evacuated. They will all be re-screened before they are allowed back on a plane to continue on to Washington. Investigators are looking into how the can came to be aboard the plane.

Category 16.3 *Infrastructure protection & homeland security*

2004-05-20 **Homeland Security DHS overreaction subway photo video ban**

DHS IAIP Daily; http://www.wnbc.com/traffic/3328661/detail.html

May 20, Associated Press — Possible ban on subway photos, videos to deter terrorists.

New York Transit officials on Thursday, May 20, proposed banning photography on subways and buses for their more than seven million daily riders to deter terrorists from conducting surveillance of the nation's largest mass transit system. NYC Transit, the division of the Metropolitan Transportation Authority that runs the subways, the buses and the Staten Island Railway, said the ban on photography and videotaping would not apply to journalists with valid ID cards or to people with written permission. Officials have paid increasing attention to transit security as the Republican National Convention approaches and following the March 11 Madrid commuter train bombings, which killed 191 people. NYC Transit President Lawrence Reuter said the rule changes were "intended to enhance security and safety" for customers and employees. NYC Transit also proposed banning passengers from using end doors to move from one subway car to another, putting feet up on seats and standing on skateboards on subways or buses, among other changes. Violators of the rules would be subject to fines. The changes need MTA board approval after a 45-day period of public comment.

Category 16.3 *Infrastructure protection & homeland security*

2004-05-24 **monitor visitors inside United State U.S. Homeland Security Computer identification databases track systems**

NewsScan

SYSTEM FOR TRACKING VISITORS TO U.S.

The Department of Homeland Security is getting ready to award a very large contract (perhaps worth as much as $15 billion) for a network of databases to track visitors to the country before and after they arrive. The system will attempt to show where the visitors are going and whether they pose a terrorist threat. The three companies vying for the contract, which is called US-Visit, are Accenture, Computer Sciences, and Lockheed Martin. Visitors arriving at checkpoints will face real-time identification to confirm they are who they say they are and to make it possible to track them while they remain inside the U.S. Asa Hutchinson of Homeland Security says, "This is hugely important for the security of our country and for the wise use of our limited resources. We're talking here about a comprehensive approach to border security." Civil libertarians are alarmed that the databases could, despite assurances from the Homeland Security department, be used to monitor American citizens. (New York Times 24 May 2004)

Category 16.3 *Infrastructure protection & homeland security*

2004-05-31 **Homeland Security foreign visitor tracking surveillance Accenture**

NewsScan

ACCENTURE BID WINS HOMELAND SECURITY PROJECT

The Department of Homeland Security has awarded Accenture LLP a contract worth up to $10 billion to expand a program called "U.S. Visit" designed to track millions of foreign visitors from the time they arrive until the time they leave. The data collected by the system includes digital
photographs and fingerprints, and is used to help authorities capture suspected terrorists and criminals. Department of Homeland undersecretary Asa Hutchinson say, "I don't think you could overstate the impact of this responsibility, in terms of security of our nation. If you look at the 9/11
terrorists, they came here in violation of our immigration laws." The subcontractors in the Accenture team include AT&T, Dell, and KBR, and 26 others. (Washinton Post 2 Jun 2004)

Category 16.3 *Infrastructure protection & homeland security*

2004-06-02 **border controls homeland security technology biometrics**

http://www.nytimes.com/2004/06/02/technology/02secure.html?th=&pagewanted=print&position=

Bermuda-based Accenture was awarded a multibillion-dollar contract by the Department of Homeland Security to establish high-technology border controls in a projected called "US-Visit." Critics complained that the contract should have gone to a firm that pays US taxes, but Accenture retorted that it does, and it has 25,000 employees in Reston, VA. The project will integrate dozens of federal databases and could use the biometric identification and authentication technologies to control traffic into the US.

Category 16.3 *Infrastructure protection & homeland security*

2004-06-16 **Internet protocol IP voice over VoIP deregulation terrorism control fear**

NewsScan

TERROR OVER INTERNET PROTOCOL?

A senior Justice Department official has told a Senate committee that law enforcement faces new threats from Internet-based telephone services, and warned that legislative efforts to deregulate VoIP (Voice over Internet Protocol) services could undermine the ability of law enforcement officials
to investigate criminal or terrorist activity. The Justice Department has asked the FCC to require Internet phone companies to design electronic conduits in their networks that would make it easier to tap conversations. James X. Dempsey of the Center for Democracy and Technology says that a
better approach would be for investigators to work cooperatively with Internet phone providers. (Washington Post 16 Jun 2004)

Category 16.3 *Infrastructure protection & homeland security*

2004-07-16 **al-Qaeda information files pictures Arkansas computer anti-terrorism Homeland Security incident**

NewsScan

'ISOLATED INCIDENT': AL-QAEDA FILES ON ARKANSAS COMPUTER

A state computer in Arkansas has been found to contain texts and images that apparently originated with the terrorist group al-Qaeda, but Gary Underwood, chief security officer for the state computer network, says the terrorist-related files were an isolated incident. He received responses from 34 of the 80 agencies he e-mailed Wednesday and said: "The vast majority of those do not have FTP servers at all. Several others responded they had basically private, internal FTP servers used among staff and offices of the agency. Those are secure, user-name and password protected. There were a few that do have publicly accessible FTP servers, but all of those, including now the highway
department, do not allow anonymous uploads. They require a user identification or password to access... Obviously, what happened the other day raised everybody's awareness. If anybody had any questions, they immediately went to find out whether or not it was secure," (AP/USA Today 16 Jul 2004)

Category 16.3 *Infrastructure protection & homeland security*

2004-07-19 **anti-terrorism Homeland Security database Americal Civil Liberties Union ACLU privacy concerns**

NewsScan

MATRIX RELOADED

The crime and terrorism database known as Matrix (the Multistate Anti-Terrorism Information Exchange) is being changed in response to various privacy and legal concerns -- yet not all of Matrix's critics are reassured by the changes. Some of the changes are intended to decentralize the database administration, but Barry Steinhardt of the American Civil Liberties Union says, "Decentralized data which is just as easily accessed as centralized data creates the same privacy problems." Matrix organizers say that the system is entirely limited to information they have always been able to obtain without a warrant. (San Jose Mercury News 19 Jul 2004)

Category 16.3 *Infrastructure protection & homeland security*

2004-07-20 **underwater security summer 2004 Athens Olympic Games Greece fiber-optic network**

NewsScan

UNDERWATER SECURITY IN ATHENS

As part of the preparations for the upcoming Olympic games in Athens, sea divers have installed an underwater monitoring network of fiber-optic cables wrapped in green plastic. Protesters contend the network is a privacy invasion. A police spokesman said: "The security measures are being
implemented with complete respect for human rights and according to the guidelines set out by the agency responsible for privacy and data protection" -- but a protest group called Campaign Anti-2004 complains: "For us the Olympic Games are not welcome. The culture of the Olympic Games is
not ours." (AP/USA Today 20 Jul 2004)

Category 16.3 *Infrastructure protection & homeland security*

2004-07-21 **anti-terrorism software law enforcement Homeland Security TimeWall information analysis**

NewsScan

SOFTWARE FOR TRACKING TERRORISTS

TimeWall, 3-D virtual presentation developed by a Xerox spinoff called Inxight, tracks people, places, relationships and events, filtering huge amounts of unstructured information from a variety of sources (e.g., e-mail and Internet reports) in two dozen languages, and finding phone numbers, names and other data to identify relationships, patterns and trends. Inxight founder and chief technology officer Ramana Rao explains: "Rather than an intelligence analyst reading all this stuff to decide what is interesting, the software pulls it out automatically and puts it on the wall." The software searches through information in real time and sorts data into various bands, arranged chronologically. The analyst can then move along the bands to go backward or forward in time to see how relationships or events change. (San Jose Mercury News 21 Jul 2004).

Category 16.3 *Infrastructure protection & homeland security*

2004-08-16 **Department Homeland Security Microsoft Windows XP service pack 2 SP2 testing US-CERT**

DHS IAIP Daily; http://www.fcw.com/fcw/articles/2004/0816/news−dhs−08−16
−04. asp

August 16, Federal Computer Week — DHS recommends agencies test Windows SP2.

The Department of Homeland Security's U.S.-Computer Emergency Readiness Team (US-CERT) is recommending that all Microsoft Windows XP users, including agencies, carefully test the company's newest security patch, Service Pack 2, and then deploy it throughout their organizations. US-CERT officials view the patch as a step in the right direction because it "makes Internet Explorer highly resistant to the types of attacks we've seen recently, such as download.ject, and enables Windows firewalls." Download.ject is a Trojan horse program 10 that attempts to download and install a file by exploiting vulnerabilities in Microsoft's Internet Explorer Web browser. Testing is important. Security features embedded in the upgraded operating system will be turned on by default, for example, and because users are being urged to install SP2 through automatic download, people unfamiliar with security policies could suddenly be faced with having to make vital decisions about their systems' protection. Those default features also could break certain custom applications that agencies have developed.

Category 16.3 *Infrastructure protection & homeland security*

2004-08-16 **cyberterrorism training Homeland Security Arkansas Center Little Rock critical infrastructure protection**

DHS IAIP Daily; http://www.usatoday.com/tech/news/2004−08−16−cyberterror −gra nts−ark_x.htm

August 16, Associated Press — Arkansas center to train officers in cyberterrorism.

Department of Homeland Security Undersecretary Asa Hutchinson announced on Sunday, August 15, a $34 million grant program that will be shared among 14 groups nationwide to counter terrorism. The National Center for Rural Law Enforcement in Little Rock was among the 14 groups that will share in the training grant program. The center is part of the University of Arkansas' Criminal Justice Institute, and was awarded $2.8 million of the total grant to train rural law enforcement officers to recognize cyberterrorism, preserve the physical evidence as they would any crime scene, and notify the appropriate federal agency. Hutchinson said said cyberterrorism presents a threat to the country's security and the operation of utilities, government infrastructure, and commerce. A majority of the nation's power companies report some kind of "cyber attack" at least once a year, he said. The program out of the Little Rock center will address such cybercrime as computer hacking into sensitive files, computer viruses, and the breakdown in water and sewer systems because of a computer adjustment to the controls, he said.

Category 16.3 *Infrastructure protection & homeland security*

2004-08-16 **Internet terrorism information Web scanner detection 95% text based pattern recognition terror content hits surfers**

DHS IAIP Daily; http://www.haaretz.com/hasen/spages/465047.html

August 16, Haaretz (Israel) — Web scanner can detect terror content.

Engineering faculty researchers at Ben-Gurion University (BGU) in Israel reported Sunday, August 15, that they have developed a system that can identify 95 percent of Internet pages with terrorism-related content. The experimental system, which is being developed to detect information regarding terror activity automatically, was designed by Dr. Mark Last of the Department of Systems Information Engineering at BGU, and Prof. Abraham Kandel of the National Institute for Systems Test and Productivity, in the United States. The system is based on the recognition of patterns in texts with terror content, based on examples from existing Internet sites. It uses these patterns to identify "hits" by surfers on other sites with similar characteristics, in order to locate users affiliated with terror organizations and new sites set up by terrorist elements, among other things. According to Last, the development has great importance in view of the considerable use of the Internet in coordinating and orchestrating terror acts. "The lack of ability to enforce limitations on Internet users allows terror organizations to set up Internet sites that spread incitement, raise money in support of terror and find new supporters for their causes," Last said.

Category 16.3 *Infrastructure protection & homeland security*

2004-08-19 **National Institute of Standards and Technology NIST security configuration checklist Windows 2000 2K XP Homeland Security sponsor**

DHS IAIP Daily; http://fcw.com/fcw/articles/2004/0816/web−nist−08−19− 04.asp

August 19, Federal Computer Week — NIST makes lists.

Officials at the National Institute of Standards and Technology (NIST) recently announced that a security configuration checklists program for information technology products, including a logo that vendors can put on their wares, is on track for completion before the end of 2004. A security configuration checklist describes the software options and settings that users can choose to minimize the security risks associated with a particular type of hardware or software. NIST officials will distribute the lists through a Web portal, checklists.nist.gov. NIST officials have already published two security checklists, one for Microsoft Corp.'s Windows 2000 and XP Professional: csrc.nist.gov/itsec. NIST's authority for creating the security checklist program comes from a 2002 law, the Cyber Security Research and Development Act. The Department of Homeland Security is listed on NIST's Website as a program sponsor.

Category 16.3 *Infrastructure protection & homeland security*

2004-08-27 **US ISPs companies terrorist information Website hosting partnership freedom of speech contractual agreement**

DHS IAIP Daily;
http://www.cnsnews.com/ViewForeignBureaus.asp?Page=%5CForeignBureaus%5Carchive%5C200408%5CFOR20040827d.html

August 27, Cybercast News Service — U.S. companies providing indirect service to terrorist websites, report says.

American Internet Service Providers are being used indirectly by the Palestinian Islamic Jihad and other terrorist groups to market their terrorist messages, Israel's Intelligence and Terrorism Information Center at the Center for Special Studies said in a recent report. "Palestinian and international terrorist organizations make massive use of the Internet to spread propaganda supporting terrorism and as a means of maintaining contact between organizations and headquarters, their infrastructures and their target populations," the report said. Two of the companies listed in the report said they were now in the process of correcting the situation. Preference for U.S. and Western companies provides terror groups with "advanced technological support," the ability to "disappear" among the multitudes of Western companies on the Internet -- and to a certain extent, allows protection under U.S. freedom of speech guarantees, the report adds. Brian Marcus, director of Internet monitoring for the Anti-Defamation League in New York, said that laws governing the posting of terrorism-related material on websites fall into a "gray area," but service agreements may enable companies to close down websites. Report: http://www.intelligence.org.il/eng/sib/8_04/internet.htm

---

Category 16.3 *Infrastructure protection & homeland security*

2004-08-30 **New York City information technology IT disaster recovery plan**

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1640674,00.asp

August 30, eWEEK — NY IT prepares for disaster recovery.

As New York City braces for the Republican National Convention (RNC) this week, IT managers at the city's financial services companies may be nervous about the potential for terrorism, but they're prepared. Having learned from the terrorist attacks of September 11, 2001, and the massive power blackout of 2003, many Manhattan-based companies are now hardened with beefed-up disaster recovery initiatives, such as encrypted data backup processes, remote backup facilities and redundant telecommunications systems. While the threat of terrorism has remained somewhat of a constant in New York, the RNC has pushed companies located in the area around Madison Square Garden to aggressively plug any holes in their disaster recovery strategies. The RNC's IT staff said they are ensuring that their own systems remain open at all times. "Our first line of defense is redundancy. Most everyone has a cell and a land line," said Max Everett, director of IT for the RNC. "We're working directly with the Secret Service and US-CERT to ensure our data integrity and network security."

Category 16.3 *Infrastructure protection & homeland security*

2004-08-30 **US states cyberattack alert plan risk assessment color code network security threats Homeland Security**

DHS IAIP Daily; http://www.nwfusion.com/news/2004/083004nastd.html

August 30, Network World — States prepping cyberalert plan.

Looking to gauge the risk of attacks against their networks, state officials this week will vote on new measures that would assess threats and dictate specific actions to take to protect key resources. If adopted, the common alert-level procedures would color-code the threat to state networks and recommend action to take in response to specific threats. The proposed cybersecurity alert system would establish a secure Website state officials could tap to determine why each state has the security ranking it does and whether they should take action based on what other states experience. Homeland security ranked among the key topics considered last week at the National Association of State Telecommunications Directors (NASTD).

Category 16.3 *Infrastructure protection & homeland security*

2004-09-01 **terrorism antiterrorism Homeland Security Al Qaeda technology computers critical infrastructure protection arrests**

DHS IAIP Daily; http://www.pcworld.com/news/article/0,aid,117658,00.asp

September 01, PC World — Al Qaeda's tech traps.

Al Qaeda and other terrorist groups are becoming more technically adept at using the Web and computers. The arrest of alleged Pakistani terrorist Mohammad Naeem Noor Khan, captured this summer with 51 optical discs and three computers full of terror intelligence, is the most recent indicator. For the past ten years, dissidents from the Middle East, Chechnya, and Latin America have used the Internet to further their cause, says Josh Devon, a senior analyst at the SITE Institute, a terrorism research group that monitors the Web. But the proliferation of the Web and the availability of more powerful and affordable graphics and multimedia processing tools have dramatically increased al Qaeda's and other terrorist groups ability to communicate, to broadcast their message, to create public lists of who and what to target, and to train others much more than was possible even five years ago. While technology can make it easier to conceal information and communicate covertly using digital tools such as encryption, it also leaves digital trails of evidence. Computer intelligence found on Khan's computers was instrumental in the arrests of Pakistani and UK terror suspects.

Category 16.3 *Infrastructure protection & homeland security*

2004-09-01 **information security technology human factors terrorism Homeland Security linguistics computation Arabic language**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/27131−1.html

September 01, Government Computer News — The human factor trumps IT in the war on terror.

Computer scientists at the University of Maryland are pushing the technology envelope to assist in intelligence gathering and analysis, but the people using the data may be the limiting factor in its effectiveness. “While there is a lot of good information out there, it isn’t getting to the right people at the right time,” said William J. Lahneman, coordinator of the Center for International and Security Studies in the School of Public Policy. Implementing recent presidential directives on moving data across agency lines will require not only changing IT architectures, but will “challenge the very culture” of those agencies, said James Hendler of the university’s Institute for Advanced Computer Studies. Hendler is focusing on the intelligence needed to use the Web effectively in gathering information and answering questions. The university’s Computational Linguistics and Information Processing Lab is developing more-fluent automated translation systems for languages such as Arabic. Co-director Amy Weinberg said the lab also is working on how to rapidly ramp up systems to handle new languages as new threats develop. Some terrorist groups already are ahead of the government in their use of existing Web technology to win the hearts and minds of people, said Lee Strickland, director of the university’s Center for Information Policy.

Category 16.3 *Infrastructure protection & homeland security*

2004-09-02 **US government agencies software security quality assurance Homeland Security DHS IA Directorate**

DHS IAIP Daily; http://www.infoworld.com/article/04/09/02/HNusgovt_1.html

September 02, IDG News Service — U.S. government agencies aim for software assurance.

U.S. government agencies need to better understand the vulnerabilities of the software they're buying, said IT workers from several government agencies during a software assurance forum in Washington, D.C., last week. The forum, sponsored by the Department of Defense (DoD) and the Department of Homeland Security (DHS), was the first step in a long-term discussion between government agencies and vendors on how to create more secure software, said Joe Jarzombek, deputy director for software assurance in the DoD Information Assurance Directorate. Prompting the forum was "a growing awareness of the fact that we've got a lot of vulnerabilties in the software we're acquiring," said Jarzombek. A major concern among government IT workers is a need to understand how and where software is developed. In many cases, software used by government agencies is developed by outsourced workers, Jarzombek said, and government purchasers need to know that information. Software developers should expect more security demands from customers in the near future, added Mike Rasmussen, principal analyst Forrester Research Inc. Government agencies are under pressure from Congress to improve their cybersecurity, and agencies are moving toward making more security demands of software vendors.

Category 16.3 *Infrastructure protection & homeland security*

2004-09-17 **Department Homeland Security DHS cyber security industry**

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1647410,00.asp

September 17, eWeek — DHS follows industry lead on cyber-terror.

Lawrence Hale, deputy director of the Department of Homeland Security's (DHS) cyber security division, said Friday, September 17, that the DHS depends on the private sector to take the lead in fighting cyber-terrorist threats. "The normal things you do to protect your network will help protect you against cyber-terrorism," he said. Speaking at a conference on cyber-security organized by NBC News and the Northern Virginia Technology Council, Hale said the department is already aware of some cyber-terror threats, as well as the activities of terrorist organizations on the Internet. "They're using cyberspace for recruiting, fund-raising and communication," he said. Private-sector businesses in the United States are already taking the lead in making sure that they are protected against attacks and intrusion, according to Hale -- and the government is following their lead. While he wouldn't divulge details, Hale said the government is working to lessen the severity of any attack on it. He said the fact that most federal departments and agencies design and build their own networks and computer systems makes it less likely that any one type of attack would succeed across the government. He also explained that the department wants to expand its role with private businesses in its fight against cyber terrorism.

Category 16.3 *Infrastructure protection & homeland security*

2004-09-19 **cyberterrorism information Internet Website identification algorithm Ben-Gurion University BGU**

DHS IAIP Daily; http://www.jpost.com/servlet/Satellite?pagename=JPost/JPArti
cle/ShowFull&cid=1095565998846

September 19, Jerusalum Post (Israel) — Algorithms can identify cyber-terrorism.

Professor Mark Last of the Ben-Gurion University (BGU) department of information systems engineering is working on ways to make terrorist's communication on the Internet more difficult by conducting pioneering research on fighting terror in cyberspace. "The Internet helps terrorists a great deal, and makes their life easier in many senses -- because it is really a very difficult problem to find something suspicious in the sea of traffic. Access to the Internet is relatively easy and affordable worldwide, and it is easy to use while concealing your identity," Professor Last says. His team has developed an experimental system that succeeded in identifying about 95% of Web pages with a terrorist content. Last's cooperation with colleagues at the University of South Florida led to the U.S. National Institute of Systems Test and Productivity in Florida getting involved in the subject. His lab is now working as a subcontractor for the National Institute to design methods that will enable government agencies and commercial companies to improve security, quality and cost effectiveness of large-scale information systems, with a focus on cyber-terror. Their ability to distinguish cyber-terror activity from normal activity is becoming increasingly more reliable thanks to changes in the algorithms.

Category 16.3 *Infrastructure protection & homeland security*

2004-10-01 **US Department Homeland Security cybersecurity chief Amit Yoran resignation**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/articles/A64915−
2004Oct 1.html

October 01, Associated Press — U.S. cybersecurity chief resigns.

The government's cybersecurity chief has abruptly resigned after one year with the Department of Homeland Security. Amit Yoran informed the White House about his plans to quit as director of the National Cyber Security Division and made his resignation effective at the end of Thursday, September 30. Yoran said he "felt the timing was right to pursue other opportunities." It was unclear immediately who might succeed him even temporarily. Yoran's deputy is Donald "Andy" Purdy, a former senior adviser to the White House on cybersecurity issues.

Category 16.3 *Infrastructure protection & homeland security*

2004-10-05 **critical infrastructure protection control systems vulnerable report hackers viruses**

DHS IAIP Daily;
http://www.forbes.com/business/feeds/ap/2004/10/05/ap1577435 .html

October 05, Associated Press — Experts say control systems vulnerable. Businesses and government agencies must re-examine the growing threat of cyberterrorism to automated computer systems running power grids, dams and other industrial facilities, security experts said at a conference Tuesday, October 5. From 1982 until about 2000, problems with such systems usually were associated with internal accidents or inappropriate employee behavior, said Eric Byres, manager of Critical Infrastructure Security Research at the British Columbia Institute of Technology. But a review by Byres of the last three years showed that 90 percent of these problems come from break-ins by hackers and computer viruses.

Category 16.3 *Infrastructure protection & homeland security*

2004-10-07 **schools terrorism data loss information warfare surveillance threat Iraq**

NewsScan; http://www.usatoday.com/tech/news/2004-10-07-school-disk_x.htm

TERROR IN THE INFORMATION AGE

Law enforcement authorities have notified school districts in six states that a computer disc found by the U.S. military in Iraq contained photos, floor plans and other information about their schools. The officials say there is no evidence of any specific plans to stage Beslan-like terrorist attacks on the schools, which are in Georgia, Florida, Michigan, New Jersey, Oregon and California. Schools have been urged to watch for various activities which, though legitimate on their own, which may suggest a threat if many of them occur together: interest in obtaining site plans for schools, bus routes and attendance lists; prolonged "static surveillance" by people disguised as panhandlers, shoe shiners, newspaper or flower vendors or street sweepers not previously seen in the area; observation of security drills; and so forth. Clevelandbased school safety consultant Kenneth Trump says: "It's a positive sign that they're finally discussing this after years of downplaying or denying even the possibility of a terrorist strike on schools. Public officials are in fear of creating fear, but we have to put the cards on the table, educate people in the school community and make sure they are well prepared."

Category 16.3 *Infrastructure protection & homeland security*

2004-10-08 **Municipal Websites information terrorism clues weakness disclosure**

DHS IAIP Daily; http://washingtontimes.com/metro/20041007−113112−4486r.htm

October 08, Washington Times — Municipal Websites may help terrorists plot attacks.

Too many details on municipal Websites can tip off terrorists to security weaknesses and vulnerable targets, a military researcher told a conference of U.S. mayors in Washington, D.C. on Thursday, October 7. Gerald G. Brown, distinguished professor of operations research at the Naval Postgraduate School in Monterey, CA, said municipal leaders must not confuse "sunshine" laws, which require public access to some government data, and the allure of "really cool Websites." Brown said that seemingly innocuous information, such as budget data, can become fodder for terrorist plots. "Frequently these sites are used to ask for things: 'We need a firetruck. We need a Hazmat crew,' " Brown said. "If I'm attacking you, that's pretty good information."

Category 16.3 *Infrastructure protection & homeland security*

2004-10-10 **Terrorism Knowledge Base terrorist information collection FBI CIA Rand Corporation Department Homeland Security funding**

DHS IAIP Daily; http://www.chicagotribune.com/technology/chi−0410100381oct10 ,1,6912082.story?coll=chi−techtopheds−hed

October 10, Chicago Tribune (IL) — Site tracks and charts terrorism information.

The Terrorism Knowledge Base, an online database available at http://www.tkb.org includes detailed reports on more than 18,000 terrorist incidents and nearly 1,000 terrorist groups and their leaders dating back to 1968. The database is still in its final shakedown stage, but it is already available for public use. Created by the National Memorial Institute for the Prevention of Terrorism in Oklahoma City, the database represents the largest repository of international terrorism information ever made publicly available on the Internet. Information sources include the FBI, the CIA and the Rand Corporation, a non-profit research think tank that for the first time is making its proprietary terrorism incident database--long regarded by government experts and scholars as the world's most extensive--available to the public. The Department of Homeland Security is providing some of the funding to support the project. The intended audience ranges from citizens curious about terrorism to journalists, researchers, intelligence and law-enforcement agencies, and even spies in the field working clandestine assignments.

Category 16.3 *Infrastructure protection & homeland security*

2004-10-11 **chat-room instant messaging IM surveillance anti-terrorism RPI professor Bulent Yener chatter pattern recognition algorithm National Science Foundation NSF grant**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/articles/A25272−2004Oct 11.html

October 11, Associated Press — U.S. funds chat-room surveillance study.

The U.S. government is funding a yearlong study on chat room surveillance under an anti-terrorism program. A Rensselaer Polytechnic Institute computer science professor hopes to develop mathematical models that can uncover structure within the scattershot traffic of online public forums. Professor Bulent Yener will use mathematical models in search of patterns in the chatter. Downloading data from selected chat rooms, Yener will track the times that messages were sent, creating a statistical profile of the traffic. "For us, the challenge is to be able to determine, without reading the messages, who is talking to whom," Yener said. The $157,673 grant comes from the National Science Foundation's Approaches to Combat Terrorism program. It was selected in coordination with the nation's intelligence agencies.

Category 16.3 *Infrastructure protection & homeland security*

2004-10-14 **state local homeland security IT program need federal guidance**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/27632−1.html

October 14, Government Computer News — CIOs: State and local homeland security IT needs more federal guidance.

State and local homeland security IT programs would be more effective if the federal government provided firmer standards and practices, senior federal officials said Thursday, October 14. Department of Homeland Security (DHS) CIO Steve Cooper, Justice Department CIO Vance Hitch and other high-level officials who spoke at an Industry Advisory Council meeting in Washington, D.C. agreed on the point. Cooper said he and Hitch should provide additional leadership to state and local governments on technology issues. Cooper noted that he was not necessarily talking about specific industry standards, but "the technology directions and the policies." DHS' state and local office has a weekly videoconference with state and local advisors, but that information may not reach all 89,000 municipalities, Cooper said.

Category 16.3 *Infrastructure protection & homeland security*

2004-10-15 **Canadian anti-terrorism cyberterrorism force NSA Communications Security Establishment CSE**

DHS IAIP Daily; http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/1097878208404_93287408/?hub=SciTech

October 15, Canadian Press (Ottawa) — Canada creates new force to fight cyber-terrorism.

A high-level national task force is being assembled to help Canada steel its defenses against potential cyber-attacks by terrorists. The head of Canada's electronic spy agency said the panel of private- and public-sector officials will help the country catch up to the United States in securing cyberspace. Communications Security Establishment (CSE) chief Keith Coulter noted Washington has already begun moving to protect their own key grids and networks. CSE, perhaps Canada's most secretive agency, has the dual role of helping protect crucial information-technology systems and eavesdropping on foreign communications. CSE and agencies in the United States, Britain, Australia and New Zealand share intercepted communications of interest with one another. Of particular importance is CSE's relationship with its American counterpart, the National Security Agency (NSA), Coulter said. "CSE and NSA share intelligence, tackle common problems posed by changing technology and track threats to our collective security."

Category 16.3 *Infrastructure protection & homeland security*

2004-10-19 **information security federal networks meeting DHS standards report**

DHS IAIP Daily; http://www.gao.gov/cgi−bin/getrpt?GAO−04−375

October 19, Government Accountability Office — GAO-04-375: Information Technology: Major Federal Networks That Support Homeland Security Functions (Report).

A key information systems challenge in homeland security is ensuring that essential information is shared in a timely and secure manner among disparate parties in federal, state, and local governments, and in the private sectors. This requires communications networks that provide information-sharing capabilities between the various levels of government—federal, state, and local. The Government Accountability Office's (GAO) objective was to identify and describe, through agency reporting, major networks and examples of applications that the agencies considered important in supporting their homeland security functions. Nine agencies identified 34 major networks that support homeland security functions -- 32 that are operational and two that are being developed. Of these 34, 21 are single-agency networks designed for internal agency communications. Six of the 34 are used to share information with state and local governments; four share information with the private sector. Highlights: http://www.gao.gov/highlights/d04375high.pdf

---

Category 16.3 *Infrastructure protection & homeland security*

2004-10-27 **Department Homeland Security DHS German Interior Ministry multilateral conference cyber security watch warning incident response**

DHS IAIP Daily; http://www.dhs.gov/dhspublic/display?content=4077

October 27, Department of Homeland Security — Homeland Security and German Interior Ministry co-host multilateral conference on cyber security.

The U.S. Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) Directorate and the German Ministry of the Interior co-hosted a multilateral conference in Berlin October 20-22, 2004, on International Cyber Security Cooperation: Watch, Warning, and Incident Response. The conference consisted of delegations from fifteen countries including those from Europe, Asia Pacific and the Americas and represented a significant collaborative effort on the need for an international framework for cyber information sharing and incident response. The goal of the conference was to bring together government cyber security policy makers, managers of Computer Security Incident Response Teams (CSIRTs) with national responsibility, and members of the cyber law enforcement community. During the conference the participating countries discussed critical areas essential for building an international framework for cyber security, including: an arrangement among sovereign states to exchange cyber information, the incorporation of existing and emerging regional information sharing arrangements, and ways to improve information sharing in the near term and in the future.

Category 16.3 *Infrastructure protection & homeland security*

2004-10-27 **database forged identities art cross border Rules of Crime Homeland Security DHS concern**

DHS IAIP Daily;
http://www.nytimes.com/2004/10/27/arts/design/27iden.html?or ef=login

October 27, New York Times — How to cross borders, social or otherwise.

Heath Bunting and Kayle Brandon, two British artists, are compiling a database exploring elements of legal status in Britain, with the ultimate goal of allowing people to create a new identity from information collected on the Internet. The first stage of their project is the focus of "Rules of Crime," a show that runs through November 13 at the New Museum of Contemporary Art's temporary home in Chelsea, NY. In its final form, their project may be viewed as the Homeland Security Department's worst nightmare: a road map enabling all sorts of undesirables to penetrate a nation's borders, banking systems, supermarket loyalty clubs. Bunting and Brandon are among a growing number of artists who are harnessing technologies associated with governments and corporations to challenge the status quo. The Website for their project, known as the Status Project (http://status.irational.org) says it will eventually provide a how-to guide to getting a passport. The Status Project grew out of BorderXing, in which the artists documented illegal treks they made across European borders. The BorderXing Website, available for individual use by request (http://irational.org/cgi-bin/border/clients/deny.pl) offers pictures, suggested routes and tips for evading the authorities.

Category 16.3 *Infrastructure protection & homeland security*

2004-10-28 **do not fly list airport TSA Transportation Safety Authority Kabay DNFL false positives authentication correction failure homeland security terrorism**

NewsScan; Ubiquity

DO-NOT-FLY LISTS: DO-NOT-TAKE-SERIOUSLY!

The current issue of Ubiquity, an online publication of the ACM (edited by the editors of NewsScan), contains an article by Norwich University professor M.E. Kabay arguing that "the current implementation of do-not-fly lists and the use of documents to authenticate passenger identity won't necessarily improve airport security." A sample: "Deirdre McNamer (how appropriate) wrote a story in The New Yorker magazine in October 2002 about a 28-year-old pinko-gray-skinned, blue-eyed, red-blond-haired criminal called Christian Michael Longo who used the alias 'John Thomas Christopher.' His alias was placed on the DNFL used by the Transportation Security Administration. He was arrested in January 2002 but his alias was not removed from the DNFL. On March 23, 2002, 70-year-old brown-skinned, dark-eyed, gray-haired grandmother Johnnie Thomas was informed that she was on the master terrorist list and would have special security measures applied every time she flew. Indeed, the poor lady found that she was repeatedly delayed by a scurry of activity when she presented her tickets at an airline counter, extra X-rays of her checked baggage, supplementary examination of her hand-baggage and extra wanding at the entrance gates. On one occasion she was told that she had graduated to the exalted status labeled, 'Not allowed to fly.' She discovered that there was no method available for having 'her' name removed from the DNFL; indeed, one person from her local FBI office dismissively told her to hire a lawyer (although ironically, he refused to identify himself). An employee of the TSA informed her that 'four other law-abiding John Thomases had called to complain.'" (Ubiquity 28 Oct 2004)

Category 16.3 *Infrastructure protection & homeland security*

2004-11-02 **computer data terrorism information extensible markup language XML metadata standard Homeland Security DHS FBI DoJ**

DHS IAIP Daily; http://www.fcw.com/fcw/articles/2004/1101/web−terrorxml−11−0 2−04.asp

November 02, Federal Computer Week — Standardizing terror data.

Government officials crafting proposals for cross-agency counterterrorism information sharing plan to assign stewardship over a core set of Extensible Markup Language (XML) standards. Members of the Information Systems Council will identify XML standards and people responsible for them, said Bill Dawson, intelligence community deputy chief information officer at the CIA. Final plans are due to the president by December 24. Metadata standards enabling the widest possible dissemination of intelligence information are required under Section 3 of Executive Order 13356. On September 20, officials connected four previously incompatible systems -- the FBI's Law Enforcement Online network, the Justice Department's Regional Information Sharing System, the Homeland Security Network and a criminal intelligence network in California.

Category 16.3 *Infrastructure protection & homeland security*

2004-11-04 **cybercrime hacker hiring FBI crime list 10 Best Wanted**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/articles/A25579−2004Nov 4.html

November 04, Washington Post — More cyber-crime cases added to FBI list.

A former technology company executive charged with hiring hackers to attack a competitor's Website has joined the FBI's most-wanted list, the latest sign of the federal law enforcement agency's growing interest in cyber-crime. The most-wanted list is a group of more than a dozen people that includes some of America's most elusive criminals. It includes alleged embezzlers, an accused child pornographer and individuals indicted on drug and murder charges. The most-wanted list is not the same list as the notorious "10 Most Wanted," rather it is a list that the bureau started almost five years ago on its Website to nab suspects who are less of a threat or less prone toward physical violence, said spokesperson Paul Bresson. "This is the first time we've had such a significant number of people being investigated and prosecuted for computer crime," said Mark Rasch, a former prosecutor in the Justice Department's computer crimes and intellectual property section. "And we're only going to see this trend continue because investigators are getting better at identifying these individuals," said Rasch. The list, which currently includes 16 suspects, is located at http://www.fbi.gov/mostwant/alert/alert.htm

---

Category 16.3 *Infrastructure protection & homeland security*

2004-11-08 **counter terrorism data sharing extensible markup language XML Department Homeland Security DHS**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/27854−1.html

November 08, Government Computer News — Counterterror data sharing will rely on XML.

The Department of Homeland Security (DHS) will tweak the new Data Reference Model (DRM) to create a data model for the exchange of counterterrorism data. Under Executive Order 13356, DHS data architect Michael Daconta is leading a revision of the Federal Enterprise Architecture's 30-page DRM to share counterterrorism data while preserving individual privacy. At a meeting of the Association for Information and Image Management's National Capital Chapter in Arlington, VA, last week, Daconta said he is looking seriously at the way the Global Justice XML data model would handle metadata about agencies' watch lists. "XML is neutral" on concepts such as watch lists' heterogeneous collections, Daconta said, but it can bridge documents and data because its primary job is information exchange. Use of federated queries will require a standard governmentwide identifier for persons of interest, as well as a central registry for the metadata, Daconta said.

Category 16.3 *Infrastructure protection & homeland security*

2004-11-30 **Department Homeland Security DHS computer data network progress advance testing and accreditation SIPRNET**

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml;jsess ionid=XC2WBO3X2RJCIQSNDBCCKH0CJUMEKJVN?articleID=54201030

November 30, InformationWeek — Homeland Security Network advances.

The Homeland Security Department is moving forward with its plans to create a data network accessible to intelligence analysts and law enforcement across federal, state, and local boundaries. Homeland Security is moving into the testing and accreditation phase of its Homeland Secure Data Network, first introduced in April. The secure network, which could cost up to $350 million to create, will initially connect Homeland Security intelligence personnel with the Defense Department's Secret Internet Protocol Router Network (SIPRNET) to send and receive information with classified security levels. Initiatives also are under way to next year connect Homeland Security, the Defense Department, and areas within the FBI and the greater intelligence community, including the CIA.

Category 16.3 *Infrastructure protection & homeland security*

2004-12-03 **CIA Central Intelligence Agency Tenet cybersecurity concerns worries issues vulnerabilities homeland security terrorism**

NewsScan;
http://www.washingtontimes.com/functions/print.php?StoryID=20041201-114750-6381r

EX-CIA CHIEF WORRIES ABOUT INTERNET SECURITY

Former CIA Director George J. Tenet sees the Internet as "a potential Achilles' heel" in the fight against terrorism, endangering "our financial stability and physical security if the networks we are creating are not protected." Calling for new cybersecurity measures, Tenet says: "I know that these actions will be controversial in this age when we still think the Internet is a free and open society with no control or accountability, but ultimately the Wild West must give way to governance and control." He believes that access to the Web might need to be limited to those who can show they take security seriously. (UPI/Washington Times 3 Dec 2004)

Category 16.3 *Infrastructure protection & homeland security*

2004-12-06 **committee cybersecurity post Department of Homeland Security DHS recommendation**

DHS IAIP Daily; http://www.fcw.com/fcw/articles/2004/1206/web−dhs−12−06−04.a sp

December 06, Federal Computer Week — Committee pushes for cybersecurity post.

Members of the House Select Homeland Security Committee have recommended establishing a new assistant secretary position within the Homeland Security Department (DHS) to better integrate and coordinate cybersecurity issues. The recommendation is one of six suggestions listed in a new 41-page, bipartisan report that was released today by the committee's cybersecurity subcommittee. The report stated that although DHS officials have created the National Cyber Security Division and several other coordination entities, "now is the time to build toward more robust capabilities." It also stated DHS officials need to exert more effort to work with the private sector and across critical infrastructure sectors in addition to state and local governments. Report: http://hsc.house.gov/files/cybersecurityreport12.06.04.pdf

---

Category 16.3 *Infrastructure protection & homeland security*

2004-12-07 **cybersecurity serious attention computer security firms report CSIA research and development R&D Department Homeland Security DHS**

DHS IAIP Daily; http://news.com.com/Cybersecurity+post+needs+a+promotion%2C+firms+say/2100−7348_3−5481497.html

December 07, CNET News — Cybersecurity post needs a promotion, firms say.

The U.S. government is not taking cybersecurity seriously enough and should spend more money and energy on the topic, a group of computer security firms said Tuesday, December 7. At an event in Washington, DC, members of the Cyber Security Industry Alliance (CSIA) warned of the potential dangers of Internet attacks and called on the next Bush administration to create a new assistant secretary position inside the Department of Homeland Security, ratify the Council of Europe's cybercrime treaty, create an emergency coordination network to handle Internet outages, increase R&D funding for cybersecurity, and designate a federal agency to track the costs of cyberattacks. CSIA members include Check Point Software Technologies, McAfee, Symantec, Entrust, PGP and Computer Associates.

Category 16.3 *Infrastructure protection & homeland security*

2004-12-08 **government homeland security cybersecurity support**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A45622-2004Dec7.html

GROUP URGES GOVERNMENT TO FOCUS ON CYBERSECURITY

The Cyber Security Industry Alliance is calling on the Bush administration to beef up its cybersecurity operations, starting with elevating the position of national cybersecurity director to assistant secretary level. "There is not enough attention on cybersecurity within the administration. The executive branch must exert more leadership," says Alliance director Paul B. Kurtz, who's a former senior cybersecurity official in the Bush administration. Kurtz was joined by Amit Yoran, the former director of Homeland Security's National Cyber Security Division who resigned in September. Meanwhile, a provision in the recently passed intelligence overhaul bill that would have raised cybersecurity's profile in the Homeland Security Department was stripped out before passage. The Alliance's recommendations mirror those outlined in a report issued Monday by the House subcommittee on cybersecurity, which also calls for the administration to consider tax breaks and other incentives for businesses that make computer security a top priority. In addition, both groups are urging the Homeland Security Department to take the lead in creating a disaster recovery and response plan, should the U.S. suffer debilitating digital sabotage. (Washington Post 8 Dec 2004)

Category 16.3 *Infrastructure protection & homeland security*

2004-12-10 **cybersecurity office Department of Homeland Security DHS IAIP CSIA proposal recommendation**

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1739061,00.asp

December 10, eWeek — Cyber-security office moving ahead.

The office in charge of cyber-security in the Department of Homeland Security (DHS) is planning to continue moving ahead on the agenda the agency has already set. According to Lawrence Hale, deputy director of the National Cyber-Security Division at DHS, the agency considers physical and cyber-security so deeply intertwined that it would be impossible to separate them. Hale said the current organization of the IAIP (Directorate of Information Analysis and Infrastructure Protection) has cyber-security and physical security working together. Earlier this week, the CSIA (Cyber-Security Industry Alliance) released a series of recommendations, including a reorganization that would make the director of the cyber-security division an assistant secretary. Supporters say such a change would raise the profile of cyber-security, thus bringing the area more clout and more funding. While Hale said he thinks CSIA's proposals are an important means to raise the visibility of cyber-security, he doesn't agree that cyber-security should be treated differently from physical security. But he said he thought the CSIA meeting in Washington, DC where the recommendations were presented was helpful.

Category 16.3 *Infrastructure protection & homeland security*

2005-01-07 **Feds national plan DHS Homeland Security government state local tribal private emergency prevention response recovery**

EDUPAGE; http://www.fcw.com/fcw/articles/2005/0103/web-response-01-06-05.asp

FEDS LAUNCH NATIONAL RESPONSE PLAN

The Department of Homeland Security has released a plan that directs how the federal government is to work with state, local, and tribal governments, as well as with the private sector, in the event of a national emergency. The National Response Plan is rooted in the National Incident Management System, which is currently under development by the Federal Emergency Management Agency and is expected to be complete by the end of fiscal 2007. The National Response Plan establishes standards for training and organization. In addition, it outlines protocols for handling incidents that span various jurisdictions, with the goal of helping officials at all levels of government better coordinate their responses despite widely varying technologies used in prevention, response, and recovery efforts.

Category 16.3 *Infrastructure protection & homeland security*

2005-02-02 **Department of Homeland Security DHS privacy office first report Congress biometric sensor network technology**

DHS IAIP Daily; http://www.fcw.com/fcw/articles/2005/0131/web-dhs-02-02-05.asp

DEPARTMENT OF HOMELAND SECURITY PRIVACY OFFICE ISSUES FIRST ANNUAL REPORT

Department of Homeland Security (DHS) officials on Wednesday, February 2, released DHS' first annual privacy report to Congress, outlining work done in numerous areas, including technology. A primary goal of the department's privacy office, which is the first Congressionally mandated one for a federal agency, is ensuring that technologies sustain "privacy protections relating to the use, collection, and disclosure of personal information," according to the 112-page report. The office is examining use of biometric technology, radio frequency identification devices, data mining, and distributed data environments -- where data is shared with users, but remains with the owner. The privacy office is also considering the effect of emerging technologies, including geospatial information systems and services, unmanned aerial vehicles, and ubiquitous sensor networks, which may potentially raise separate privacy protection concerns, according to the report. Report: http://www.dhs.gov/dhspublic/interweb/assetlibrary/privacy_a nnualrpt_2004.pdf

---

Category 16.3 *Infrastructure protection & homeland security*

2005-02-18 **Department Homeland Security DHS regional technology initiative Seattle local government cybersecurity readiness**

DHS IAIP Daily; http://www.dhs.gov/dhspublic/display?content=4362

HOMELAND SECURITY LAUNCHES REGIONAL TECHNOLOGY INTEGRATION INITIATIVE IN SEATTLE

The Department of Homeland Security on Friday, February 18, announced the addition of a new urban area to its Regional Technology Integration (RTI) initiative, which focuses on speeding the effective integration of innovative technologies and organizational concepts to the homeland security efforts of regional, state, and local jurisdictions. Through the program, managed by Homeland Security's Science & Technology directorate, four urban areas across the country have now been announced as the initial pilot locations for this program. The Seattle, Washington urban area joins Memphis, Tennessee; Anaheim, California; and Cincinnati, Ohio, as the pilot locations. These initial locations will provide the science and technology community with a realistic environment to test maturing hardware and concepts. The program will also provide information on how best to choose, deploy, and manage these technologies to strengthen the security posture of these and other communities. The goal of Homeland Security's Regional Technology Integration initiative is to facilitate the successful transfer and integration of existing and advanced homeland security technology systems to local governments in order to improve their preparedness and response.

Category 16.3 *Infrastructure protection & homeland security*

2005-02-22 **federal government preparedness exercise Department of Homeland Security DHS RSA conference San Francisco**

DHS IAIP Daily; http://www.fcw.com/fcw/articles/2005/0221/web−cyber−02−22−05 .asp

FEDERAL GOVERNMENT TO HOLD CYBER PREPAREDNESS EXERCISE

The federal government and several international partners will hold a cyber preparedness exercise in November, Department of Homeland Security (DHS) officials said at the RSA Conference in San Francisco last week. Its purpose is to give federal agencies an opportunity to test their plans for responding to a direct or indirect attack on the computer networks that control the nation's critical infrastructure such as power plants and oil pipelines. The exercise will be unclassified, and the public will be informed, said Hun Kim, deputy director of the National Cyber Security Division at DHS. The RSA Conference brings together IT professionals from industry, academia, and government to share information and exchange ideas on technology trends and best practices in IT security.

Category 16.3 *Infrastructure protection & homeland security*

2005-03-01 **Department Homeland Security DHS Justice DoJ Extensible Markup Language XML information exchange sharing Collaboration on Objects for Reuse and Exchange**

DHS IAIP Daily; http://www.fcw.com/fcw/articles/2005/0228/web−dhsdoj−03−01−0 5.asp

DEPARTMENTS OF HOMELAND SECURITY AND JUSTICE WORK ON XML MODEL TO HELP SHARE INFORMATION

Department of Homeland Security (DHS) and Department of Justice officials have a new partnership to enhance development of an Extensible Markup Language (XML) model that could save federal, state, local and tribal agencies billions of dollars as they improve their computer systems to share information with one another. Officials said this represents a significant step in broadening the use of the Global Justice XML Data Model, which was started about three years ago, across the federal government. It could mean future partnerships with other departments, such as Transportation and Health and Human Services, and the intelligence community, which used the model as the basis for a schema to share the terrorism watch list. XML is essentially an open standard or translator that systems can use to communicate with one another. Development of the core model would ensure long-term stability of the model and ensure that early efforts in its use are not wasted. The information-sharing initiative is called the Collaboration on Objects for Reuse and Exchange.

Category 16.3 *Infrastructure protection & homeland security*

2005-03-18 **cybersecurity report prioritization government advisory committee vulnerabilities recommendations**

RISKS; http://www.nitrd.gov/pubs/ 23 81

PRESIDENT'S INFORMATION TECHNOLOGY ADVISORY COMMITTEE RELEASES NEW REPORT -- CYBER SECURITY: A CRISIS OF PRIORITIZATION

Vital to the Nation's security and everyday life, the information technology (IT) infrastructure of the United States is highly vulnerable to disruptive domestic and international attacks, the President's Information Technology Advisory Committee (PITAC) argues in a new report. While existing technologies can address some IT security vulnerabilities, fundamentally new approaches are needed to address the more serious structural weaknesses of the IT infrastructure.

In Cyber Security: A Crisis of Prioritization, PITAC presents four key findings and recommendations on how the Federal government can foster new architectures and technologies to secure the Nation's IT infrastructure. PITAC urges the Government to significantly increase support for fundamental research in civilian cyber security in 10 priority areas; intensify Federal efforts to promote the recruitment and retention of cyber security researchers and students at research universities; increase support for the rapid transfer of Federally developed cyber security technologies to the private sector; and strengthen the coordination of Federal cyber security R&D activities.

To request a copy of this report, please complete the form at http://www.nitrd.gov/pubs/, send an e-mail to nco@nitrd.gov, or call the National Coordination Office for Information Technology Research and Development at (703) 292-4873. Cyber Security: A Crisis of Prioritization can also be downloaded as a PDF file by accessing the link at http://www.nitrd.gov/pubs/.

About PITAC

The President's Information Technology Advisory Committee (PITAC) is appointed by the President to provide independent expert advice on maintaining America's preeminence in advanced information technology. PITAC members are IT leaders in industry and academia representing the research, education, and library communities, network providers, and critical industries, with expertise relevant to critical elements of the national IT infrastructure such as high-performance computing, large-scale networking, and high-assurance software and systems design. The Committee's studies help guide the Administration's efforts to accelerate the development and adoption of information technologies vital for American prosperity in the 21st century.

Contact: "Alan S. Inouye 1-703-292-4540" <inouye@nitrd.gov>

Category 16.3 *Infrastructure protection & homeland security*

2005-03-21 **IT infrastructure cybersecurity criticism Presidential committee Cyber Security: A Crisis of Polarization report**

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml?artic leID=159903541&t

PRESIDENTIAL COMMITTEE CRITICIZES IT INFRASTRUCTURE SECURITY

The President's IT Advisory Committee (PITAC) on Friday, March 18, released the results of a report, "Cyber Security: A Crisis Of Prioritization," criticizing the country's IT infrastructure as highly vulnerable to attack by terrorists and cybercriminals. "The IT infrastructure is highly vulnerable to premeditated attacks with potentially catastrophic effects," committee chair Marc Benioff and co-chair Edward Lazowska wrote in a February 28 letter to President Bush. This infrastructure includes the public Internet as well as power grids, air-traffic-control systems, financial systems, and military and intelligence systems, they add. The committee comprised of IT leaders and academia, makes four key recommendations to help curb security exposures and provide long-term IT infrastructure stability: increase federal support for fundamental research in civilian cybersecurity; intensify federal efforts to promote recruitment and retention of cybersecurity researchers and students at research universities; provide increased support for the rapid transfer of federally developed, cutting-edge cybersecurity technologies to the private sector; and, better federal coordination of cybersecurity R&D. Report: http://www.itrd.gov/pitac/reports/20050301_cybersecurity/cyb ersecurity.pdf

---

Category 16.3 *Infrastructure protection & homeland security*

2005-03-22 **British intelligence warning Internet cyber attack UK computer critical infrastructure protection network counter terrorism al Qaeda**

DHS IAIP Daily; http://thescotsman.scotsman.com/index.cfm?id=305582005

BRITISH INTELLIGENCE WARNS OF POSSIBLE CYBER ATTACK IN UK

International terrorists are training to launch cyber-terror attacks on Britain which could cripple vital economic, medical and transport networks, the government's counter-terrorism coordinator said Monday, March 21. Sir David Omand, one of the most senior members of the British intelligence community, said surveillance of suspected al Qaeda affiliates suggests they are working to use the Internet and other electronic communications systems to cause harm. Intelligence officials say that no matter how much the state does to prepare for cyber-terrorism, a great deal will rest on the willingness of the private sector to "harden" their systems against attack. Britain has not yet experienced genuine acts of cyber-terrorism, but Sir David said intelligence chiefs are in little doubt that the country must be ready for such an attack. The authorities' greatest fears about electronic attacks relate to the more exposed networks that make up what is known as "critical national infrastructure", many of which are in civilian hands. The global nature of the Internet means the threat from cyber-attacks is equally international, forcing British agents to work closely with nations they say they would often regard with suspicion or even hostility.

Category 16.3 *Infrastructure protection & homeland security*

2005-03-25 **data confidentiality government agency homeland security transportation safety agency inspector general audit safeguards failures**

RISKS; http://tinyurl.com/cu56e 23 81

DHS FAILED TO PROTECT PASSENGER DATA IN TSA'S CAPPS 2 TESTS

Richard M. Smith reported on questionable data safeguards in the DHS:

A new government report says officials in the Department of Homeland Security didn't do enough to keep airline-passenger data secure when using it to test a traveler-screening program. DHS's Inspector General says the Transportation Security Administration gathered 12 million passenger records from February 2002 to June 2003 and used most of them to test the Computer Assisted Passenger Prescreening System, or CAPPS 2, which was designed to check passenger names against government watch lists. Passengers weren't told their information was being used for testing. TSA officials shelved CAPPS 2 last year amid complaints it was an invasion of passenger privacy. The agency has replaced it with a similar system, called Secure Flight, which is being tested and is expected to debut in August.

The report raises concerns because Secure Flight ultimately will gather private information, such as names, addresses, travel itineraries and credit-card information, on anyone who takes a domestic flight. That effort could be slowed by a Government Accountability Office study due Monday which is expected to be critical of TSA's efforts to develop passenger-privacy protections.

The report said TSA "did not ensure that privacy protections were in place for all of the passenger data transfers" and noted that "early TSA and [CAPPS 2] efforts were pursued in an environment of controlled chaos and crisis mode after the Sept. 11 attacks."

Investigators also found TSA provided inaccurate information to the media about the agency's use of real passenger records for CAPPS 2 testing and wasn't "fully forthcoming" to the agency's own internal privacy officer during an investigation into the matter. "Although we found no evidence of deliberate deception, the evidence of faulty processes is substantial," investigators said.

Category 16.3 *Infrastructure protection & homeland security*

2005-04-04 **cyber terrorism analyst warning counterterrorism national cyber event critical infrastructure InfoSec World 2005 voice over Internet protocol VoIP**

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1782286,00.asp

CYBER-TERRORISM ANALYST WARNS AGAINST COMPLACENCY

Cyber-security and counterterrorism analyst Roger Cressey on Monday, April 4, pleaded with IT executives not to underestimate the threat of "national cyber-event" targeting critical infrastructure in the United States. During a keynote address at the InfoSec World 2005 conference, Cressey warned against discounting the danger of the Internet being used in a terrorist-related attack. "It may not be a terrorist attack, but a cyber-event is a very, very serious possibility. When it happens, it will have serious economic impact on our critical infrastructure." Cressey, who served as chief of staff to the president's Critical Infrastructure Protection Board at the White House, said there was enough evidence that U.S. enemies were actively using the Web to recruit, organize and communicate terrorism activities. Cressey, the on-air counterterrorism analyst for NBC News, said the rapid rate in which Internet security vulnerabilities was being detected only adds to the worry. Cressey used part of his keynote to call on VoIP (Voice over Internet Protocol) developers to put security on the front burner. Describing VoIP security as the great challenge of this decade, he said it would be a "big mistake" for another nascent industry to emerge without built-in protections.

Category 16.3 *Infrastructure protection & homeland security*

2005-04-06 **Department Homeland Security DHS privacy issues briefing personal data theft abuse anti-terrorism**

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml?articleID=160501384

COMMITTEE TO INFORM DHS ON PRIVACY ISSUES

A new group of public- and private-sector leaders in academia, business, and technology met Wednesday, April 6, in Washington, DC, to help the Department of Homeland Security (DHS) gain a greater understanding of how IT can be used to fight terrorism without exposing personal data to theft or abuse. The department's Data Privacy and Integrity Advisory Committee launched with a statement of mission and the selection of its inaugural chairman and vice chairwoman. Paul Rosenzweig, the committee's new chairman and a senior legal research fellow at the Heritage Foundation, said that the committee's greatest challenge will be helping the department as a whole focus on preserving individual freedoms while tightening security, and doing this in a public way. The committee will serve to inform DHS about privacy concerns related to all of the department's various agencies and directorates, which protect the nation's borders, waterways, and critical infrastructure. DHS Privacy Office: http://www.dhs.gov/privacy

---

Category 16.3 *Infrastructure protection & homeland security*

2005-04-18 **European Union EU information technology IT critical infrastructure study CI2RCO project national security protection**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/story/0,10801,101160,00.html

EU TASK FORCE TO STUDY IT CRITICAL INFRASTRUCTURE

The European Union has set up a task force to explore what its 25 member states are doing to combat cyberthreats against the region's critical infrastructure. As part of the EU's Critical Information Infrastructure Research Coordination (CI2RCO) project, announced Friday, April 15, the task force aims to identify research groups and programs focused on IT security in critical infrastructures, such as telecommunications networks and power grids. "We want to bring together experts across the European Union, learn more about their programs and how we can cooperate in curbing what we view as a global problem," said Paul Friessem, a director at the Fraunhofer Institute for Secure Information Technology (SIT), one of the organizations in the European task force. "We also intend to collaborate with experts outside the EU, in particular in the U.S., Canada, Australia and even possibly Russia." One of the problems facing the task force is convincing parties to divulge information that some governments view as critical to their national security. The task force will also ask the critical infrastructure players about their requirements. The plan is to submit an overview of the situation to the European Commission over the next few months.

Category 16.3 *Infrastructure protection & homeland security*

2005-04-20 **cyber attack warning center pilot project CIDDAC infrastructure protection University of Pennsylvania**

DHS IAIP Daily;
http://www.infoworld.com/article/05/04/20/HNcyberpilot_1.htm l

CYBER ATTACK EARLY WARNING CENTER BEGINS PILOT PROJECT

A fledgling nonprofit group working to develop an automated cyber-attack early warning system, the Cyber Incident Detection Data Analysis Center (CIDDAC), is about to begin a pilot project to collect data on network intrusions from a group of companies in national-infrastructure industries. Backed by a grant from the Department of Homeland Security, CIDDAC has set up an operations center at the University of Pennsylvania's Institute of Strategic Threat Analysis and Response laboratory. Around 30 organizations will eventually participate in the project, although some are still being selected, according to CIDDAC Executive Director Charles Fleming. He expects to have useful data from the pilot test in about five months. CIDDAC's focus is on linking together organizations in industries such as banking, electrical power, gas and oil, telecommunications and transportation. The center will use a network of sensors, dubbed RCADSs (Real-Time Cyber Attack Detection Sensors), to gather information on intrusions and attempts. CIDDAC will also pass collected information on to law enforcement agencies, but Fleming emphasized that serving private-sector alert needs is the group's priority. CIDDAC Website: http://www.ciddac.org/

Category 16.3 *Infrastructure protection & homeland security*

2005-04-21 **DHS program University of Pennsylvania cyberattach study Cyber Incident Detection Analysis Center**

EDUPAGE; http://chronicle.com/prm/daily/2005/04/2005042101t.htm

PENN TO HEAD STUDY OF CYBERATTACKS

A new program sponsored by the Department of Homeland Security will attempt to collect real-time data on cyberattacks in the private sector, with the goal of using such data to prevent future attacks. Led by the University of Pennsylvania, the Cyber Incident Detection Analysis Center will install monitors on corporate networks. In the event of an attack on the network, the monitors, which will cost companies $10,000 annually, will transmit data to the Institute for Strategic Threat Analysis and Response at the university, where it will be analyzed and made available to researchers at other institutions. Those with access to the data will not be able to see which company it came from, and researchers will not be directly involved in prosecuting individuals responsible for cyberattacks. Charles Fleming, executive director of the center, said a pilot program will be carried out before the monitors become widely available. Chronicle of Higher Education, 21 April 2005 (sub. req'd)

Category 16.3 *Infrastructure protection & homeland security*

2005-04-28 **microchip industry protection outsourcing security concern**

DHS IAIP Daily;
http://www.infoworld.com/article/05/04/28/HNmicrochip_1.html

U.S. SEEKS GREATER MICROCHIP INDUSTRY PROTECTION

The migration of microchip production outside the U.S. poses a major threat to the nation's security and economy and the Department of Defense should take the lead in efforts to rebuild the industry at home, warns a recent report from a federal advisory committee. It points to China as a beneficiary of current trends. "From a U.S. national security view, the potential effects of this restructuring are so perverse and far reaching and have such opportunities for mischief that, had the United States not significantly contributed to this migration, it would have been considered a major triumph of an adversary nation's strategy to undermine U.S. military capabilities," says the report, from the U.S. Defense Science Board Task Force on High Performance Microchip Supply, dated February 2005. The report puts renewed emphasis on a call for revitalizing U.S. chip production in the face of its continued migration overseas, and warns that losing the manufacturing end of the chip industry ultimately puts research and development at risk since, historically, "R&D tends to follow production. Report: http://www.acq.osd.mil/dsb/reports/2005-02-HPMS_Report_Final .pdf

---

Category 16.3 *Infrastructure protection & homeland security*

2005-05-04 **NSF cyber infrastructure plan Internet2 improving security colleges universities**

EDUPAGE; http://chronicle.com/prm/daily/2005/05/2005050401t.htm

NSF WORKING ON CYBERINFRASTRUCTURE PLAN

Arden L. Bement Jr., director of the National Science Foundation (NSF), this week told attendees of an Internet2 meeting in Virginia that the NSF is developing a plan to support development of the nation's cyberinfrastructure, including that of colleges and universities. Bement said that funding for cyberinfrastructure is "one of the most important investments of the 21st century," though the announcement was short on specifics. The NSF's Cyberinfrastructure Interim Working Group submitted a report to Bement that reportedly outlines the details of the plan, but the agency said it will not release the report until some issues are cleared up. In his comments, Bement noted that higher education in particular is in need of improvements. What he described as six-lane superhighways for data "are reduced to two-lane roads at most college and university campuses." Such "information overload," as he called it, impedes research from being conducted efficiently. Still, Bement noted that money for the NSF "is not plentiful" and that it will likely be even scarcer in the future. Chronicle of Higher Education, 4 May 2005 (sub. req'd)

Category 16.3 *Infrastructure protection & homeland security*

2005-05-05 **US Computer Emergency Readiness Team US-CERT service expansion Department of Homeland Security**

DHS IAIP Daily; http://fcw.com/article88781−05−05−05−Web

US-CERT EXPANDS SERVICES

The Department of Homeland Security's U.S. Computer Emergency Readiness Team (US-CERT) will offer federal agencies expanded cybersecurity alerts and threat management services. Federal employees who are designated as first responders in their agencies will have greater access to advanced warnings about cyberattacks. With such early warnings, network and computer security managers often can block incoming worm or virus attacks before they cause damage or disrupt computer network services. "We're been working for some time with public- and private-sector partners to build a better understanding of what we need by way of cyber situational awareness," said Andy Purdy, acting director of the National Cyber Security Division in DHS' Information Analysis and Infrastructure Protection Directorate. Cybersecurity officials who are members of the federal Government Forum of Incident Response and Security Teams will use the new alert and threat management services, along with existing government and commercial services, to protect federal agency networks and computer systems.

Category 16.3 *Infrastructure protection & homeland security*

2005-05-09 **Department Homeland Security secure network installation issue**

DHS IAIP Daily;
http://www.washingtontechnology.com/news/1_1/daily_news/2616 1−1.html

DHS SECURE NETWORK WAS RUSHED.

The Department of Homeland Security's (DHS) $337 million network for sharing top-secret data was developed in a rush, and as a result is inadequate and does not meet the needs of its users, according to a new report by the department's Acting Inspector General Richard L. Skinner. Department officials developing the Homeland Security Secure Data Network (HSDN) hurried to finish the job in nine months because they believed they would be cut off from the Pentagon's secure data network by a December 31, 2004 deadline, the inspector general (IG) said. The IG report stated, "…the methods for collecting and documenting the functional and security needs of users during the requirements definition phase for the new network did not provide adequate assurance that user needs at the 600 sites will be met." The 600 sites referred to are DHS intelligence gathering units and federal, state and local agencies involved in homeland security. The inspector general is recommending that all system users be involved in defining its requirements in the future, and that completion of all testing be verified before deployment. Inspector General's Report: http://www.dhs.gov/dhspublic/interweb/assetlibrary/OIG_05-19 _Apr05.pdf

---

Category 16.3 Infrastructure protection & homeland security

2005-05-18 **survey Homeland Security information technology IT initiative complete**

DHS IAIP Daily;
http://www.washingtontechnology.com/news/1_1/daily_news/2619 9−1.html

SURVEY: HOMELAND SECURITY IT INITIATIVES NEARLY COMPLETED

Most homeland security IT initiatives may be near completion for federal agencies governmentwide, according to the new 2005 Federal IT Marketing Report published by Market Connections Inc. The findings are based on a survey of 600 federal IT professionals, including 181 from Defense agencies, 44 from the Department of Homeland Security and 375 from other civilian agencies. Anti-terrorism IT projects appear to be in the final stages. Forty-six percent of the respondents said they had completed at least 75 percent of their homeland security IT initiatives. The five most important homeland security IT initiatives reported were IT security, physical security, disaster recovery, threat assessments and threat response. The least important IT initiatives were information-sharing with the public, support of state and local agencies, information-sharing between agencies and adapting existing technology, the report said. Report: http://www.marketconnectinc.com/IT_report.html

---

Category 16.3 Infrastructure protection & homeland security

2005-05-26 **GAO report DHS unprepared computer cybersecurity**

EDUPAGE; http://news.com.com/2100-7348_3-5722227.html

GAO SAYS DHS UNPREPARED FOR CYBERSECURITY

The Government Accountability Office (GAO) has issued a report strongly critical of the readiness of the Department of Homeland Security (DHS) to deal with threats to the nation's cybersecurity. According to the report, DHS "has not fully addressed any" of 13 areas of cybersecurity, including bot networks, criminal gangs, foreign intelligence services, spammers, and spyware. "DHS cannot effectively function as the cybersecurity focal point intended by law and national policy," said the authors of the report. During the past year, DHS has seen the departure of a number of high-level officials, including the director and deputy director of Homeland Security's National Cyber Security Division, the undersecretary for infrastructure protection, and the assistant secretary responsible for information protection. A representative of DHS refuted the GAO's findings, saying that DHS has made improvements to the "nation's cybersecurity posture." He noted that DHS, as a new federal agency, measures progress in nonquantitative, less formal ways. CNET, 26 May 2005

Category 16.3 Infrastructure protection & homeland security

2005-05-26 **Government Accountability Office GAO critical infrastructure protection DHS report**

DHS IAIP Daily; http://www.gao.gov/new.items/d05434.pdf

CRITICAL INFRASTRUCTURE PROTECTION: DEPARTMENT OF HOMELAND SECURITY FACES CHALLENGES IN FULFILLING CYBERSECURITY RESPONSIBILITIES (REPORT)

GAO was asked to determine (1) DHS's roles and responsibilities for cyber critical infrastructure protection, (2) the status and adequacy of DHS's efforts to fulfill these responsibilities, and (3) the challenges DHS faces in fulfilling its cybersecurity responsibilities. DHS established the National Cyber Security Division to take the lead in addressing the cybersecurity of critical infrastructures. While DHS has initiated multiple efforts to fulfill its responsibilities, it has not fully addressed any of the 13 responsibilities, and much work remains ahead. DHS established the US-CERT as a public/private partnership to make cybersecurity a coordinated national efforts. However, DHS has not yet developed national cyber threat and vulnerability assessments or government/industry contingency recovery plans for cybersecurity, including a plan for recovering key Internet functions. DHS faces a number of challenges which include achieving organizational stability, gaining organizational authority, overcoming hiring and contracting issues, increasing awareness about cybersecurity roles and capabilities, establishing effective partnerships with stakeholders, achieving two-way information sharing with these stakeholders, and demonstrating the value DHS can provide. Until it confronts and resolves these underlying challenges and implements its plans, DHS will have difficulty achieving significant results in strengthening the cybersecurity of our critical infrastructures. Highlights: http://www.gao.gov/highlights/d05434high.pdf

---

Category 16.3 *Infrastructure protection & homeland security*

2005-05-31 **FBI DHS Homeland Security cell phones airplane objection anti-terrorism FCC**

DHS IAIP Daily; http://news.zdnet.com/2100−1035_22−5726850.html

FBI AND DHS OBJECT TO CELL PHONES ON AIRPLANES

The FBI and Department of Homeland Security (DHS) are objecting to a proposal to permit the use of cellular telephones and other wireless devices on airplanes. Unless telecommunications providers follow a lengthy list of eavesdropping requirements for calls made aloft, the FBI and DHS don't want cellular or wireless connections to be permitted. In a letter to the Federal Communications Commission (FCC) sent last Thursday, May 26, the police agencies said any rule permitting "in-flight personal wireless telephone use must consider public safety and national security" concerns. At the moment, technical and social reasons keep cell phones muted during flight. The FCC is considering proposals to relax those restrictions The FBI and DHS say that the 1994 Communications Assistance for Law Enforcement Act, or CALEA, requires that airlines follow strict wiretapping guidelines. The police agencies, for instance, want to be able to eavesdrop on conversations no "more than 10 minutes" after the call is made. "There is a short window of opportunity in which action can be taken to thwart … crisis situations onboard an aircraft, and law enforcement needs to maximize its ability to respond to these potentially lethal situations," the agencies say in their letter. Letter to FCC: http://www.askcalea.com/docs/20050526_doj_fcc-wt-04-435.pdf

---

Category 16.3 *Infrastructure protection & homeland security*

2005-06-06 **DHS funding cybersecurity research Idaho National Laboratory INL critical infrastructure protection**

DHS IAIP Daily; http://www.dhs.gov/dhspublic/display?content=4532

IDAHO NATIONAL LABORATORY RECEIVES SECOND ROUND OF HOMELAND SECURITY FUNDING FOR CYBER THREAT REDUCTION PROGRAM

The U.S. Department of Energy's Idaho National Laboratory (INL) received a second round of funding this week from U.S. Department of Homeland Security to continue a multi-year cyber security program. The Control System Security Center will receive $11.7 million in 2005 to continue its efforts to secure the computer-aided control systems that operate the nation's critical infrastructures. Control systems are the digital automation systems that operate infrastructures such as the electric power grid, oil and gas refineries, and telecommunication systems. "This year we plan to focus our efforts on establishing baseline security assurance levels and cyber recommendations to increase industry security," said Julio Rodriguez, INL department manager for Critical Infrastructure Assurance. "We're at the point where industry is beginning to recognize the potential threats of unsecured control systems and they are more willing to work with government agencies to improve the security of the nation' s critical infrastructures." The Department of Homeland Security selected INL for this project because of its expertise in design, assessments and operational management of control systems across several industrial sectors.

Category 16.3 *Infrastructure protection & homeland security*

2005-06-09 **DHS lacking disaster backups TSA Coast Guard insufficient money management**

DHS IAIP Daily; http://www.nytimes.com/2005/06/09/politics/09home.html

INTERNAL AUDIT FINDS DHS IS LACKING DISASTER BACKUPS

An internal inspector general audit released on Wednesday, June 8, concluded the computer systems at 19 Department of Homeland Security (DHS) sites that served agencies like the Transportation Security Administration, Customs and Border Protection and the Coast Guard had no functioning backups or relied on obviously deficient or incomplete backups. Even the Federal Emergency Management Agency, which is in charge of disaster recovery, was unprepared, the report said. The department "must be able to provide mission-essential services with minimal disruption following a disaster," the report said. Adequate backups were lacking for networks that screen airline passengers, that inspect goods moving across borders and that communicate with department employees and outside officials. Those same agencies, the auditors found, have in most cases failed to prepare sufficiently written disaster recovery plans that would guide operations if a main office or computer system was knocked out. The problems, the audit said, are insufficient money and insufficient management attention. "We recognize that information-technology continuity is important to lead an effective recovery, which is why we are developing a plan to ensure critical systems continuity," a spokesperson, Brian Roehrkasse, said. Inspector General's Report: http://www.dhs.gov/interweb/assetlibrary/OIGr_05-22_May05.pdf

---

Category 16.3 *Infrastructure protection & homeland security*

2005-06-13 **US dumps drops ditches biometric passport requirement UK DHS terrorism anti-terrorism civil liberties privacy concerns**

EDUPAGE; http://www.theregister.com/2005/06/13/us_bio_passports/

U.S. EXPECTED TO DITCH BIOMETRIC PASSPORT REQUIREMENT

Government officials in the United Kingdom are optimistic that the United States will withdraw an upcoming requirement that individuals traveling under the Visa Waiver program have biometric passports. The program allows people from 27 countries to make short visits to the United States without a visa. The U.S. Department of Homeland Security had issued a ruling that participants in the Visa Waiver program would be required to have biometric identifying information added to their passports by October 2004, which was extended to October 2005. Officials in Ireland have put on hold their efforts to comply with the regulation, believing that U.S. officials have come to see the technology as sufficiently unreliable to compel its use by this fall. Critics of biometric technology also point to the possibility that such information could be used to violate individuals' civil liberties. The Register, 13 June 2005

Category 16.3 *Infrastructure protection & homeland security*

2005-06-17 **Homeland Security Information Network critical infrastructure protection retailers join**

DHS IAIP Daily;
http://www.washingtontechnology.com/news/1_1/homeland/26420− 1.html

RETAILERS JOIN HOMELAND SECURITY INFORMATION NETWORK

Retailers are among the industry groups being invited to join a recent incarnation of the federal Homeland Security Information Network (HSIN) specifically intended for critical infrastructure owners and operators and designed to help share unclassified information to guard against terrorist attacks. The National Retail Federation (NRF) has recruited executives from nearly 100 retail companies to participate in the network, called HSIN-CL, the trade group said in a press release. The information network is a composite of several regional networks that share information among law enforcement, fire departments, local government agencies and businesses. Technologies used within the network include wired and wireless telephones, e-mail, facsimiles, and text pagers to share alerts and notifications. The network sends real-time information to its members, may be used "to discuss day-to-day security issues" and "to share information on suspicious activities with federal authorities" according to the NRF release. Other industry sectors, including the chemical industry, ports and financial services, are expected to participate in the HSIN-CL as well. NRF news release: http://www.nrf.com/content/press/release2005/hsin0605.htm

---

Category 16.3 *Infrastructure protection & homeland security*

2005-06-20 **USAPATRIOT Act surveillance search seizure constitutional rights warrants investigation counter-terrorism civil rights libraries reading**

RISKS; http://www.nytimes.com/2005/06/20/politics/20patriot.html? 23 91

LEOs MONITOR READING MATERIALS

Law enforcement officials have made at least 200 formal and informal inquiries to libraries for information on reading material and other internal matters since October 2001, according to a new study that adds grist to the growing debate in Congress over the government's counterterrorism powers. In some cases, agents used subpoenas or other formal demands to obtain information like lists of users checking out a book on Osama bin Laden. Other requests were informal -- and were sometimes turned down by librarians who chafed at the notion of turning over such material, said the American Library Association, which commissioned the study. [Source: Eric Lichtblau, *The New York Times*, 20 Jun 2005; Abstract by Peter G. Neumann]

Category 16.3 *Infrastructure protection & homeland security*

2005-07-19 **GAO Infrastructure Protection DHS summarize work status challenges cybersecurity recommendations**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/36434−1.html

CRITICAL INFRASTRUCTURE PROTECTION: CHALLENGES IN ADDRESSING CYBERSECURITY (TESTIMONY)

The Homeland Security Act of 2002 and federal policy established the Department of Homeland Security (DHS) as the focal point for coordinating activities to protect the computer systems that support our nation's critical infrastructures. GAO was asked to summarize previous work, focusing on (1) DHS's responsibilities for cybersecurity-related critical infrastructure protection (CIP), (2) the status of the department's efforts to fulfill these responsibilities, (3) the challenges it faces in fulfilling its cybersecurity responsibilities, and (4) recommendations GAO has made to improve 13 cybersecurity of our nation's critical infrastructure. While DHS has initiated multiple efforts to fulfill its responsibilities, it has not fully addressed any of the 13 responsibilities, and much work remains ahead. The department established the US-CERT as a public/private partnership to make cybersecurity a coordinated national effort, and it established forums to build greater trust and information sharing among federal officials with information security responsibilities and law enforcement entities. However, DHS has not yet developed national cyber threat and vulnerability assessments or government/industry contingency recovery plans for cybersecurity, including a plan for recovering key Internet functions.

Category 16.3 *Infrastructure protection & homeland security*

2005-07-20 **Government News DHS IT Department of Homeland Security congressional NCSD**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/36434−1.html

DHS TO MOUNT MAJOR IT SECURITY EXERCISE

The Department of Homeland Security plans to conduct a major cybersecurity preparedness and response exercise to be called Cyber Storm in November, a department official said in congressional testimony Tuesday, July 19. Andy Purdy, acting director of DHS' National Cyber Security Division (NCSD), described Cyber Storm as "a national exercise" during a hearing of the Senate Homeland Security and Governmental Affairs Subcommittee on Federal Financial Management, Government Information and International Security. According to written testimony Purdy presented, the division has worked with the Justice and Defense departments to help form the National Cyber Response Coordination Group (NCRCG). "The NCRCG has developed a concept of operations for national cyber incident response that will be examined in the National Cyber Exercise, Cyber Storm, to be conducted by NCSD in November 2005 with public and private-sector stakeholders."

Category 16.3 *Infrastructure protection & homeland security*

2005-08-01 **DHS government agency business vendor law improve security SAFETY Act**

EDUPAGE; http://news.zdnet.com/2100-1009_22-5814289.html

DHS URGES INDUSTRY TO USE LAW TO IMPROVE SECURITY

Following the terrorist attacks of September 2001, Congress passed a law designed to encourage private-sector research into security technology, but so far, relatively few companies have taken advantage of the law, according to the Department of Homeland Security (DHS). Michael Chertoff, secretary of DHS, said that despite the provisions of the Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act of 2002, which shields approved companies from civil litigation if their technologies fail to perform, only 17 products and services have earned the law's highest level of protection. None of the 17 specifically focuses on information technology security. To increase the nation's security infrastructure, said Chertoff, "we have to look beyond the walls of DHS itself, to the private sector and to the world of high tech." Chertoff pointed to technologies currently used to screen airline passengers as one area that needs attention, saying that current screening is at a "basic, primitive" stage. ZDNet, 1 August 2005

Category 16.3 *Infrastructure protection & homeland security*

2005-08-02 **terrorism cyberterrorists copy hacker tactics information cyber warfare security government**

DHS IAIP Daily; http://www.techweb.com/wire/security/167100173#_

TERRORISTS COPYING HACKER TACTICS.

Cyber-terrorists are trying to break into government networks around the world using the same tactics as run-of-the-mill hackers, a U.S. State Department official said Tuesday, August 2. "The same technique that a hacker would use, the same technology, will be utilized by somebody with a different political motivation," Michael Alcorn, branch chief of the State Department's Office of Anti-Terrorism Assistance, in a statement made to the AFP wire service in Kuala Lumpur on Tuesday. The Office of Anti-Terrorism Assistance trains foreign law enforcement personnel on a variety of terrorism-related topics, including cyber-security. "The problem we're all facing is a global borderless problem, where attacks can occur anywhere in the world and originate from anywhere else in the world," Alcorn told the AFP. He went on to say that cyber-security problems and resulting terrorist activity was widespread, and claimed that some of the evidence of attacks has come from overseas law enforcement agencies which have confiscated militants' computers. "They're finding evidence on these computers that indicates militants have looked into or are researching this type of technology," Alcorn said.

Category 16.3 *Infrastructure protection & homeland security*

2005-08-03 **DHS SAFETY Act anti-terrorism civil lawsuit immunity**

DHS IAIP Daily; http://news.zdnet.com/2100−1009_22−5814289.html

DHS CALLS FOR TECH INDUSTRY INVOLVEMENT

Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act of 2002 provides government-authorized companies with immunity from civil lawsuits if their anti-terrorism products fail to perform. In order to get on the approved list, companies must first go through a two-step application process. But only 17 offerings -- none related to information technology -- have received such approval. In a speech at the Commonwealth Club in Santa Clara, CA, Thursday, July 29, Department of Homeland Security (DHS) Secretary Michael Chertoff said the newly created position of assistant secretary for Cyber and Telecommunications Security would be in charge of stepping up the government's collaboration with tech companies. So far, none of the approved services pertain specifically to information technology security. The latest technology to make the list was a cargo container inspection system for use at ports. DHS is eyeing technological advances to beef up border enforcement, emergency preparedness, transportation and cybersecurity, Chertoff said. "But there is a way forward," Chertoff said, pointing to high-tech biometric identifiers and radio frequency identification tags as potential new avenues for screening. A transcript of Secretary Chertoff's remarks is available on the DHS Website: http://www.dhs.gov/dhspublic/display?content=4700 More about the SAFETY Act of 2002: https://www.safetyact.gov/DHS/SActHome.nsf/Main?OpenFrameset &6EWVEC

Category 16.3 *Infrastructure protection & homeland security*

2005-08-11 **DHS report private vendor domestic security improvement businesses**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/story/0 ,10801,103827,00.html

BUSINESSES NEED TO FOCUS ON CYBERSECURITY

The Department of Homeland Security (DHS) will focus significant efforts on cybersecurity and on working with private vendors to develop technologies designed to provide domestic security in the coming months, DHS Secretary Michael Chertoff said Wednesday, August 10. Chertoff, speaking at the InfraGard National Conference in Washington, DC, also called on private companies to make more of an effort to protect their cyberinfrastructures. He also said more incentives are needed for IT vendors to focus on cybersecurity. InfraGard is an organization started by the FBI to improve information sharing about critical infrastructure between the U.S. government and private industry. One incentive for private companies to develop cybersecurity products would be to institute legal reforms that limit damages from product lawsuits, Chertoff said. As an example, he cited the Support Anti-terrorism by Fostering Effective Technologies Act of 2002, which limits liability for products designed to combat terrorism. But he said Congress should go further in protecting companies from product lawsuits. However, private companies should already have good reasons to protect their infrastructures, he said. "In today's threat environment, active security measures are critical to businesses themselves, because the cost of an attack will very, very greatly outweigh the cost of protection." InfraGard 2005 National Conference: http://www.infragardconferences.com/

Category 16.3 *Infrastructure protection & homeland security*

2005-09-16 **national security policy critical infrastructure report vulnerabilities weakness testimony Congress committee information warfare physical attack counter-terrorism Internet robustness resiliance cooperation**

RISKS; http://www.house.gov/science/press/109/109-129.htm 24 04

CIOs WARN CONGRESSIONAL COMMITTEE OF CRITICAL INFRASTRUCTURE VULNERABILITIES

On Sep 15, 2005, CIOs of several major US corporations warned the House Science Committee "the nation's critical infrastructure remains vulnerable to cyber attack. The witnesses said the economy is increasingly dependent on the Internet and that a major attack could result in significant economic disruption and loss of life."

….

"Urging action to address this vulnerability, the witnesses advocated increased funding for cybersecurity research and development (R&D) and greater information sharing between industry and government and among various sectors of industry. Witnesses also urged greater federal attention to cybersecurity and praised the creation of an Assistant Secretary for Cybersecurity at the Department of Homeland Security (DHS)."

….

>[Mr. John Leggate, Chief Information Officer, British Petroleum Inc.] testified that an informal survey earlier this year found that executives in the telecommunications, energy, chemical, and transportation sectors estimated that about 30 percent of their revenue depends directly on the Internet. He also said that, because of interdependency among various industry sectors, a single attack could reverberate throughout the global economy: "These cascading dependencies all too quickly create 'domino effects' that are not obvious to the corporate customer or the policymaker."<

[Extracts by MK]

Category 16.3 *Infrastructure protection & homeland security*

2005-10-07 **Federal Computer Week Armstron DHS CIO DHS deputy sharing management screening**

DHS IAIP Daily; http://www.fcw.com/article91039−10−07−05−Web

ARMSTRONG NAMED DHS DEPUTY CIO

Charles Armstrong, the CIO of the Department of Homeland Security's (DHS) Border and Transportation Security Directorate, has been named as the department's new deputy CIO. Armstrong will help DHS work with industry on identity-management issues, including information sharing, case management and passenger screening.

Category 16.3 *Infrastructure protection & homeland security*

2005-10-20 **security evaluation legal ruling court judgement shut down denial-of-service DoS government agency department**

http://sfgate.com/cgi-bin/article.cgi?file=/n/a/2005/10/20/national/w145958D47.DTL

US DEPT OF INTERIOR ORDERED OFF THE 'NET

Security expert Stephen Cobb, CISSP writes, "The US Department of the Interior has spent $100 million on security improvements in the last 3 years but still gets an "F" for security and so has to stay off the 'net until it can prove the data on its network is safe." A story by Jennifer Talhelm, AP writer, begins, "A judge ordered the Interior Department to disconnect from the Internet all computer equipment holding data related to trust accounts it manages for American Indians, a decision that could cripple large sections of the agency's computer network. In a 205-page opinion declaring the department's computer security 'disorganized and broken,' U.S. District Judge Royce Lamberth on Thursday (2005/10/20) said the order applies to all networks with access to trusted data -- from servers to BlackBerrys -- except what is necessary to protect from fire or threats to life, property or national security."

Category 16.3 *Infrastructure protection & homeland security*

2005-10-27 **US Presidential executive order inter-agency information sharing**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/37432−1.html

EXECUTIVE ORDER BOLSTERS INFORMATION-SHARING AMONG AGENCIES

On Tuesday, October 25, President Bush issued Executive Order 13356 that restructures information-sharing responsibilities among agencies combating terrorism. The Order grants authority to the Office of the Director of National Intelligence. Executive Order 13356: http://www.whitehouse.gov/news/releases/2005/10/20051025-5.html

---

Category 16.3 *Infrastructure protection & homeland security*

2005-10-28 **US SCADA systems protection security industrial control critical infrastructure homeland security**

DHS IAIP Daily; http://www.securityfocus.com/news/11351

U.S. MAKES SECURING SCADA SYSTEMS A PRIORITY

Wary of the increasing number of online attacks against industrial control systems, the U.S. government has stepped up efforts to secure the systems used to control and monitor critical infrastructure, such as power, utility, and transportation networks. Andy Purdy, acting director of the National Cyber Security Division at the Department of Homeland Security (DHS), stated, "The exposure of these systems to malicious actors in cyberspace is greater than in the past, because these systems are more often connected to the Internet. With the profit margins of many of the owners and operators, it is a challenge to convince them to spend to reduce the risk." DHS has become increasingly concerned over the lack of security of such control networks -- among which the best known is the supervisory control and data acquisition (SCADA) system -- because the majority of such control systems are owned by private companies and are increasingly being interconnected to improve efficiency.

Category 16.3 *Infrastructure protection & homeland security*

2005-11-02 **DHS IT system audit report systems uncertified unaccredited FISMA**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/37474−1.html

DHS'S INSPECTOR GENERAL AUDITS IT SYSTEMS

An audit by the Department of Homeland Security's inspector general, Richard L. Skinner, found that many of the department's IT systems remain uncertified and unaccredited, while plans to correct weaknesses are undeveloped. The report also said contingency plans have not been developed and tested for all systems, and added that tools used to measure progress are neither complete nor current. "We recommend that DHS continue to consider its information security program a significant deficiency for [fiscal] 2005," the report concluded. DHS officials agreed with the recommendations and, according to the report, have developed remediation plans for fiscal 2006. Skinner evaluated DHS' compliance with the Federal Information Security Management Act of 2002, which focuses on program management, implementation and evaluation of the security of unclassified and national security IT systems. The department has made progress on several fronts, including developing so-called Plans of Action and Milestones, as well as a Trusted Agent FISMA tool to collect and track data related to FISMA compliance. Report: http://www.dhs.gov/interweb/assetlibrary/OIG_05-46_Sep05.pdf

---

Category 16.3 *Infrastructure protection & homeland security*

2005-11-07 **infrastructure collapse natural disaster hurricane Katrina telecom weak link**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/37515−1.html

TELECOM INFRASTRUCTURE IS WEAK LINK IN DISASTERS

During Hurricane Katrina, getting enough power was a major issue for the Gulf Coast telecom providers, as was keeping the basic infrastructure running and providing physical security for workers and equipment. A recent Federal Communications Commission meeting with two telecommunication providers revealed that outages in physical infrastructure remains a problem for networks in disaster situations. Anthony Melone, vice president of network operations support for Verizon Wireless stated that Katrina "was probably the most severely impacted situation that we've experienced...There were a lot of unique learning experiences." Verizon Wireless' cellular phone coverage for Alabama, Louisiana, and Mississippi dipped to less than 50 percent of its full coverage, and about six percent of BellSouth's customer base -- about 1.2 million users -- lost landline telephone usage.

Category 16.3 Infrastructure protection & homeland security

2005-11-11 **US government IT infrastructure security anti-terrorism DHS information sharing**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/37550−1.html

INFORMATION TECHNOLOGY SECTOR COORDINATING COUNCIL DEBUTS

A newly formed Information Technology Sector Coordinating Council -- consisting of owners and operators of critical information technology (IT) infrastructures -- will work with the Department of Homeland Security (DHS) to safeguard the IT sector from terrorist attacks. IT industry leaders have been organizing the group for several months under the guidance of Homeland Security Presidential Directive-7 and DHS. Under the National Infrastructure Protection Plan, private-sector owners in each of 17 critical sectors -- IT, water, energy, food, banking, and transportation -- have been advised to self-organize and to create sector coordinating councils to share information with a lead government agency for their sector. For IT, the lead agency is DHS.

Category 16.3 Infrastructure protection & homeland security

2005-11-28 **US government agencies CIA cybersecurity expert recommendation monitor insider network threats**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/37654−1.html

AGENCIES MUST MONITOR INSIDER NETWORK THREATS, EXPERT SAYS

Agency networks are more vulnerable than ever, according to a former Central Intelligence Agency (CIA) official and cybersecurity expert, and the greatest threat to an organization's network security may come from within. Eric Cole, who worked for the CIA for more than five years, told an audience of government and corporate security professionals Monday, November 28, at the inaugural Techno Forensics Conference at the National Institute of Standards and Technology that despite their best efforts, networks are only getting more porous. Cole said an emerging threat for organizations is that the emphasis on thwarting outside attacks and tracing their origins has led them to overlook the insider threat. In several recent cases, organizations conducted preliminary forensic examinations after network incidents and identified employees as being responsible. Aside from network insecurity, Cole said agencies need to have standardized procedures for computer forensics. A lack of standardized procedures for computer forensics, he warned, will jeopardize organizations' abilities to use forensic examinations at trial.

Category 16.3 Infrastructure protection & homeland security

2005-12-02 **DHS software vulnerability flaw database grading system**

DHS IAIP Daily; http://www.securityfocus.com/news/11360

FEDERAL FLAW DATABASE COMMITS TO GRADING SYSTEM

A federal database of software vulnerabilities funded by the U.S. Department of Homeland Security has decided on a common method of ranking flaw severity and has assigned scores to the more than 13,000 vulnerabilities currently contained in its database, the group announced last week. The National Vulnerability Database (NVD), unveiled in August, completed its conversion over to the Common Vulnerability Scoring System (CVSS), an industry initiative aimed at standardizing the severity rankings of flaws. The CVSS gives vulnerabilities a base score based on their severity, a temporal score that measures the current danger -- which could be lessened by a widely available patch, for example -- and an environmental score that measures an organization's reliance on the vulnerable systems. The move to the CVSS gives the flaw-ranking initiative a major boost. Created by security researchers at networking giant Cisco, vulnerability management software provider Qualys and security company Symantec, the CVSS has not been used widely, though many companies are considering scoring flaws with the system. To date, no software vendor has yet graded vulnerabilities in its product using the CVSS.

Category 16.3 *Infrastructure protection & homeland security*

2005-12-05 **DHS large-scale disaster recovery research center John Hopkins University terrorism anti-terrorism**

EDUPAGE; http://www.govtech.net/magazine/channel_story.php/97475

DHS PICKS JOHNS HOPKINS FOR DISASTER PREPAREDNESS

The Department of Homeland Security (DHS) has chosen Johns Hopkins University to lead an effort to investigate nationwide preparedness for and response to large-scale disasters. The Center for the Study of High Consequence Event Preparedness and Response will look at ways the country can prevent and manage disasters, particularly through the interactions of networks and through models and simulations. The center will address issues including risk assessment, decision making, infrastructure integrity, surge capacity, and sensor networks. The center is the fifth Center of Excellence, administered by DHS's Office of University Programs and dedicated to university-based interdisciplinary research. Michael Chertoff, secretary of Homeland Security, said Johns Hopkins will "lead a talented and deeply experienced team of professionals from institutions across the country" to help prevent and respond to "high-consequence disasters or terrorist attacks."
Government Technology, 5 December 2005

Category 16.3 *Infrastructure protection & homeland security*

2005-12-13 **Cyber Security Industry Alliance CSIA federal government DHS rating D+**

EDUPAGE; http://www.fcw.com/article91710-12-13-05-Web

CSIA GIVES FEDS D+ ON CYBERSECURITY

In a report card released by the Cyber Security Industry Alliance (CSIA), the federal government received a grade of D+ for cybersecurity. CISA gave credit to the Department of Homeland Security for establishing a new position, the assistant secretary for cybersecurity. Six months after that job was created, however, it remains unfilled. Paul Kurtz, executive director of CSIA, commented that "Cybersecurity research is in a crisis." CSIA also launched what it calls a Digital Confidence Index, a measure of public confidence in efforts to protect computers and systems. The initial rating for the index is 58 out of 100. CSIA issued a set of 13 recommendations, called the National Agenda for Information Security in 2006, designed to improve the nation's cybersecurity. Among the recommendations are calls to increase funding for cybersecurity research and to promote cooperation among federal agencies. Federal Computer Week, 13 December 2005

Category 16.3 *Infrastructure protection & homeland security*

2006-01-10 **US DHS open source support source code bug hunt**

DHS IAIP Daily; http://news.com.com/Homeland+Security+helps+secure+open 23
−sour ce+code/2100−1002_3−6025579.html?tag=nefd.lede

DEPARTMENT OF HOMELAND SECURITY HELPS SECURE OPEN-SOURCE CODE

The U.S. Department of Homeland Security (DHS) is extending the scope of its protection to open-source software. Through its Science and Technology Directorate, DHS has given $1.24 million in funding to Stanford University, Coverity and Symantec to hunt for security bugs in open-source software and to improve Coverity's commercial tool for source code analysis. The DHS grant will be paid over a three-year period, with $841,276 going to Stanford, $297,000 to Coverity and $100,000 to Symantec. In the effort, which the government agency calls the "Vulnerability Discovery and Remediation, Open Source Hardening Project," Stanford and Coverity will build and maintain a system that does daily scans of code contributed to popular open-source projects. The automated system should be running by March, and the resulting database of bugs will be accessible to developers, they said. Symantec will provide security intelligence and test the source code analysis tool in its proprietary software environment, said Brian Witten, the director of government research at the Cupertino, CA, security software vendor. The list of open-source projects that Stanford and Coverity plan to check for security bugs includes Apache, BIND, Ethereal, KDE, Linux, Firefox, FreeBSD, OpenBSD, OpenSSL. and MySQL, Coverity said.

Category 16.3 *Infrastructure protection & homeland security*

2006-01-11 **DHS Department of Homeland Security funding open source security research software Symantec Coverity Stanford University**

EDUPAGE; http://www.internetnews.com/security/article.php/3576886 23

DHS GRANT FUNDS OPEN SOURCE RESEARCH

The Department of Homeland Security (DHS) has awarded a $1.24 million, three-year contract to improve the quality of open source software. Given the growing reliance on open source technologies for infrastructure that underpins national security, DHS expects to see real benefits from the grant. The award will be split among Stanford University, Symantec, and Coverity, a firm that specializes in code analysis. Rob Rachwald, senior director of marketing at Coverity, said, "The DHS in many ways is obviously brokering this and they are the main beneficiary." For the grant, Coverity will identify security flaws and risks; Stanford will offer academic analysis of trends and provide opinions about the relative security of various technologies; and Symantec will provide consulting on how governmental agencies can incorporate open source products in a secure fashion into their own applications.

Category 16.3 *Infrastructure protection & homeland security*

2006-01-18 **DHS cybersecurity guidance grant kit XML-based information sharing**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/38026−1.html 23

DEPARTMENT OF HOMELAND SECURITY GRANT KIT OFFERS CYBERSECURITY GUIDANCE

The Department of Homeland Security's (DHS) new preparedness unit is urging state governors to prepare cybersecurity plans, adopt a new national XML-based model for information-sharing and implement newly developed common rules for geospatial content. The recommendations are some of the most detailed that the federal government has made to state and local governments on using IT in the fight against terrorism. The IT-related guidance is included in the fiscal 2006 grant application kit for the distribution of $3.9 billion in federal homeland security grants to states and localities this year, published by the preparedness directorate. Cybersecurity guidance was attached as an appendix for the first time. Guidelines for topics to be included in the cyberplans are somewhat open-ended. Recommendations cover about two-dozen questions related to policy, training, IT deployment and vulnerability. In addition, DHS is recommending that states, local and tribal government adopt geospatial data guidelines developed by the Information Content Subgroup of the Federal Geographic Data Committee Homeland Security Working Group in October 2005.

Category 16.3 *Infrastructure protection & homeland security*

2006-01-24 **DHS privacy national database critical infrastructure information**

DHS IAIP Daily; 23
http://www.washingtontechnology.com/news/1_1/homeland/27812−1.html

DHS VOWS TO PROTECT INFO ON NATIONAL DATABASE.

The Department of Homeland Security (DHS) has stepped up assurances that it will maintain the confidentiality of critical infrastructure information submitted to the National Asset Database, according to the newly revised draft National Infrastructure Protection Plan (NIPP) Base Plan version 2.0. DHS will evaluate all requests to view the database and will grant access only to select DHS employees and others on a "tightly controlled, need-to-know" basis, the revised plan states. The new language is set forth in the 234-page NIPP distributed by DHS this week. The plan was delivered by e-mail via NIPP@dhs.gov. The plan establishes a work and time frame for assessing vulnerabilities and risks and coordinating protections for 17 critical infrastructure sectors, including IT and telecommunications. Cybersecurity is treated as a cross-sector responsibility. DHS' assurances about database access appear to address concerns raised by IT executives and others over protecting confidentiality of the information they might submit on specific vulnerabilities within their sectors. One fear raised by IT industry members is that disclosing weak spots in their own networks may result in leaks that can be exploited by competitors.

Category 16.3 *Infrastructure protection & homeland security*

2006-01-27 **AT&T disaster recovery exercise Dallas**

DHS IAIP Daily; http://www.physorg.com/news10220.html 23

AT&T TO CONDUCT DISASTER EXERCISE.

AT&T will conduct its largest-ever network disaster recovery exercise in Dallas, TX, on Wednesday, February 8, the company said Wednesday, January 25. The telecommunications group said that self-contained equipment trucks will test and evaluate how well the company can support services in the event of a disaster. A total of 43 trailers will be used for the latest exercise in the Dallas-Fort Worth area. AT&T said it has invested over $300 million in its network disaster recovery program, which includes engineers and technicians across the country. The team has been activated 21 times since 1990, including responding to Hurricanes Katrina and Rita last year, the San Diego wildfires in 2003 and the September 11, 2001, attacks in New York City.

Category 16.3 *Infrastructure protection & homeland security*

2006-01-30 **Homeland Security DHS federal agencies Cisco Citadel Computer Associates Intel Microsoft Symantec VeriSign Cyber Storm exercise**

DHS IAIP Daily; 23
http://www.washingtontechnology.com/news/1_1/daily_news/2787 7−1.html

DHS, AGENCIES PLAN JOINT CYBER STORM EXERCISE.

The Department of Homeland Security (DHS) will test how well it works with other federal agencies and private IT companies to protect cybersecurity in a national exercise from February 6-10. The Information Technology Information-Sharing and Analysis Center will take part in the exercise, known as "Cyber Storm," with DHS to test its draft concept of operations for responding to cybersecurity incidents. Participating in Cyber Storm are Cisco Systems Inc., Citadel Security Software Inc., Computer Associates International Inc., Computer Sciences Corp., Intel Corp., Microsoft Corp., Symantec Corp., and VeriSign Inc., the center announced on its Website. Cyber Storm also will involve government agencies. According to Donald Purdy, acting director of DHS' National Cyber Security Division, the division established the Government Forum of Incident Response and Security Teams (GFIRST) to facilitate interagency information sharing and cooperation for readiness and response. The teams, comprising government computer experts, are responsible for IT security at government agencies. In addition to the GFIRST teams, the agency has worked with the Defense and Justice departments to form the National Cyber Response Coordination Group to provide an organized federal response to cybersecurity breaches.

Category 16.3 *Infrastructure protection & homeland security*

2006-02-09 **TSA audit Secure Flight Program privacy concern watch lists**

EDUPAGE; http://www.wired.com/news/technology/0,70198-0.html 23

TSA CALLS FOR AUDIT OF SECURE FLIGHT PROGRAM

The federal government's Secure Flight program has suffered another setback, this time from Kip Hawley, head of the Transportation Security Administration (TSA). Hawley told Congress that he has ordered a "comprehensive audit" of the program, though he did not say what prompted his decision. The program is intended to increase airline security by checking the names of all passengers against watch lists, a task currently carried out by airlines. Under the Secure Flight program, the federal government would assume that responsibility. Critics of the program point to its cost--$200 million over four years--noting that even last month Hawley said the TSA still was not entirely sure how it would work. They also have complained about privacy concerns of the program and routine mistakes that airlines reportedly make in checking passenger names against watch lists.

Category 16.3 *Infrastructure protection & homeland security*

2006-02-10 **DoD computer security survey cybercrime businesses**

DHS IAIP Daily; http://www.ebcvg.com/press.php?id=2071 23

DOJ ANNOUNCES NATIONAL COMPUTER SECURITY SURVEY.

The Department of Justice (DoJ) announced plans Friday, February 10, to conduct the first-ever national survey to measure the prevalence and impact of cybercrime on businesses within the United States. The survey, conducted by DoJ's Bureau of Justice Statistics and the Department of Homeland Security's National Cyber Security Division, will estimate the number of cyber attacks, frauds and thefts of information and the resulting losses during 2005. The survey, which will start this month and will be completed by the end of the year, will provide critical information for businesses, industry, government and other users to make more informed decisions about how to target resources to fight cybercrime. The comprehensive survey will collect information from a wide range of industry sectors. Currently no national baseline measure exists on the extent of cybercrime. The survey data will enable the federal government to assess what needs to be done to reduce computer security vulnerabilities and will provide the first official national statistics on the extent and consequences of cybercrime among the country's 5.3 million firms with salaried employees.. Additional details about this survey:
http://www.ojp.usdoj.gov/bjs/survey/ncss/ncss.htm

Category 16.3 *Infrastructure protection & homeland security*

2006-02-15 **hurricane Katrina response IT weakness FEMA DHS Michael Chertoff**

DHS IAIP Daily; http://www.techweb.com/wire/security/180202527 23

CHERTOFF SAYS IT WEAKNESSES HURT KATRINA RESPONSE.

Department of Homeland Security Secretary Michael Chertoff took responsibility for the poor response to Hurricane Katrina Wednesday, February 15, but he also blamed the department's inability to conduct surveillance, communicate efficiently, track shipments, and handle Web traffic. Testifying before the U.S. Senate Committee on Homeland Security and Governmental Affairs, Chertoff said the Department of Homeland Security and the Federal Emergency Management Agency need interoperability, hardened communications, a tracking system for shipments, improved surveillance resources, upgraded software and better hardware. Without hardened communications equipment, leaders could not obtain the information they need to make proper decisions during disasters, Chertoff said. Improvements are underway, but the department has to come up with agreements for supply chain management and real-time monitoring, Chertoff said. Chertoff's remarks:
http://www.dhs.gov/dhspublic/interapp/testimony/testimony_00 46.xml

---

Category 16.3 *Infrastructure protection & homeland security*

2006-02-15 **FBI Director Robert Mueller RSA Conference cyber threats fluid far reaching foreign agency international law enforcement**

DHS IAIP Daily; http://www.pcworld.com/news/article/0,aid,124741,00.asp# 23

FBI DIRECTOR: CYBER THREATS FLUID AND FAR REACHING.

Hacker hunters need to develop new techniques to take on the latest generation of sophisticated and well-organized cyber criminals, FBI Director Robert Mueller told attendees of the RSA Conference 2006 on Wednesday, February 15. In particular, Mueller said in a keynote address, the FBI must work with corporations and international law enforcement to help combat online criminal acts that are seldom reported. "Increasingly our cyber threats originate outside of the United States," he said. "The once-clear divisions of jurisdiction and responsibility between agencies [and nations]...have been rendered obsolete by the fluid and far-reaching nature of today's threats." The FBI now has more flexibility to work with international law enforcement and is helping build relationships with those foreign agencies by putting operatives "on the ground" in countries that may be hotbeds for cybercrime, according to Steven Martinez, the deputy assistant director for the FBI's Cyber Division, who spoke after Mueller.

Category 16.3 Infrastructure protection & homeland security

2006-02-16 **FBI Director Mueller call partnerships fighting cyber crime**

EDUPAGE; http://www.fcw.com/article92354-02-16-06-Web 23

FBI DIRECTOR CALLS FOR MORE PARTNERSHIPS

Speaking at the RSA Conference this week, FBI Director Robert Mueller called for more partnerships among law enforcement agencies, the private sector, and colleges and universities. Mueller characterized cyberspace as a "largely unprotected frontier with seemingly limitless opportunity," noting that much of that opportunity is exploited by criminals. He said the changing landscape of technology infrastructure makes traditional jurisdictional boundaries obsolete. The FBI now includes a division created in 2002 that focuses exclusively on cybersecurity, and each of the bureau's 56 field offices includes a squad that deals with computer crimes. The FBI has a number of existing programs coordinated with private-sector organizations, but those partnerships need to expand, Mueller said.

16.4 Military & government perspectives on INFOWAR

Category 16.4 *Military & government perspectives on INFOWAR*

1997-01-07 **infowar information warfare**

EDUPAGE

A task force organized by the Defense Science Board recommended that a central authority for information warfare be set up by the U.S. government. The proposal recommends at least $580M in expenditures to harden civilian and military systems against penetration and sabotage. One of the most interesting proposals is that the Pentagon be allowed in law to retaliate against attackers.

Category 16.4 *Military & government perspectives on INFOWAR*

1997-01-10 **InfoWar information warfare**

RISKS 18 75

In January, a Defense Department panel issued a report demanding an additional $3B of spending on information warfare defensive measures to protect the US telecommunications and computing infrastructure. The authors predicted significant attacks on the information infrastructure by the early years of the new millennium.

Category 16.4 *Military & government perspectives on INFOWAR*

2000-02-19 **information warfare**

Central News Agency, Taipei via BBC Monitoring

The Taiwan Research Institute warned that the country should gird itself against information warfare by the People's Republic of China. Elements of IW, they explained, included disruption of critical infrastructure, disruption of military communications, command, control and intelligence (C3I) operations, and misinformation campaigns to damage economic activity and lower morale on the island before initiating conventional warfare.

Category 16.4 *Military & government perspectives on INFOWAR*

2000-06-24 **virus worm information warfare disclosure espionage bungling error mistake**

RISKS, The Times of London http://www.the-times.co.uk/news/pages/sti/2000/06/18/stinwenws01024.html 20 93

Monty Solomon summarized a report in The Times of London about an information warfare experiment gone wrong: "Bungling NATO scientists have created a computer virus "by mistake", causing military secrets to find their way onto the internet. The virus, called Anti-Smyser 1, was created by scientists at NATO'S Kfor peacekeeping force headquarters in Pristina, Kosovo. They were seeking protection from virus attacks similar to those launched at NATO by the Serbs during the Kosovo conflict. But the experiment went wrong, and scientists accidentally unleashed the virus on themselves. The virus, which plucks documents from the hard drives of computers and sends invisible attachments to e-mails, recently resurfaced at the Czech ministry of defence."

Category 16.4 *Military & government perspectives on INFOWAR*

2000-07-13 **unstable operating system operations production**

RISKS, ACM Ubiquity http://www.acm.org/ubiquity/views/m_kabay_3.html 20 95

Much derision resulted from the announcement on 13 July 2000 that the US Navy would be using Windows 2000 for critical control systems on a new nuclear-powered aircraft carrier. [See "Monty Python's Flying Circus: Microsoft and the Aircraft Carriers" (2000-08-15) on the ACM Ubiquity Web site for your editor's comments.]

Category 16.4 *Military & government perspectives on INFOWAR*

2001-05-02 **military information warfare defacement attacks**

NIPC Daily Report

The Air Force has experienced a steady increase in the number of attacks against its information systems, and experts agree that the number of attacks is only going to increase. One reason is the availability, ease of use, and sophistication of publicly available computer-attack software. To combat these threats, the Air Force Office of Special Investigations brings to bear a number of capabilities, including computer crime investigators who specialize in combating crimes against computers and information systems and counterintelligence investigations.

Category 16.4 *Military & government perspectives on INFOWAR*

2001-05-02 **information warfare international Germany hacker attacks CERTs cooperation**

NIPC Daily Report

The German government is planning an early warning system to protect the country's Internet resources against potential international hacker attacks. According to ministry spokesman, Dirk Inger, The Interior Ministry wants to build a network of the Computer Emergency Response Teams (CERTs). Cooperation between CERTs should help prevent major damage from coordinated attacks on German networks, without the necessity of publicizing every hacker attack. German security experts have warned about the potential vulnerability of the country's networks, especially after a recent series of hacker attacks accompanying increased political tension between China and the U.S. (Source: Federal Computer Week, 2 May)

Category 16.4 *Military & government perspectives on INFOWAR*

2001-05-06 **international information warfare conflict political Web vandalism defacement criminal hackers DoS denial of service**

NIPC Daily Report

The ROK Ministry of Information and Communication warned domestic organizations to take precautionary measures against U.S. and Chinese hackers using Korean Internet sites as a stop over to attack each other's computer systems in a cyber war. The ministry warned against the possibility that U.S. and Chinese hackers will try to launch denial of service (DOS) attacks on each other's sites by way of the sites of Korean government agencies, universities, and private institutions. The ministry and the Korea Information Security Agency (KISA) has launched a special task force against possible attacks from U.S. and Chinese hackers. The Ministry and KISA advised operators of domestic Internet sites to report to the "cyber 118" anti-hacking squad if signs of unusually excessive loads of communications are found. (Source: Seoul Yonhap, 6 May)

Category 16.4 *Military & government perspectives on INFOWAR*

2002-02-14 **information warfare critical infrastructure protection counterattack response military action policy prediction**

NewsScan

RESPONSE TO CYBERATTACK ON U.S. COULD INCLUDE MILITARY ACTION
White House technology advisor Richard Clarke told a Senate Judiciary subcommittee that a cyberattack on the United States would be answered "in any appropriate way: through covert action, through military action, any one of the tools available to the president." Clarke pointed out that a serious cyberattack is almost inevitable from the nation's enemies, because it is cheaper and easier than a physical attack. Senator Charles Schumer (D, NY) pointed out the potentially serious consequences of a successful attack over the Internet: "A well-planned and well-executed cyberattack wouldn't just mean the temporary loss of e-mail and instant messaging. Terrorists could gain access to the digital controls for the nation's utilities, power grids, air traffic control systems and nuclear power plants." (AP/USA Today 14 Feb 2002)
http://www.usatoday.com/life/cyber/tech/2002/02/14/cyberterrorism.htm

---

Category 16.4 *Military & government perspectives on INFOWAR*

2002-03-11 **reliability availability battlespace information warfare operating system palmtop handheld**

RISKS, http://www.newscientist.com/news/news.jsp?id=ns99992005 21 94

David Wagner in RISKS: "*New Scientist* is reporting that the US military is planning to deploy palmtops for ground troops to use in transmitting targeting information for air strikes and the like. The application software will be running on top of Windows CE."

Category 16.4 *Military & government perspectives on INFOWAR*

2002-03-11 **military battlefield information warfare battlespace availability reliability**

RISKS, http://insideout.wbur.org/documentaries/reshapingmilitary/ 21 94

Reports from the US Army indicated that new battlefield computers would be used to help soldiers receive battlespace data. An executive officer was quoted on a radio program as saying, "We use nothing but Windows NT systems, that are hardened, to provide HTML products, which are nothing but homepage products, to disseminate the information via regular Internet protocols." Commented a RISKS correspondent, "Gives new meaning to 'Blue Screen of Death' ".

Category 16.4 *Military & government perspectives on INFOWAR*

2002-04-22 **information warfare infowar asymmetrical communications consolidation cooperation hardening networks**

Security Wire Digest 4 31

*ARMY UNITS JOIN FORCES IN IT NETWORK DEFENSE
By Cheryl Balian

The U.S. Army's institutional and tactical divisions, as well as other defense agency partners, are stepping up plans to develop a fully consolidated and more secure computer network.

Military units such as the Space and Missile Defense Command, the Defense Information Systems Agency, and the U.S. Army Signal Command are making the changeover, entitled "The Mannheim Project," a priority as part of a larger information technology merger. The centralized network is designed to provide increased security against asymmetrical warfare that may target the Department of Defense's (DoD) information systems.

"Much greater collaboration is needed," says Lt. Gen. Robert W. Noonan, Jr., the Army's deputy chief of staff for intelligence. The technological framework of government and military agencies like the DoD is considered a ripe target for attacks that could target anything from tactical and personnel information to the network's structure, he adds.

One of the first stages of this informational movement is occurring at the Army Signal Command, which is transforming its operations and will become known as the Network Enterprise Technology Command (Netcom). Netcom will be charged with overseeing and managing day-to-day operations for all of the Army's IT systems and networks. Netcom will also provide regular situation reports to the Army's CIO beginning May 1, but formally launches in October.

One expert cites private industry as a useful role model for securing military and government IT systems, because large companies tend to operate under a framework of free-flowing information and interoperability.

"(The military) should tap into that," said Gilman Louie of In-Q-Tel, a venture capital vehicle established by the Central Intelligence Agency. "They are going to have to deal with industry anyway if they're going to face asymmetrical warfare." Louie stressed that the Army needs to take advantage of the IT processes--including the information sharing model--and infrastructure established by the corporate world to maximize security.

Category 16.4 *Military & government perspectives on INFOWAR*

2002-05-05 **information warfare cyberattacks international infowar**

RISKS, http://www.latimes.com/news/nationworld/world/la-042502china.story 22 05

In May 2002, reports surfaced about U.S. intelligence on Chinese military efforts to launch wide-scale cyber-attacks on American and Taiwanese computer networks, including Internet-linked military systems considered vulnerable to sabotage.

Category 16.4 *Military & government perspectives on INFOWAR*

2002-06-04 **battlespace information warfare infowar**

FindLaw Download This 88

WEB SITE AIDS AFGHAN WAR EFFORTS
The war in Afghanistan is going online. A drab tent under the Afghan sun hides a high-tech war room that soon will become the nerve center of the campaign: Inside, tables are lined with soldiers bent over laptops. . . All are logged onto the Tactical Web Page, a secret, secure website being used in combat for the first time, through which American commanders at Bagram air base and in the United States can direct the fight in Afghanistan.
http://news.findlaw.com/ap/ht/1700/5-30-2002/20020530054502_28.html

Special Coverage: War On Terrorism
http://news.findlaw.com/legalnews/us/terrorism/index.html

Category 16.4 *Military & government perspectives on INFOWAR*

2002-11-15 **infowar information warfare intelligence surveillance spying**

NewsScan

WHAT IS NRO?
NRO, or National Reconnaissance Office, was mentioned in Stephen and Chey Cobb's "Safe & Sound in the Cyber Age" column in NewsScan the other day, and some of readers asked for more information about it. Here is Stephen's elaboration on the topic: Although many Americans have never heard of it, the NRO is probably the biggest of all the U.S. intelligence agencies in terms of dollars spent. Until the '90s the government repeatedly denied the existence of the NRO, which was established by Eisenhower. Some people think the agency would still be secret today if it had not decided to build a very visible $300-million headquarters on the edge of Dulles airport. Serving as the collector of intelligence data, via satellites, spy planes, and other means, the NRO does not have as many direct employees as the slightly better known National Security Agency (with 20,000 workers, the NSA is the largest employer in Maryland). And the NRO budget, publicly listed at $6 billion per year, appears to be less than that of the NSA. But a lot of NSA/CIA/USAF personnel actually work at the NRO, together with a huge band of contractors. And the director of the NRO just happens to control the Pentagon's $68-billion space budget. Remember when a Titan 4 rocket exploded shortly after launch from Cape Canaveral in 1998? The NRO satellite it was carrying was reported to be worth $1 billion. That was only one of many such, not to mention planes, drones, etc. They all generate huge amounts of traffic requiring highly complex networks and massive computing power to handle and digest. Chey Cobb worked on securing those networks and computers. Note that all of the above is unclassified. Here are links to 2 views of the agency: Official: http://www.nro.gov/index1.html Unofficial:
http://www.fas.org/irp/eprint/thompson.html Also note that the unofficial view, while generally critical of the agency, points out recent advances in security as one area of improvement.

Category 16.4 *Military & government perspectives on INFOWAR*

2003-01-22 **battlespace battlefield videophones communications wireless**

NewsScan

PENTAGON TO SUPPLY COMBAT VIDEOPHONES
In an effort to counter hostile propaganda, the Pentagon plans to equip public-affairs officers with two-way videophones, enabling them to set up on-the-spot video interviews with frontline military commanders. The $27,000 Austrian-made Scotty Tele-Transport videophones come in a rugged briefcase that cradles a laptop computer with video-editing and recording capability and includes a built-in camera, a keyboard and a pair of collapsible satellite dish antennas. Television networks have begun using such equipment extensively in the past year, and the Department of Defense and U.S. intelligence agencies already own similar devices. "They have these systems, but they hadn't thought about using it in this kind of way," says Lt. Col. David Lamp, a spokesman for the U.S. Joint Forces Command. "We're finally getting a realization in the world that information is power." Instead of sitting quietly while enemy forces broadcast claims that U.S. forces have bombed a hospital or distributed poisoned emergency food rations to refugees, as happened in Afghanistan, "the best thing to do is to try to manage it, to use it. Commanders who don't do that, or leaders who don't do that, they usually end up learning the hard way." (AP 22 Jan 2003)

Category 16.4 *Military & government perspectives on INFOWAR*

2003-02-07 **cyberattacks retaliation response infowar information warfare homeland defense deterrence policy government**

NewsScan

BUSH SIGNS ORDER AUTHORIZING CYBER-ATTACKS
President Bush has signed a secret order allowing the government to proceed with developing guidelines on circumstances under which the U.S. could launch cyber-attacks against foreign computer systems. The directive signals Bush's desire to pursue new forms of potential warfare — already the Pentagon has moved ahead with development of cyber-weapons that could by used by the military to invade foreign networks and shut down radar, disable electrical facilities and disrupt phone service. (AP 7 Feb 2003)
http://apnews.excite.com/article/20030207/D7P1UJDO0.htm

Category 16.4 *Military & government perspectives on INFOWAR*

2003-02-10 **Department of Defense DOD US computer network attack CNS task force**

NIPC/DHS

February 07, Federal Computer Week — DOD plans network attack task force.

The Defense Department is planning to form a joint task force focused solely on computer network attack (CNA) as part of the ongoing reorganization of U.S. Strategic Command (Stratcom). Stratcom recently acquired oversight of DOD's information operations and global command, control, communications, computer, intelligence, surveillance and reconnaissance (C4ISR) capabilities. Currently, Stratcom's Joint Task Force-Computer Network Operations is charged with defending all DOD networks from attack, as well as initiating cyberattacks when instructed by the president or Defense secretary. However, Stratcom's reorganization also will result in splitting the JTF-CNO into two separate task forces - one focused on computer network defense, and the other on CNA, according to DOD officials. A DOD spokesman said that CNA is "bound by largely the same rules that apply to any war strategy or tactic - very clear rules of engagement (ROE) will prove necessary. "All pieces of the enemy's system of systems that are valid military targets have been - and will be - on the table as we go about war planning," the spokesman said. "It is unimportant whether we take out a computer center with a bomb or a denial-of-service program. If it's critical to the enemy and we go to war, it will be in our sights."

Category 16.4 *Military & government perspectives on INFOWAR*

2003-03-12 **infowar information warfare traffic analysis interception e-mail**

NewsScan

E-MAIL GOES TO WAR
E-mail is a great morale-booster for military personnel, but military historian Keith Eiler worries that "the volume of message traffic can be very dangerous. It's a potentially serious problem and not one that is easily solved." There are fears that enemy forces could obtain a soldier's message home and find ways of misusing it. But though some military advisors have discussed ways of clamping down on personal e-mail from the front lines, Army chief information officer Lt. Gen. Peter M. Cuviello says: "We have not had a problem in Bosnia, Kosovo, Sinai, East Timor, or Korea in recent times, so I don't expect there is going to be a problem," and an Army spokesman in Qatar says, "There are no restrictions on e-mails, it's kind of up to the judgment of the individual person." The father of Army soldier, Gary K. Richardson probably speaks for most families of service men and women, saying that the Internet is "more wonderful than you can imagine. When you get a message, you know that her hands were just on the keyboard and that she was alive and well just a few minutes ago." (New York Times 12 Mar 2003)

Category 16.4 *Military & government perspectives on INFOWAR*

2003-03-14 **Iraq war satellite communication jam subvert GPS US**

NIPC/DHS

March 12, Associated Press — Iraqis could try to jam satellite signals.

Iraq could try to jam U.S. military satellite signals during a possible invasion, but the United States has defenses against such attempts, Pentagon officials said Wednesday. Iraq also reportedly is seeking ways to jam the Global Positioning Satellite (GPS) signals that help guide U.S. bombs. At the Pentagon, Brig. General Franklin Blaisdell and Army Col. Steven Fox promoted what they said was America's dominance of space as a key strength in any future military operations. Satellites allow U.S. commanders to see what is going on in hostile countries, communicate with soldiers and pilots, and guide precision weapons. The Army has more than 1,000 transmitters that help it keep track of soldiers and units while a battle is going on, Fox said. As it did during the 1991 Persian Gulf War, the Defense Department is buying access to commercial communications satellites to help serve the massive bandwidth needed to connect all the high-tech gear, Blaisdell said. The military also successfully launched a broadband communications satellite on Monday, he said.

Category 16.4 *Military & government perspectives on INFOWAR*

2003-03-28 **US Army Defense Message System DMS faster secure e-mail**

NIPC/DHS

March 27, Federal Computer Week — Army taps DMS for wartime comm.

The Army recently implemented the Defense Message System (DMS) to provide users with better-protected and faster communications than e-mail over the Defense Department's Secret Internet Protocol Router Network (SIPRNET). DMS messages travel over the Defense Information Systems Network, which distributes voice, video and data messages. The system - a $1.6 billion effort to secure DOD communications worldwide - is designed to provide writer-to-reader service for classified and top-secret information, delivering messages to DOD users at their desktops and to other agencies and contractors, if necessary. Retired Air Force Master Sgt. Arthur Edgeson, senior systems engineer at the Fort Detrick, MD, office of Data Systems Analysts Inc., said DMS became active at Camp Doha (Kuwait) at the end of last month and has experienced a noticeable increase in traffic since Operation Iraqi Freedom began March 20. "Yes, SIPR e-mail is classified, but it could be hacked into. Or if we're overrun by the enemy, they would have access to the computers and could send messages...to mislead or misdirect [coalition] forces," said Edgeson. Edgeson acknowledged that DMS still has bugs to work out and that many DOD users remain faithful to Autodin, another system. But Autodin does not allow users to include attachments. It requires users to pick up messages at a central message center twice daily and is run on antiquated equipment. DMS may not be perfect, but it can send and receive all messages for both systems and deliver them to the user's desktop quickly and securely, Edgeson said. The other military services also are using DMS, but each has its own time lines, personnel and priorities, he said.

Category 16.4 *Military & government perspectives on INFOWAR*

2003-04-02 **Iraq war computer cyber warfare information virus scanning Army**

NIPC/DHS

March 31, Federal Computer Week — Cyberwarriors guard virtual front.

As coalition forces continue to engage the enemy throughout Iraq, the number of battles being fought in cyberspace also has risen, according to one Army information assurance officer. Col. Mark Spillers, information assurance program manager in the Coalition Forces Land Component Command communications office at Camp Doha, Kuwait, said "if a device is thought to be compromised, it is immediately isolated, taken off the network and scanned for viruses." Spillers said he could not go into any details about how the Army is protecting its systems or if any have been compromised." On the physical battlefield, if troops are in danger of being defeated, procedures are in place to safeguard or even destroy endangered equipment and systems to keep sensitive data from falling into enemy hands.

Category 16.4 *Military & government perspectives on INFOWAR*

2003-04-02 **Iraq war communication network Internet computer hardware software intelligence support**

NIPC/DHS

March 29, Washington Post — Computer support staff at home is crucial to war effort.

To a greater extent than any war before it, Operation Iraqi Freedom depends on an elite group of technicians, engineers and other specialists in the United States who are standing by 24 hours a day, seven days a week to assist the troops. Pentagon officials have called this conflict a "network centric" one, with computers and wireless technology linking intelligence from the 250,000 U.S. troops and the drones, tanks, planes and other vehicles in a way that has compressed decision-making from what in the past might have been days into minutes. A single mix-up, glitch or crash in the technology could cost lives. So far, the technology has held up well, and there have been few major problems, according to about a dozen of the contractors who provide technical support services to the military. Working in classified "safe rooms" or reachable via pagers and cell phones around the country, they have been working behind the scenes to make sure the multitude of software and hardware systems is working properly.

Category 16.4 *Military & government perspectives on INFOWAR*

2003-04-11 **physical infrastructure attack Iraq war bomb communication Corporate America disaster recovery**

NIPC/DHS

April 08, Security Net — Physical attack still the biggest threat.

Baghdad's telecommunications infrastructure fell silent during the first week of April under a rain of precision-guided bombs. U.S. and British planes targeted phone facilities and other critical pieces of the Iraqi communications infrastructure to isolate the leadership from the levers of power. The U.S. military chose to use bombs — not hackers — to drop Iraqi networks for a reason. Nothing brings a network to a halt more easily and quickly than physical damage. Yet as data transmission becomes the lifeblood of Corporate America, most big companies haven't performed due diligence to determine how damage-proof their data lifelines really are. Only 20% of midsize and large companies have seriously sussed out what happens to their data connections after they go beyond the company firewall, says Peter Salus of MatrixNetSystems, a network-optimization company based in Austin, TX. The collapse of the World Trade Center left most of Lower Manhattan, the epicenter of the global financial system, without data connections for a week or more. Many of the affected companies thought they were covered for any eventuality, having contracted for not one but two high-capacity data connections from their offices. Redundancy doesn't help much, however, if your connections pass through the same geographical location. Unfortunately, massing huge chunks of connectivity in so-called "telecom hotels" is the norm.

Category 16.4 *Military & government perspectives on INFOWAR*

2003-04-22 **government Infosec White House security advisor resigns**

NewsScan

WHITE HOUSE SECURITY ADVISER RESIGNS
Howard Schmidt, the former Microsoft security chief who became White House cybersecurity adviser in February following Richard Clarke's departure from that office, has tendered his resignation, saying: "While significant progress has been made, there still is much to do. The nation as a whole is much better at responding to cyberattacks then at any time in the past, but cybersecurity cannot now be reduced to a `second tier' issue. It is not sufficient to just respond to attacks, but rather proactive measures must also be implemented to reduce vulnerabilities and prevent future attacks." (AP/San Jose Mercury News 22 Apr 2003)

Category 16.4 *Military & government perspectives on INFOWAR*

2003-05-14 **cyber R&D DHS center Charles McQueary cybersecurity cyberterrorism**

NIPC/DHS

May 14, Federal Computer Week — DHS creating cyber R & D center.

Charles McQueary, the under secretary for Department of Homeland Security 's (DHS) Science and Technology Directorate, told the House Science Committee Wednesday that the DHS is creating a research and development center to coordinate cybersecurity efforts across civilian and defense agencies, universities, and the private sector. In an effort to help develop state-of-the-art and low-cost technology to prevent cyberterrorism, the DHS center will partner with the National Science Foundation and the National Institute of Standards and Technology, two federal agencies that deal with R & D, as well as with academic institutions and private corporations. "The center will foster national and international cooperation in creating a robust and defensible cyber infrastructure," McQueary said. DHS spokesman David Wray said there is no date yet for the start-up of the cybersecurity center.

Category 16.4 *Military & government perspectives on INFOWAR*

2003-07-03 **Illinois supercomputer cybersecurity thwart hackers NCSA battlefield communications**

NIPC/DHS

July 03, Associated Press — Illinois supercomputer center to head military cybersecurity effort.

Hoping to thwart hackers, the military is launching a new research effort at the University of Illinois to improve the security of battlefield computers and communications systems. Officials at the school's National Center for Supercomputing Applications (NCSA) on Thursday announced an initial $5.7 million grant from the Office of Naval Research to establish a new research center to develop technology against enemy hackers, NCSA director Dan Reed said. Other research projects will include developing remotely programmed radios and refining ways for monitoring battlefield environments. The NCSA is a high-performance computing center that develops and deploys computing, networking and information technology for government and industry. Software developers will try to determine the best way to share information among military forces without fear of interception. The government also is seeking a framework for determining quickly when and how a computer network is under attack, Reed said.

Category 16.4 *Military & government perspectives on INFOWAR*

2003-07-29 **new jersey army intrusion detection systems IDS cyberterrorism**

NIPC/DHS

July 29, InformationWeek — New Jersey teams with the Army on intrusion detection.

The Army will help New Jersey analyze the state's network as a step in developing an intrusion-detection system. The agreement with the U.S. Army Communications-Electronics Command Research, Development, and Engineering Center based at Fort Monmouth, NJ, is the first such collaboration between the center and a state. Charles Dawson, New Jersey's chief technology officer, says a comprehensive intrusion-detection program is a key component in the state's homeland security plans to protect its IT infrastructure from cyberterrorism. The technical components of the program include host-based intrusion-detection systems, network-based intrusion-detection systems, and security information-management systems. The state also will receive guidance in developing policies and procedures to effectively manage the program.

Category 16.4 *Military & government perspectives on INFOWAR*

2004-02-27 **virtual war games military exercises Navy battle**

NewsScan

VIRTUAL WAR GAMES

Three aircraft carriers at Navy bases on both U.S. coasts are engaged this week in a virtual war game that uses computers to simulate battle conditions at sea. Vice Adm. Albert H. Konetzni Jr. says: "This will bring war-gaming to a new level. It will put the operators, the players, under great stress. They will be making decisions that are truly, truly critical to the carrying out of the operations, and it allows the operators, even down to the unit level, to really understand how they play in these scenarios." One of the participants in the exercise says: "We're trying to simulate all conditions of warfare that we could encounter: mine, surface, air, asymmetric threats like a small boat attack. All that stuff that could be damaging to the Navy is put forward into this war game." (San Jose Mercury News 27 Feb 2004)

Category 16.4 *Military & government perspectives on INFOWAR*

2004-04-23 **cyber war game Army information warfare West Point NSA**

DHS IAIP Daily;
http://www.reuters.com/newsArticle.jhtml?type=technologyNews
&storyID=4897789&section=news

April 21, Reuters — Army confronts enemies within in cyber war game.

The mission: to secure an entire computer network for the United States and its allies against a vague enemy force. Hostile agents aim to wreak havoc on military plans, sabotaging databases, computer terminals and communications. But the cyber warriors planning a best defense aren't analysts hunkered down at the Pentagon. They are cadets at West Point competing against military academies and other schools in a four-day Cyber Defense Exercise this week. And the "enemy" isn't al Qaeda or Iraqi insurgents. It's a team led by none other than the National Security Agency (NSA). The NSA team, known as the "Red Cell," launches attacks on selected networks at the Air Force, Army, Coast Guard, Merchant Marine and Naval academies from an operations center somewhere in Maryland. The computer scenario plays out virtually inside the cadets' computers. Going on the offensive, or using so-called hackback techniques, is against competition rules. Also out-of-bounds are forms of sabotage in which computers can be turned into zombies and used to attack opponent machines with millions of data messages, shutting down communication.

Category 16.4 *Military & government perspectives on INFOWAR*

2004-05-12 **war games military academy NSA cyber defense**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/25867−1.html

May 12, Government Computer News — Merchant Marine Academy wins cybersecurity exercise.

The United States Merchant Marine Academy (USMMA) won out over four other service academies recently in a cybertraining exercise organized by the National Security Agency (NSA) and the United States Military Academy at West Point. During the Cyber Defense Exercise, a team of cadets from each academy had to design, build and configure a computer network that simulated a deployed joint services command. NSA and Department of Defense security experts tested the networks over a four-day period, attempting intrusions and identifying vulnerabilities. Teams were evaluated on maintaining services and their ability to recover from and prevent future security breaches, according to an NSA release. NSA found that the USMMA's network was stronger and more flexible then the 2003 champion, the U.S. Air Force Academy. Other teams participating were West Point, a former two-time winner; the U.S. Coast Guard Academy; and the U.S. Naval Academy.

Category 16.4 *Military & government perspectives on INFOWAR*

2004-05-13 **broadband access bandwidth federal government DISA**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/25882−1.html

May 13, Government Computer News — DISA seeks bandwidth tech ideas.

The Defense Information Systems Agency (DISA) is seeking industry feedback on technologies that will add bandwidth to the Defense Information Systems Network (DISN). Under the DISN Access Transport Services request for information, released last week, the Defense agency is looking to industry for ideas to upgrade the older network at roughly 600 sites so it can be integrated with the $900 million Global Information Grid-Bandwidth Expansion program. As part of the DISN upgrade, many legacy voice, data and video systems, as well as emerging capabilities—such as the department's premier network-centric warfare initiatives—will move to operate over IP. DISN currently operates via a switched-circuit transport system. According to the RFI, which closes on May 24, DATS will provide leased access transmission services between the government-owned backbone network and customer locations. The transmission services will be required to support bandwidths up through OC-192. The DATS contract will provide similar services to two current DISA contracts that are expiring over the next two years, including the DISN Transmission Services CONUS (Continental United States) contract and the DISN Switched/Bandwidth Manager Services CONUS contract.

Category 16.4 *Military & government perspectives on INFOWAR*

2004-05-17 **computer security US army military network defense**

DHS IAIP Daily; http://www.fcw.com/fcw/articles/2004/0517/news−army−05−17−04 .asp

May 17, Federal Computer Week — Army-wide security plan takes shape.

The Army will devise a servicewide computer security plan to boost protection of its information technology assets, according to Army and industry officials. Army officials say they want to develop a strategy that treats all systems as part of a cohesive enterprise, rather than securing each system individually. They realized the need for such a plan when they began taking an enterprise approach to managing their hardware and software, officials said. Their participation in military network defense groups also raised their awareness about the importance of cybersecurity, they said. Top Army IT officials, citing Army policies, would not confirm that their networks have seen more cyberattacks during the past five months. "The military typically experiences increases in computer network attacks when the geopolitical climate is the way it is," said Lt. General Steve Boutelle, the Army's chief information officer.

Category 16.4 *Military & government perspectives on INFOWAR*

2004-08-04 **cyber terrorism information asymmetrical warfare China Russia US Homeland Security concern**

DHS IAIP Daily; http://www.usatoday.com/tech/news/2004−08−02−cyber−terror_x. htm

August 04, USA TODAY — Cyberterror impact, defense under scrutiny.

A coordinated cyberattack against the U.S. could topple parts of the Internet, silence communications and commerce, and paralyze federal agencies and businesses, government officials and security experts warn. Such an attack could disrupt millions of dollars in financial transactions, hang up air traffic control systems, deny access to emergency 911 services, shut down water supplies and interrupt power supplies to millions of homes, security experts say. But from whom the attacks would come is unclear. Intelligence shows al Qaeda is more fixated on physical threats than electronic ones, government officials and cybersecurity experts say. That hasn't dissuaded other groups and nations from eyeing cyberterrorism as a means to damage the U.S., whose infrastructures are increasingly tied to the Internet. "There are a large number of threats: hackers, cybercriminals, other countries," says Amit Yoran, director of the Department of Homeland Security's National Cyber Security Division. "It goes beyond al Qaeda." More than two dozen countries, including China and Russia, have developed "asymmetrical warfare" strategies targeting holes in U.S. computer systems. Because of U.S. military firepower, those countries see electronic warfare as their best way to pierce U.S. defenses, military experts say.

Category 16.4 *Military & government perspectives on INFOWAR*

2004-10-04 **Korea INFOWAR information warfare hackers**

NewsScan; http://news.ft.com/cms/s/3d592eb4-15f0-11d9-b835-00000e2511c8.html

SOUTH KOREA VULNERABLE TO CYBER ATTACKS FROM NORTH

South Korea's defense ministry says that North Korea has trained hundreds of computer hackers who could launch a cyber-war on South Korea, the US or Japan. Because South Korea has the world's highest usage of broadband services yet maintains relatively low levels of Internet security, the country is especially vulnerable to network attacks.

Category 16.4 *Military & government perspectives on INFOWAR*

2004-10-04 **North Korea international Level 1 cyberwarfare 500 trained computer hackers**

DHS IAIP Daily; http://www.channelnewsasia.com/stories/afp_asiapacific/view/109911/1/.html

October 04, Agence France Presse — North Korea ready to launch cyber war: report.

North Korea has trained more than 500 computer hackers capable of launching cyber warfare against the United States, South Korea's defense ministry says. In a report to the National Assembly's National Defense Committee, the ministry said that hackers from North Korea were among the best in the world.

Category 16.4 *Military & government perspectives on INFOWAR*

2004-10-20 **US Canada NORAD security role join forces marine cyber security collaboration**

DHS IAIP Daily; http://www.alertnet.org/thenews/newsdesk/N20568513.htm

October 20, Reuters — U.S., Canada seen broadening NORAD security role.

The United States and Canada are considering expanding their joint aerospace command to cover maritime and and cyber-security, U.S. Ambassador Paul Cellucci said on Wednesday, October 20. The North American Aerospace Defense Command (NORAD) was established to protect against Soviet bombers and was activated during the September 11 attacks on the United States, but it needs to take on a broader mandate, Cellucci said. "We believe that NORAD, which has been there for over 40 years protecting the airspace ... that in the age we live in we also have to be very concerned about marine security (and) cyber-security," he said.

Category 16.4 *Military & government perspectives on INFOWAR*

2004-10-21 **international cyberterrorism possibility 2006**

DHS IAIP Daily; http://news.zdnet.co.uk/internet/0,39020369,39170864,00.htm

October 21, ZDNet (UK) — Cyberterrorism a possibility in two years.

Cyberterrorism could become a reality in 2006, a leading UK information security expert has said. Speaking at the SC Magazine Conference in London on Thursday, October 21, director of information security for Royal Mail David Lacey said that that the world would witness cyberterrorism within two years. Lacey said, “there is a lot of consistency in research that shows many of the real risks won't come to a crescendo until then. We know a lot about some of the trends coming. Real terrorists have not had the capability to carry out threats. But that will change as the stakes get higher."

Category 16.4 *Military & government perspectives on INFOWAR*

2004-11-12 **DARPA military intelligence counterintelligence war ideas computer information warfare**

DHS IAIP Daily; http://www.fcw.com/fcw/articles/2004/1108/web−darpa−11−12−04 .asp

November 12, Federal Computer Week — DARPA wants info about war ideas.

Defense Advanced Research Projects Agency (DARPA) officials want ideas on using computational techniques to disrupt enemy leaders' decision-making processes. DARPA officials want papers on the topic by December 10. They will choose the best ones and ask the authors attend a meeting in late January 2005. Military officials' growing emphasis on information warfare precipitated the request. Notice posted at: http://www2.eps.gov/spg/ODA/DARPA/CMO/SN05%2D09/Synopsis.htm l

---

Category 16.4 *Military & government perspectives on INFOWAR*

2005-02-28 **cyberdefense antiterrorism command center Joint Task Force-Global Network Operations (JTF-GNO) military computer network DoD**

DHS IAIP Daily; http://www.fcw.com/fcw/articles/2005/0221/web−jtfg−02−25−05. asp

CYBER WARRIORS ANTICIPATE CENTER.

Personnel in the military's new cyberdefense organization hope to operate a new command center by late spring. The facility will include new hardware and software to help workers of the Joint Task Force-Global Network Operations (JTF-GNO) operate, manage and defend the military's 10 computer networks. "It will be a state-of-the-art facility," said Army Brig. Gen. Dennis Via, deputy commander of the JTF-GNO. He spoke Wednesday, February 23 at the Department of Defense Global Information Grid Enterprise Services conference held by the Association for Enterprise Integration, an industry trade group. The opening of the new command center coincides with JTF-GNO becoming fully operational.

Category 16.4 *Military & government perspectives on INFOWAR*

2005-04-07 **US official warning Chinese intelligence Latin South America trade economic cyberwarfare capability Level-1 INFOWAR**

DHS IAIP Daily; http://www.miami.com/mld/miamiherald/11332057.htm

U.S. OFFICIALS WARN OF CHINESE INTELLIGENCE AND CYBERWARFARE ROLES IN LATIN AMERICA

U.S. officials said Wednesday, April 6, there is no evidence that China is seeking to boost its military presence in Latin America, but for the first time warned about Chinese intentions to establish an intelligence and cyberwarfare beachhead in the region. Roger Noriega, assistant secretary of state for Latin America, and Rogelio Pardo-Maurer, the top Defense Department official for the Western Hemisphere, testified before a House panel as several legislators argued that China is trying to fill the void left by the lack of U.S. involvement in the region. Noriega and Pardo-Maurer said China's interests in Latin America were mostly on the economic side, but warned that Beijing could also have an intelligence agenda as it increased trade with Latin America. Pardo-Maurer said that "we need to be alert to rapidly advancing Chinese capabilities, particularly in the fields of intelligence, communications and cyberwarfare, and their possible application in the region." This is the first time that a senior Pentagon official warned so directly about Chinese cyberwarfare capabilities in the region.

Category 16.4 *Military & government perspectives on INFOWAR*

2005-08-30 **US Army military perspective INFOWAR blogging disintermediation Web sites classified sensitive information**

EDUPAGE; http://www.fcw.com/article90522-08-30-05-Web

ARMY ON THE LOOKOUT FOR SENSITIVE INFO ONLINE U.S.

Army officials have said they will take a closer look at blogs and Web sites maintained by soldiers. Many such blogs and Web sites include photographs or other information that inadvertently exposes classified or sensitive information to anyone with access to the Internet. Gen. Peter Schoomaker, the Army's chief of staff, noted that soldiers routinely post pictures online that include "tactics, techniques, and procedures" for weapons systems. According to Richard Cody, Army vice chief of staff, "The enemy is actively searching the unclassified networks for information, especially sensitive photos." Schoomaker issued a memo saying that the Army will work to closely monitor Web sites and blogs to avoid operational security violations, which "needlessly place lives at risk and degrade the effectiveness of our operations." Federal Computer Week, 30 August 2005

Category 16.4 *Military & government perspectives on INFOWAR*

2005-10-20 **DOD Wilma military industry alert telephone wireless networks DataPath Qualcomm**

DHS IAIP Daily; http://fcw.com/article91167−10−20−05−Web

DOD, INDUSTRY ON ALERT FOR WILMA

The Defense Department has put military and industry teams on alert to provide communications if Hurricane Wilma disrupts the operation of telephone and wireless networks in the country. According to Brig. Gen. Nick Justice, deputy program executive officer in the Army's Program Executive Office for Command, Control, Communications-Tactical (PEO-C3T), " Teams are standing up right now at Fort Monmouth, NJ." In addition, Army signal units, which operate the service's battlefield communications systems, are also on call. According to Brig. Gen. Carroll Pollett, commanding general of the Army's Network Enterprise Technology Command and 9th Army Signal Command located at Fort Huachuca, AZ. In addition, Industry officials with DataPath and Qualcomm said they have personnel and equipment ready to provide communications with the Army.

Category 16.4 *Military & government perspectives on INFOWAR*

2005-12-13 **research report hacker attack US network Chinese military information warfare INFOWAR**

DHS IAIP Daily; http://www.physorg.com/news8992.html

RESEARCHERS: HACKER ATTACKS IN U.S. LINKED TO CHINESE MILITARY

A systematic effort by hackers to penetrate U.S. government and industry computer networks stems most likely from the Chinese military, the head of a leading security institute said. The attacks have been traced to the Chinese province of Guangdong, and the techniques used make it appear unlikely to come from any other source than the military, said Alan Paller, the director of the SANS Institute, an education and research organization focusing on cybersecurity. In the attacks, Paller said, the perpetrators "were in and out with no keystroke errors and left no fingerprints, and created a backdoor in less than 30 minutes. How can this be done by anyone other than a military organization?" Paller said that despite what appears to be a systematic effort to target government agencies and defense contractors, defenses have remained weak in many areas. Security among private-sector Pentagon contractors may not be as robust, said Paller, because "they are less willing to make it hard for mobile people to get their work done." The U.S. military has code-named the recent hacker effort "Titan Rain" and has made some strides in counter-hacking to identify the attackers, Paller said.

Category 16.4 *Military & government perspectives on INFOWAR*

2006-01-16 **military security efforts Joint Task Force JTF DISA DoD**

DHS IAIP Daily; http://www.networkworld.com/news/2006/011606−military−security.html 23

MILITARY CLAMPING DOWN ON SECURITY

Lt. General Charles Croom, commander of the Joint Task Force (JTF) on Global Network Operations (GNO) and director of the Defense Information Systems Agency (DISA), last week said a sweep is underway of all Department of Defense (DoD) networks to uncover security holes amid a get-tough policy. “The attacks are coming from everywhere and they’re getting better, ” said Croom in his keynote address at the DoD Cyber Crime Conference last week. The discovery of a botnet last November 5th inside DoD networks contributed to the decision to clamp down security. So far, the results are troubling. “Almost 20 percent of our accounts are unauthorized or had expired,” Croom said, noting that military personnel tend to move every two or three years and accounts are sometimes left open. The exact tally of improper accounts won’t be known until March, he said. The biggest changes to come may be in the next six months as the JTF-GNO, the organization set up to centralize decisions about security and operations in the Army, Navy, Air Force and Marines, evaluates a possible redesign of its two primary global IP-based military networks.

Category 16.4 *Military & government perspectives on INFOWAR*

2006-01-27 **information warfare INFOWAR United States US**

DHS IAIP Daily; http://www.fcw.com/article92121−01−27−06−Web 23

EXPERTS: COUNTRIES MAKE DANGEROUS CYBER ADVERSARIES.

When other countries launch cyber attacks, the United States should expect to see more robust ways to crack systems and more dangerous methods to manipulate them, two cybersecurity experts said Thursday, January 26. Countries have many resources and can attack at least as effectively as independent cybercriminals can, said Matthew Devost, president and chief executive officer of the Terrorism Research Center. China, North Korea and Russia already use cyber attacks to advance their interests, Devost said, speaking on a panel at the Black Hat Federal conference in Arlington, VA. Cyber attacks from countries can be difficult to investigate because analysts may not be able to tell if a given country is launching the attack or if other organizations are attacking through the country’s resources, he said. Countries and terrorist organizations can have a different perception of time than other cyber attackers do, Devost said. They can wait years, performing reconnaissance and placing agents inside target organizations to find vulnerabilities, he said. Preparation is important to stopping attacks from other countries, said Tom Parker, security research group manager at MCI. Organizations must anticipate their adversaries’ actions and look at all data, attack profiles and threat types, he said.

Category 16.4 *Military & government perspectives on INFOWAR*

2006-02-03 **hacker Greek government phone tap wiretapping illegal software Vodafone**

DHS IAIP Daily; http://news.zdnet.com/2100−1009_22−6034895.html 23

HACKERS TAP GREEK GOVERNMENT CELL PHONES.

Unknown eavesdroppers tapped the cell phones of Greek Prime Minister Costas Karamanlis, five cabinet members and dozens of top officials for about a year, the Greek government said on Thursday, February 2. Illegal software installed at Greece's second biggest mobile phone operator, Vodafone Greece, allowed calls to and from about 100 phones to be recorded. Most belonged to the government but one was owned by the U.S. embassy in Athens, officials said. "The phones tapped included the prime minister's, the whole leadership of the defense ministry and the whole leadership of the public order ministry, some foreign ministry phones, one former minister, now in opposition, and others," government spokesperson Theodore Roussopoulos told a news conference. The wiretaps lasted from just months before the 2004 Athens Olympics until March 2005, when Vodafone Greece discovered the incident. "As soon as we discovered the phone-tapping software, we removed it and informed the state, as was our obligation," George Koronias, head of Vodafone Greece, said in a statement. But the shutdown of the illegal software in the Vodafone system wiped out all traces of how and from where it had been installed, Public Order Minister George Voulgarakis told the news conference.

Category 16.4 *Military & government perspectives on INFOWAR*

2006-02-06 **China hacker attack UK Parliament Windows WMF vulnerability information warfare INFOWAR**

DHS IAIP Daily; 23
http://computerworld.co.nz/news.nsf/scrt/AFAC1C3187BF9027CC2
5710900773FD8

CHINA ATTACKS UK PARLIAMENT USING WINDOWS SECURITY HOLE.

Chinese hackers attacked the UK Parliament in January, the government's e-mail filtering company, MessageLabs, has confirmed. The attack, which occurred on January 2, attempted to exploit the Windows Meta File (WMF) vulnerability to hijack the PCs of more than 70 named individuals. E-mails were sent to staff with an attachment that contained the WMF-exploiting Setabortproc Trojan. Anyone opening this attachment would have enabled attackers to browse files and possibly install a key-logging program to attempt the theft of passwords. None of the e-mails got through to the intended targets, MessageLabs says, but the UK authorities were alerted. MessageLabs said the e-mails had been traced to servers in China's Guangdong Province, hence the suspicion that the latest attack was part of a more general campaign of electronic subversion. This is not the first time the UK Government has come under Trojan attack from China. Last summer, the National Infrastructure Security Coordination Center (NISCC) reported that UK government departments had been hit by a wave of Trojans originating in China.

Category 16.4 *Military & government perspectives on INFOWAR*

2006-02-10 **DHS Cyber Storm exercise evaluation**

DHS IAIP Daily; 23
http://www.techweb.com/wire/security/179103522;jsessionid=WO
VM0LSQLDIUSQSNDBCSKHSCJUMEKJVN

DHS WEATHERS CYBER STORM.

The U.S. Department of Homeland Security (DHS) still has to evaluate how well it fared through a series of simulated cyber attacks this week, but government and private companies avoided real-world damage and complications during their preparedness exercise. More than 100 public, private and international groups participated in mock attacks replicating the invasion of a utility company's computer system and the disruption of power grids. The exercise, called Cyber Storm, was designed to test the abilities of private companies and government agencies to deal with a major cyber security incident. DHS announced the completion of the exercise on Friday, February 10, but has yet to fully evaluate how effectively the groups communicated, cooperated and responded. Participants will evaluate the exercise, gauge interagency coordination and try to identify how current policies would affect response and recovery in the event of a real attack. The lessons learned this week are expected to be incorporated into a National Response Plan, which could be used if real attacks occur.

Category 16.4 *Military & government perspectives on INFOWAR*

2006-03-02 **Israel software company Check Point Technologies US acquisition investigation govt secrets Snort IDS**

DHS IAIP Daily; 23
http://www.forbes.com/entrepreneurs/feeds/ap/2006/03/02/ap25 64113.html

ISRAELI SOFTWARE COMPANY FACES U.S. PROBE.

Days after the Bush administration approved a ports deal involving the United Arab Emirates, the same review panel privately notified an Israeli software company it faced a rare, full-blown investigation over its plans to buy a smaller U.S. rival. The company was told U.S. officials feared the transaction could endanger some of the government's most sensitive computer systems. The objections by the Federal Bureau of Investigations and Pentagon were partly over specialized intrusion detection software known as "Snort," which guards some classified U.S. military and intelligence computers. Snort's author is a senior executive at Sourcefire Inc. based in Columbia, MD, which would be sold to publicly traded Check Point Software Technologies Ltd. in Ramat Gan, Israel.

Category 16.4 *Military & government perspectives on INFOWAR*

2006-03-08 **Internet cloaking Web security threats bogus terrorist criminal Websites**

DHS IAIP Daily; http://www.gcn.com/online/vol1_no1/40075−1.html 23

INTERNET "CLOAKING" EMERGES AS NEW WEB SECURITY THREAT.

Terrorist organizations and other national enemies have launched bogus Websites that mask their covert information or provide misleading information to users they identify as federal employees or agents, according to Lance Cottrell, founder and chief scientist at Anonymizer of San Diego, CA. The criminal and terrorist organizations also increasingly are blocking all traffic from North America or from Internet Protocol addresses that point back to users who rely on the English language, Cottrell told an educational seminar in Washington at the FOSE 2006 trade show's Homeland Security Center Tuesday, March 7. Among the risks of the terrorist cloaking practice are that the organizations can provide bogus passwords to covert meetings. By doing so they can pinpoint federal intelligence agents who attend the meetings, making them vulnerable to being kidnapped or becoming the unwitting carriers of false information, Cottrell said.

Category 16.4 *Military & government perspectives on INFOWAR*

2006-03-24 **Check Point Software Technology Israel Internet security company acquisition withdrawn protect US Department of Defense DoS NSA**

DHS IAIP Daily; 23
http://www.infoworld.com/article/06/03/24/76772_HNcheckpoint
withdraws_1.html

CHECK POINT WITHDRAWS BID FOR SOURCEFIRE.

Check Point Software Technologies, an Israeli-owned Internet security company, on Thursday, March 23, withdrew its application to acquire intrusion-prevention firm Sourcefire, whose technology is used to protect the computer assets of the U.S. Department of Defense and the U.S. National Security Agency. This comes amid national security concerns voiced by the Federal Bureau of Investigations and the Department of Defense.

Category 16.4 *Military & government perspectives on INFOWAR*

2006-04-11 **Internet sociology role terrorism recruitment Europe**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/story/0 23
,10801,110417,00.html

WEB ROLE EXAMINED IN LONDON, MADRID BOMBINGS.

Investigations into the Madrid and London bombings highlight two worrying trends for European security services -- the emergence of autonomous, homegrown radical cells and their skilled exploitation of the Internet. "It is quite clear that the Internet is playing an ever greater role in radicalization and recruitment, and indeed also in facilitating the practical planning [of attacks]," European Union counterterrorism chief Gijs de Vries told a conference in Berlin last week. The Islamic militants involved in the Madrid attacks, for example, derived inspiration from an Islamist Website. In addition, the suicide bombers involved in last July's London attacks developed their plan using information they obtained from the Internet; they were not part of an international terror network.

Category 16.4 *Military & government perspectives on INFOWAR*

2006-04-13 **portable computer drives peddled Bagram Air Base Afghanistan sensitive information disclosure**

DHS IAIP Daily; http://www.msnbc.msn.com/id/12305580/ 23

PORTABLE COMPUTER DRIVES PEDDLED AT BAZAAR OUTSIDE BAGRAM AIR BASE, AFGHANISTAN.

This week in Bagram, Afghanistan, an NBC News producer, using a hidden camera, visited a bazaar and bought a half dozen of the memory drives the size of a thumb known as flash drives. Some of the discovered data would be valuable to the enemy, including: Names and personal information for dozens of Department of Defense interrogators; documents on an " interrogation support cell" and interrogation methods; IDs and photos of U.S. troops. The tiny computer memories are believed to have been smuggled off base by Afghan employees and sold to shopkeepers. Whoever buys one can simply plug it into another computer, and in a couple of minutes, see thousands of files.

Category 16.4 *Military & government perspectives on INFOWAR*

2006-04-13 **terrorist Web chatter Internet privacy concern proxy server**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/content/article/2006/04/12/AR2006041201968.html?nav=rss_technology/special/08 23

TERRORISTS' WEB CHATTER SHOWS CONCERN ABOUT INTERNET PRIVACY.

Terrorist groups, which for years have used the Internet and its various tools to organize and communicate, are paying more attention to addressing security and privacy concerns similar to those of other Web users, counterterrorism experts say. Recently, postings on jihadist Websites have expressed increasing concern about spyware, password protection, and surveillance on chat rooms and instant-messaging systems. One forum recently posted a guide for Internet safety and anonymity on the Internet, advising readers of ways to circumvent hackers or government officials. "The Shortened Way of How to be Cautious; To the User of the Jihadi Forums, In the Name of Allah, the most Gracious and Merciful" was posted last month by an al-Qaeda-affiliated group calling itself the Global Islamic Media Front. The posting advised Internet cafe users to set up a proxy -- a software program that erases digital footsteps such as Web addresses or other identifiable information -- before Web surfing. "There's a lot of things like that," said Evan Kohlmann, a consultant on international terrorism. Last month, Kohlmann said, he found a jihadist Website posting pirated McAfee anti-spyware software, which the site encouraged users to download to avoid monitoring.

Category 16.4 *Military & government perspectives on INFOWAR*

2006-05-02 **US businesses WTO Russia talks intellectual property rights enforcement weak**

EDUPAGE; http://www.abcnews.go.com/Politics/wireStory?id=1914448 23

BUSINESS GROUPS URGE CAUTION IN WTO TALKS WITH RUSSIA

U.S. businesses urged the Office of the United States Trade Representative to demand more efforts from Russia in addressing intellectual property crimes before granting approval for the country to join the World Trade Organization (WTO). Russia, with one of the largest global economies not represented in the WTO, is in bilateral talks with the United States over admission to the group. Industry organizations point to Russia as one of the worst offenders for piracy of copyrighted music, movies, and software and called on U.S. officials to take a tough stance. Eric Schwartz, vice president of the International Intellectual Property Alliance, said, "Enforcement at present is very, very weak." Businesses calling for renewed pressure on Russia pointed to proposed legislation in the country that would actually weaken protections for copyright owners. Christin Baker, a spokeswoman for the U.S. Trade Representative's office, said, "We made it very clear to Russia that improvements...are necessary for them to enter the WTO."

Category 16.4 *Military & government perspectives on INFOWAR*

2006-05-03 **information warfare cyberwar insidious attacks data corruption mole insider employee damage scenarios**

TechTarget http://tinyurl.com/nnf72

DIGITAL DOOMSDAY CAN BE AVOIDED WITH PREPARATION

Bill Brenner began his report in TechTarget's SearchSecurity with the following paragraphs which reflect a scenario long described by Winn Schwartau since the early 1990s:

"A common nightmare scenario in the business world is that a hacker will crack a company's digital defenses, steal sensitive data or disable the network. Scott Borg, director and chief economist at the U.S. Cyber Consequences Unit (US-CCU), an independent organization that churns out information security data on behalf of the government, says enterprises face a darker possibility.

Online outlaws could quietly penetrate the network and, over six to eight months, alter critical data so that it's no longer accurate. For instance, an attacker could access a health insurance company's patient records and modify information on a person's prescriptions or surgical history. Or an attacker could access an automotive company's database and tamper with specifications on various car parts."

Category 16.4 *Military & government perspectives on INFOWAR*

2006-05-30 **information warfare cyberconflict computer network attack PRC China**

RISKS; DoD 24 30
http://www.defenselink.mil/pubs/pdfs/China%20Report%202006.pdf

CHINA CONTINUES PUSH FOR CYBERWAR CAPABILITIES

The annual "Military Power of the People's Republic of China" for 2006 was presented to Congress by the US DoD in May. Two sections in particular speak to concerns about information warfare capabilities (pp. 35-36):

Exploiting Information Warfare The PLA considers active offense to be the most important requirement for information warfare to destroy or disrupt an adversary's capability to receive and process data. Launched mainly by remote combat and covert methods, the PLA could employ information warfare preemptively to gain the initiative in a crisis.

Specifi ed information warfare objectives include the targeting and destruction of an enemy's command system, shortening the duration of war, minimizing casualties on both sides, enhancing operational effi ciency, reducing effects on domestic populations and gaining support from the international community.

The PLA's information warfare practices also refl ect investment in electronic countermeasures and defenses against electronic attack (e.g., electronic and infrared decoys, angle refl ectors, and false target generators.

Computer Network Operations. China's computer network operations (CNO) include computer network attack, computer network defense, and computer network exploitation. The PLA sees CNO as critical to seize the initiative and achieve " electromagnetic dominance" early in a confl ict, and as a force multiplier. Although there is no evidence of a formal Chinese CNO doctrine, PLA theorists have coined the term "Integrated Network Electronic Warfare" to outline the integrated use of electronic warfare, CNO, and limited kinetic strikes against key C4 nodes to disrupt the enemy's battlefi eld network information systems. The PLA has established information warfare units to develop viruses to attack enemy computer systems and networks, and tactics and measures to protect friendly computer systems and networks. The PLA has increased the role of CNO in its military exercises. For example, exercises in 2005 began to incorporate offensive operations, primarily in fi rst strikes against enemy networks.

Formation of Information Warfare Reserve and Militia Units

The Chinese press has discussed the formation of information warfare units in the militia and reserve since at least the year 2000. Personnel for such units would have expertise in computer technology and would be drawn from academies, institutes, and information technology industries. In 2003, an article in a PLA professional journal stated "coastal militia should fully exploit its local information technology advantage and actively perform the information support mission of seizing information superiority." Militia/reserve personnel would make civilian computer expertise and equipment available to support PLA military training and operations, including "sea crossing," or amphibious assault operations. During a military contingency, information warfare units could support active PLA forces by conducting "hacker attacks" and network intrusions, or other forms of "cyber" warfare, on an adversary's military and commercial computer systems, while helping to defend Chinese networks.

The PLA is experimenting with strategy, doctrine, and tactics for information warfare, as well as integrating militia and reserve units into regular military operations. These units reportedly participate with regular forces in training and exercises.

16.5 Hacktivism

Category 16.5 *Hacktivism*

2000-01-19 **criminal hackers hacktivists political Web vandalism attacks ideology politics denial of service**

AP, Newsbytes

According to the Seattle Host Organization that organized the World Trade Organization meetings in Seattle (1999-11-30/12-03), hackers probed their Web site 700 times and tried to penetrate defenses 54 times. Attackers briefly forged the WTO's own Web site to close at one point. On the last day of the meetings, the Web site was subjected to an unsuccessful denial-of-service attack by a group calling itself the "Electrohippies."

Category 16.5 *Hacktivism*

2000-01-31 **political hactivism Web vandalism damage defacement propaganda**

NewsScan, New York Times
http://www.nytimes.com/library/tech/00/01/biztech/articles/31japan.html

In the last days of January 2000, political activists (hacktivists) defaced and damaged Japanese government and business Web sites in protest for the failure of Japan to admit responsibility for the Rape of Nanking (also called the Nanjing Massacre) of 1937. Some sites (e.g., that of the National Personnel Authority) suffered major data destruction ; others (e.g.,Posts and Telecommunications Ministry, Government Data Research Center) saw propaganda messages added to their content. The Bank of Japan reported that its Web site was attacked 1,600 times in a single day. The attacks stimulated concern that Japanese enterprises as a whole were failing to implement effective network and Web security.

Category 16.5 *Hacktivism*

2000-02-17 **information warfare INFOWAR Web attacks vandalism**

AP

Throughout Latin America, cybervandals went on a rampage in the weeks following the high-profile distributed denial-of-service attacks that hit prominent Web sites in the US e-commerce community. Many of the criminal hackers posted propaganda about the Elian Gonzalez case. Security experts commented that the INFOSEC situation in South and Central America is even worse than in the US and Europe, with few sites adequately protected against intrusion and limited knowledge of computer security among law enforcement authorities there.

Category 16.5 *Hacktivism*

2000-02-17 **INFOWAR information warfare hactivism politics international conflict Balkans**

AP

In the Balkans, the ancient hostilities among different communities continued to have cyberspace repercussions. Armenian and Azerbaijani criminal hackers vandalized Web sites run by various organizations in each others' countries. Accusations flew through the news media about misinformation campaigns and one group, the Armenian hacker collective calling itself Liazor, actually changed the text in newspaper articles. "It wasn't a punitive action, we simply wanted to oppose spreading computer vandalism," said a Liazor spokesman, Gevork. [Hmm, opposing vandalism by vandalism. . . . Is that like having intercourse for virginity? Killing for peace?]

Category 16.5 *Hacktivism*

2000-02-18 **international conflict information warfare INFOWAR China Japan propaganda law enforcement censorship**

AP

According to the Associated Press, the Chinese government shut down an anti-Japanese Web site whose sponsors, allegedly the "China Extreme Right Wing Anti-Japanese Alliance", were urging cyberwar against Japan in the wake of revisionist right-wing claims that the Nanjing Massacre of 1937 never happened. The criminal hackers had put up lists of their victims; among the sites allegedly penetrated were Web sites of the Edogawa Women's University, the Management and Coordination Agency, Japan's Science and Technology Agency, the Mainichi Shimbun newspaper, and many other commercial sites.

Category 16.5 *Hacktivism*

2000-02-19 **criminal hackers vandalism Web idiots cretins fools stupid jerks**

EFE (Spanish News Agency)

Criminal hackers bewildered Mexican government officials in the state of Chiapas by vandalizing their Web site in mid-February with pro-Zapatista slogans and also leaving FREE KEVIN graffiti behind. "Kevin? Kevin who?" was the essence of the officials' reactions. Ironically, Kevin Mitnick was released from prison on 2000-01-21.

Category 16.5 *Hacktivism*

2001-05-10 **information warfare hactivism vandalism international Web defacement**

NewsScan

CHINESE HACKERS DECLARE A TRUCE
Boasting that its members have defaced a thousand U.S. Web sites since Chinese-American tensions mounted after the collision in April of a U.S. surveillance airplane and a Chinese jet fighter, the Honker Union of China at Chinabyte has declared the cyberwar over and said that "any attacks from this point on have no connection to the Honker Union." (Reuters/New York Times 10 May 2001)
http://www.nytimes.com/2001/05/10/technology/10HACK.html

Category 16.5 *Hacktivism*

2001-07-17 **hactivist hacktivist Web vandalism information warfare**

NewsScan

HACKER GROUP DECLARES "ARMS RACE" AGAINST WEB CENSORSHIP
A hacker group called Hactivismo has developed anti-censorship software called "Peekabooty" to circumvent attempts to deny citizens of any country access to political information, pornography, or other restricted material. The group cited censorship activities conducted by the United Arab Emirates, Saudia Arabia, Myanmar, China, and North Korea. Oxblood Ruffin, a leader of the group, said: "We believe that access to information is a basic human right guaranteed by law. It is going to be an arms race." Hactivismo will use a distributed privacy network to go around sites that use software filters to block access." (Reuters/San Jose Mercury News 17 Jul 2001)
http://www.siliconvalley.com/docs/news/svfront/047040.htm

Category 16.5 *Hacktivism*

2001-09-19 **hacktivism retaliation Web vandalism law enforcement police**

NewsScan

FBI WARNS AGAINST VIGILANTE HACKTIVISIM [19 Sep 2001]
A 60-member network of computer hackers calling themselves the Dispatchers has vandalized 200-300 Web sites in the Middle East, including the official Web site of the Presidential Palace of Afghanistan and a site of its ruling Taliban party. The FBI wants the vandalism stopped and says: Those individual who believe they are doing a service to this nation by engaging in acts of vigilantism should know that they are actually doing a disservice to this country." (USA Today 19 Sep 2001)
http://www.usatoday.com/life/cyber/tech/2001/09/19/hack-attack-launched.htm

---

Category 16.5 *Hacktivism*

2001-10-01 **hacktivists penetration terrorists police FBI**

http://www.vnunet.com/News/1125741

According to an article by James Middleton on vnunet.com, a well-known group of criminal hackers calling themselves "Young Intelligent Hackers Against Terror" (Yihat) located some confidential banking information about terrorist Osama bin Laden and the Al Qaeda organization by penetrating systems at the AlShamal Islamic Bank. The espionage was supposedly a response to convicted hacker Kim Schmitz, who announced a $10M reward and received insider information from "an unidentified member of the Islamic banking community" about which bank was handling Al Qaeda accounts.

Category 16.5 *Hacktivism*

2002-05-20 **hacktivisists investigation Web vandalism defacement arrests confidentiality penetration probation juvenile**

Security Wire Digest, SecurityFocus; http://online.securityfocus.com/news/414 4 39

Hacktivists calling themselves the Deceptive Duo were arrested in May after an FBI investigation. Using handles "Pimpshiz" and "The Rev," the pair vandalized dozens of Web sites supposedly to stress the importance of improving security in the face of international threats to the USA's infrastructure. In one case, the pair posted a page apparently stolen from a bank system that showed customer names and account numbers.

Robert Lyttle, 18, was ordered into house arrest for having violated the terms of his probation for a previous hacking conviction only four months prior to the latest alleged crimes. In the previous conviction, Lyttle had defaced more than 200 Web sites, replacing them with pro-Napster e-graffiti and had been ordered to serve 90 hours of community service and was barred from hacking and from using pseudonyms online. As an 18-year-old, Lyttle faced federal charges instead of juvenile court this time. Little information was made available by the FBI about the second hacker suspected in the case.

Category 16.5 *Hacktivism*

2002-10-03 **Web hijacking cult politics repression**

NewsScan

NEWSPAPER SITE REROUTED TO FALUN GONG
Surfers who tried to visit the site of the Hong Kong newspaper Mingpao were diverted to another site filled with messages about Falun Gong, the organization of a meditation group that is outlawed in mainland China and described by Chinese officials as an "evil cult." A Falun Gong spokesman in Hong Kong denied the organization was responsible for the vandalism: "Just because the users are redirected to the Falun Gong Web site doesn't mean Falun Gong did it. We suspect others are trying to frame Falun Gong with these kinds of tricks. In a free and open society, you don't have to resort to these tactics." (AP/New York Times 3 Oct 2002)

Category 16.5 *Hacktivism*

2002-12-18 **hacktivism harassment invasion privacy denial-of-service attacks spam e-mail**

NewsScan

WEB ACTIVISTS GO AFTER RALSKY AND POINDEXTER
Web activists have uncovered the home address and phone numbers for government surveillance head John Poindexter and bulk spammer Alan Ralsky, and have posted the information on more than 100 Web sites. The action has led to Ralsky being deluged with junk mail and Poindexter undergoing the scrutiny that every American soon will experience. An article in the Detroit Free Press quoted Ralsky as complaining, "They're harassing me," after anti-spammers signed him up with as many direct mail agencies as possible. In Poindexter's case, his home address, complete with satellite photos, has been published online as well as his phone number and those of his neighbors. That's actually just a small portion of the personal information the U.S. government plans to collect under Poindexter's Total Information Awareness program, which will compile credit card, medical, travel, school and other records in an effort to spot terrorists. (BBC News 16 Dec 2002)
http://news.bbc.co.uk/2/hi/technology/2580089.stm

Category 16.5 *Hacktivism*

2003-03-18 **hacktivism Iraq war Web defacement propaganda**

NIPC/DHS

March 17, Computer Weekly — U.S. Diplomatic site hacked by anti-war protestors.

The website of the American Academy of Diplomacy (www.academyofdiplomacy.org) was hacked into Sunday while U.S., U.K. and Spanish leaders met at the Azores summit to discuss the crisis over Iraq. A message of "No War" was plastered over the site by hacking group "Rooting Sabotage Forced". Other messages on the site included protests over the Israeli-Palestinian situation. With a war on Iraq thought to be as little as days away digital attacks on American and British business and government targets remain at an all-time high, according to the British-based digital risk specialist mi2G. For 12 months, the number of independently verifiable digital attacks on the US stand at 48,155 and for the UK they stand at 7,607 according to the mi2g SIPS database. In comparison, the number of attacks recorded over the same period for France was 3,082.

Category 16.5 *Hacktivism*

2003-03-21 **Iraq war hacktivism Web defacement warn cyber attack**

NIPC/DHS

March 20, Washington Post — Antiwar digital graffiti prompts security experts to warn of further cyberattacks.

A hacker group marred hundreds of Web sites with digital graffiti Wednesday night in an apparent response to the onset of the U.S.-led war against Iraq, prompting security experts to warn of further cyberattacks in the days to come. Unix Security Guards, a pro-Islamic hacking group which includes hackers from Egypt, Morocco, Kuwait and Indonesia, defaced nearly 400 Web sites Wednesday evening with antiwar slogans written in Arabic and English, according to iDefense, a U.S. Internet security firm. Text posted on sites by the hacker group said the defacements were the beginning of "the new era of cyber war we promised! More is coming, just like the US do [sic] what it wants to the world, we will do what we want to the Internet. Stop the US terroristes [sic] and we will stop! Viva Iraq!" The attacks were typical of the sort of "hacktivism" that has accompanied international conflicts in the past, said Jim Melnick, director of threat intelligence for iDefense.

Category 16.5 *Hacktivism*

2003-03-25 **Denial of Service DoS hacking hackivism Al-Jazeera Iraq**

NewsScan

AL-JAZEERA SITE ATTACKED

The Web site of Al-Jazeera, the Arab satellite TV network, was subjected to denial-of-service attacks yesterday, making it intermittently unavailable. The servers that host the Al-Jazeera site are in both France and the U.S., but only the U.S. servers were affected. The site's English-language page, which was launched one day before the attacks began, had been showing images of U.S. soldiers killed in Iraq. (AP/Washington Post 25 Mar 2003)

Category 16.5 *Hacktivism*

2003-03-26 **anti-war Web defacement vandalism hacker hacking Iraq war**

NIPC/DHS

March 25, Associated Press — Anti-war hackers alter South Carolina Secretary of State's Web site.

Hackers apparently took over the South Carolina Secretary of State's Web site this weekend, posting anti-war slogans and obscenities. Officials were notified of the altered page Sunday afternoon and took it down. The regular site was restored later the same day. The pirated site was up for about 12 hours, officials said. "This country has a history of civil disobedience, but this has crossed the line and is a criminal matter," Secretary of State Mark Hammond said Monday. The State Law Enforcement Division is investigating, spokesman Kathryn Richardson said.

Category 16.5 *Hacktivism*

2003-04-02 **Utah Internet Service Provider hacking attack Al-Jazeera anti-war Iraq war Web vandalism**

NIPC/DHS

March 28, Associated Press — Utah ISP is victim of retaliation following hackers' attack on al-Jazeera.

The Salt Lake City-based Internet service provider Networld Connections became the unwitting tool of hackers attacking Arab television network al-Jazeera, and then was itself struck by a retaliatory attack, possibly from anti-war hackers. The original hackers, impersonating an al-Jazeera employee, tricked the Web addressing company Network Solutions into making technical changes that effectively turned over temporary control of the network's Arabic and English Web sites. "We have no idea who the hacker is, but now there is a 'denial-of-service' attack going on against us because of what happened," Ken Bowman, Networld's president and chief executive, said late Thursday. Bowman said the attacks were from all over the world, but seemed concentrated most from nations such as Russia, China and France that have among the most vocal opponents of the U.S.-British coalition's attack.

Category 16.5 Hacktivism

2003-04-03 **Al-Qaeda terrorism information warfare Web vandalism hacktivism**

NIPC/DHS

April 01, The Oregonian — Al Qaeda supporters hack into student's Web site.

The Web site of a Portland State University graduate student was targeted in a wave of Internet hackings supporting al Qaeda. Files planted in Conrado Salas Cano's personal Web site housed threats against the United States, tributes to the September 11 attacks and purported messages from Osama bin Laden. The FBI reportedly launched an investigation, and some cyberterrorism followers said it resembled attacks by al Neda, the online propaganda unit of al Qaeda. Josh Devon, an analyst at the Search for International Terrorist Entities Institute, said some of the pages contain pictures of guns and bomb-making manuals in Arabic. Specific plans of future attacks aren't on the site, although Devon said it's possible they use code words to communicate attacks. Since losing their domain name last summer, Devon said al Neda has been hacking into various sites around the globe to spread its message. Once the sites are discovered and shut down, a new al Neda site pops up within 48 hours. News of the Web sites, he said, spreads by word of mouth and in Arabic newspapers.

Category 16.5 Hacktivism

2003-04-18 **Iraq war protest Internet hacktivism Web defacement vandalism security attack**

NIPC/DHS

April 16, Mena Report — High profile digital targets hit by hackers protesting Iraq war.

Over 3,000 successful digital attacks took place last weekend primarily against U.S. and U.K. online targets with hackers protesting a further escalation in the war with Iraq. The main concern being expressed by hackers is over the conflict spreading to Syria or Iran. High profile targets hit include Coca-Cola's web site in Singapore, which was attacked on Saturday, April 12. It was unreachable throughout Sunday and is now back up again. There are other examples of NASDAQ and NYSE listed companies, such as one with over 1,650 employees and a market capitalization in excess of $275 million that were hit over the weekend. Also, Fuji Film online sites in the U.S. and Switzerland were targeted by Hackweiser—a pro-war U.S. patriotic group — and in the U.K., the London Fire Brigade and Scottish Police online sites were successfully targeted by Unix Security Guards (an anti-U.S./U.K./Israel group).

Category 16.5 Hacktivism

2004-05-19 **hacking government hacktivism patriot hacker Internet Web security**

DHS IAIP Daily; http://www.securityfocus.com/news/8717

May 19, Security Focus — 'Patriot' hacker pleads guilty.

A Florida man pleaded guilty in federal court in Washington DC, on Wednesday, May 19 to charges stemming from his role as one-half of the high-profile hacking team "The Deceptive Duo," responsible for obtaining sensitive information from government systems, and defacing dozens of government and private Websites with patriotic messages exhorting the U.S. to shore up cyber defenses. In a plea agreement with prosecutors, Benjamin Stark, 22, admitted to cracking eleven computer networks belonging to nine U.S. government departments and private commercial entities. The Deceptive Duo drew public attention in April 2002. As part of the plea, Stark admitted to working with an unnamed partner to crack systems at the Federal Aviation Administration (FAA), the Federal Highway Administration, the Defense Logistics Agency; the Department of Defense's Health Affairs office, the Department of Energy's Sandia National Lab, the Naval Air Systems Command, the Air Force Publishing Office, Dynamic Systems Inc. and Midwest Express.

Category 16.5 Hacktivism

2004-05-20 **Athens 2004 Olympics cyberattacks defense**

DHS IAIP Daily; http://software.silicon.com/security/0,39024655,39120825,00.
htm

May 20, — Athens Olympics braced for wave of cyberattacks.

The Athens Olympics organizers are bracing themselves for a wave of cyberattacks once the games are under way, but insist that a physical breach of security still represents the biggest threat. Although questions remain about whether some of the venues will be ready for August 13, the IT planning is on course with a second technical rehearsal using some of the venues and simulating the four busiest days of the games taking place on June 14. By the start of the games some 200,000 people-hours of testing will have been completed and 10,000 defects are expected to be found and corrected. The infrastructure itself is fairly tried and tested with a policy of keeping complexity and risk down by only introducing new technology where it is essential. As such the platforms of choice are Unix and Windows, with Linux not getting a look-in.

Category 16.5 *Hacktivism*

2004-06-23 **Web vandalism Taiwan political site Chinese**

NewsScan

HACKERS ATTACK TAIWAN RULING PARTY WEBSITE

Suspected Chinese hackers have attacked the website of Taiwan President Chen Shui-bian's pro-independence Democratic Progressive Party (DPP). The party's homepage was replaced with pro-China pictures and digitally altered images of Chen and his Vice President Annette Lu, a DPP official said. One photo shows a Chinese People's Liberation Army soldier aiming his rifle at a
target while another shows two men raising the Chinese national flag. Another picture shows Chen's head transposed onto the body of a man clad in traditional Japanese costume of kimono while Lu was transplanted onto an unclothed woman. (The Age 23 Jun 2004)

Category 16.5 *Hacktivism*

2004-07-14 **Web hacktivism vandalism South Korean government Website China origin**

NewsScan

SOUTH KOREAN GOVERNMENT SITES ATTACKED

South Korea's spy agency says important government data may have been stolen during a spate
of recent cyber-attacks launched from China. The attacks were considered a serious threat to South
Korea's national security and the Chinese government has been urged to carry out its own investigation. Hackers using information-stealing viruses had broken into 211 computers at ten government agencies, including the Korea Institute for Defense Analyses and the Agency for Defense Development involved in weapons development. In addition, 67 computers at private companies, universities and media firms were hacked. (The Age 14 Jul 2004) Rec'd from John Lamp

---

Category 16.5 *Hacktivism*

2004-07-20 **Web hacktivism vandalism Chinese hackers Taiwan military Website**

NewsScan

VANDALS ATTACK TAIWAN WEBSITE

Suspected Chinese hackers have launched an offensive against the website of Taiwan's Military News Agency ahead of practice freeway landings by fighter jets on the island. The hackers replaced the agency's homepage with a slogan that said 'Reunification with Taiwan in 2021' in an attack identical to one that occurred a month ago when suspected Chinese hackers attacked the site of Taiwan President Chen Shui-bian's pro-independence Democratic Progressive Party. Hong Kong's pro-Beijing Wen Wei Po daily last week quoted Chinese military sources as warning that Taiwan must re-enter the Chinese fold or face military action within the next 20 years. (The Age 20 Jul 2004) Rec'd from John Lamp

---

Category 16.5 *Hacktivism*

2004-08-04 **Japanese government Websites attack hacktivism**

DHS IAIP Daily; http://securityfocus.com/news/9274

August 04, Associated Press — Japanese government's computers hit by cyber attacks.

A wave of cyber attacks disrupted Japanese government computer networks earlier this week, but no damage was reported, an official said Thursday, August 5. The attacks, late Sunday and early Tuesday, targeted eight ministries and agencies and caused computers to freeze up under a deluge of data, Chief Cabinet Secretary Hiroyuki Hosoda told a news conference. Hosoda said the barrage also made it impossible for anybody to access Websites for the eight government bodies--the Cabinet Office, Foreign Ministry, Finance Ministry, Justice Ministry, National Police Agency, Defense Agency, Coast Guard and Fair Trade Commission. "We don't know where the attack came from, or who did it," he said.

Category 16.5 Hacktivism

2004-08-25 **political Websites electronic e-jihad Israel**

DHS IAIP Daily;
http://www.eweek.com/article2/0,1759,1639243,00.asp?kc=EWRSS03119TX1K0000594

August 25, eWeek — Some concerns over electronic jihad.

Russian security researcher Yevgeny Kaspersky of Kaspersky Labs International said Wednesday, August 25, that a number of Arabic and Hebrew language Websites contained an announcement of an 'electronic jihad' against Israel to start on Thursday. However, Kaspersky stressed that such information was not necessarily trustworthy. "The e-jihad has been discussed for years, but an undisputed attack has yet to surface," said Ken Durham, director of malicious code at iDefense Inc. But Durham said security pros are increasingly worrying about when political activists might join with like-minded security and Internet programmers. While Kaspersky's warning appears to suggest wide-scale DDoS (distributed denial of service) attacks, experts suggested that important Internet services, as well as its root servers, are also at risk. For example, a DDoS attack in June against Akamai Technologies Inc. slowed traffic across the Internet for several hours. And in July, DoubleClick Inc.'s DNS (domain name system) was attacked and unable to serve ads for a similar time frame.

Category 16.5 Hacktivism

2005-04-14 **Vietnam government Website attack defacement Turkish hacker hacktivism**

DHS IAIP Daily; http://www.thanhniennews.com/society/?catid=3&newsid=6150

VIETNAMESE GOVERNMENT WEBSITES ATTACKED

In recent days, several Vietnamese Websites including some government sites have been defaced and a Turkish hacker is claiming responsibility for the attacks. The hacker calls himself iSKORPiTX. After the attacks, he posted a list of hacked Websites on the Internet at http://www.zone-h.org. He said that five Vietnamese Websites were hacked into in just one day on April 11, including some government Websites with the domain names gov.vn and edu.vn. Hacker iSKORPiTX has claimed to deface 316 Websites. Currently, the hacker ranks fourth on the top 10 list of world Website hackers. He said that he randomly liked to hack into Websites, but had no dark intentions. Related article on hacked Anchorage airport Website: http://www.usatoday.com/travel/news/2005-04-13-ala-airport-h acking_x.htm

---

Category 16.5 Hacktivism

2005-04-14 **Japan cyber attack Websites hacktivism China bilateral disagreement**

DHS IAIP Daily;
http://story.news.yahoo.com/news?tmpl=story&cid=1509&ncid=738&e=11&u=/afp/20050414/tc_afp/japanchinainternet

JAPAN SUSPECTS CYBER ATTACK ON OFFICIAL WEBSITES

Japan's police and defense agencies said they had come under cyber attack, amid reports a Chinese website was calling for the jamming of Japanese servers amid a heated bilateral disagreement. "Access to the homepage of the National Police Agency was hampered from around 9:00 pm (1200 GMT Wednesday, April 13) to 3:00 am (1700 GMT)," the national police said in a statement. "We are investigating the cause but it is highly possible that it was a cyber attack in which a large volume of information was sent to the address of the homepage," it said. Japanese media reports said a Chinese website had urged Internet users to flood Japanese servers with irrelevant data. A police spokesperson said the agency was "aware of the call" from China but had not identified what hampered the access. The Defense Agency also said its Website had been experiencing access problems from late Wednesday, April 13. Tensions have been rising between Japan and China. Japan announced Wednesday that its companies would have the right to drill for oil and gas in an area of the East China Sea bitterly disputed between the Asian economic powers.

Category 16.5 *Hacktivism*

2005-04-25 **Web server attacks growing quickly survey hacktivism Iraq war teenager involvement**

DHS IAIP Daily; http://news.bbc.co.uk/1/hi/technology/4480689.stm

SURVEY: WEB SERVER ATTACKS 'GROWING FAST'

A survey by Zone-H revealed that web server attacks and Website defacements grew by 36% during 2004 when almost 400,000 incidents were recorded. The attacks include 49 separate sorties against U.S. military servers and huge numbers of Website defacements. The figures were collated by Zone-H , a web-based organization that uses a world-wide network of volunteers to spot and investigate web server attacks and site defacements. "Defacement is just one option for an attacker," said Roberto Preatoni, Zone-H coordinator. "In most circumstances the techniques used by defacers are the same techniques used by serious criminals to cause more serious damage." The report found that more than half of all attacks and defacements, 55%, succeeded by exploiting a known bug or vulnerability or an administration mistake. The figures show that the many incidents occur on the anniversaries (mid-March) of the start of the most recent war in Iraq when both pro-Muslim and pro-American groups defaced sites. The survey also found that the long holidays around Christmas provoke a spike in attacks and incidents. The frequency of attacks also dips around the time that schools re-open suggesting that many teenagers are behind the defacements. Survey: http://www.zone-h.com/news/read/id=4457/

Category 16.5 *Hacktivism*

2006-02-07 **Denmark Website defacements hacktivism F-Secure suicide bombing warnings**

DHS IAIP Daily; http://www.securitypipeline.com/news/179101482 23

ISLAMIC MESSAGES DEFACE HUNDREDS OF DANISH SITES.

Muslim protests over editorial cartoons originally published by a Danish newspaper have spilled onto the Internet and resulted in defacements of nearly 600 Danish Websites with anti-Dane, pro-Muslim messages in the past week, Helsinki-based F-Secure said Tuesday, February 7. This has been the latest fallout in the uproar over cartoons that include one depicting Mohammed with a bomb for a turban. The defacements included warnings of suicide bombings, Arabic-language messages sprawled across home pages, and threats such as "die plez."

Category 16.5 *Hacktivism*

2006-03-31 **Chinese government Websites attack vandalism cracking China defacement information warfare hacktivism**

DHS IAIP Daily; http://www.shanghaidaily.com/press/2006/03/31/attacks−on− 23
gov 11 −websites−skyrocket/

ATTACKS ON CHINESE GOVERNMENT WEBSITES SKYROCKET.

Hackers cracked various levels of the Chinese government official Websites and changed information on the Web pages 2,027 times last year, doubling that of 2004. Additionally, more than 13,000 Chinese Websites were altered last year, one-sixth of which were government Websites.

16.6 Disinformation, PSYOPS

Category 16.6 *Disinformation, PSYOPS*

1997-01-10 **Sabotage infowar information warfare disinformation PSYOPS**

RISKS 18 75

A letter drive attacking a mail-order pharmacy in 6,000 mailed warnings was linked to Shoppers Drug-Mart employee. The "Society of Concerned Pharmacists," ostensibly an organization devoted to protecting consumers against the dangers of the Meditrust service, seems to have been the product of an secretary from the competing firm.

Category 16.6 *Disinformation, PSYOPS*

1997-02-11 **AI fraud infowar**

EDUPAGE

In a scary development, the New York Times reported in February 1997 that there are scientists developing software "capable of lying, cheating and stealing." The report stated, "Commercial and entertainment applications, rather than military ones, increasingly are driving artificial intelligence, and some AI software developers are even working on the design of a networked world in which software agents might try to take unfair of each other in commercial transactions."

Category 16.6 *Disinformation, PSYOPS*

2003-01-14 **information warfare Iraq war e-mail campaign convince leaders defect United Nations UN**

NIPC/DHS

January 12, CNN — U.S. E-mail attack targets key Iraqis.

U.S. military and other U.S. government agencies have begun a surreptitious e-mail campaign inside Iraq in an effort to get some Iraqis to defy President Saddam Hussein. Thousands of e-mail messages have been sent out since Thursday. The disguised e-mails, being sent to key Iraqi leaders, include instructions to the e-mail recipients to contact the United Nations in Iraq if they want to defect. If they do not, the messages warn, the United States will go to war against them. Senior military sources told CNN this was the first time the military had engaged in this type of "information warfare campaign." The U.S. military and intelligence officials were apparently hoping that the Iraqis do not realize where the e-mails are coming from. One official tells CNN the Pentagon wanted "to preserve this capability as long as possible," but once the e-mail campaign was discovered it would be acknowledged publicly. The official also says the United States acknowledges that Iraq may have already shut off some Internet gateways to prevent the e-mails from getting through. He said these same types of messages will now be sent by radio broadcast in the days ahead from U.S. airborne and ground platforms.

Category 16.6 *Disinformation, PSYOPS*

2003-03-26 **disinformation malicious imposters news corporate Web sites Iraq war**

NIPC/DHS

March 25, The Register — Malicious impostors sow seeds of disinformation.

Security testing outfit NTA Monitor has warned of the increased likelihood of attacks against news sites and corporate Web sites during the current war in Iraq. News sites are especially at risk, because attackers could use weaknesses in sites or domain registration tricks to 'rewrite' breaking news to try to create confusion and panic, according to NTA. The most obvious risk is denial of service attacks, in which sites are deliberately brought down by extreme traffic volumes. However the subtler attacks are of much greater concern. By registering similar domain names or 'typo squatting' - booking domains with common typo errors (e.g., wwwcompany.com) - traffic intended for official news sites could be re-directed. Attackers can impersonate Internet news sites and make major changes to the news, with potentially disastrous impact.

Category 16.6 *Disinformation, PSYOPS*

2003-04-03 **biological virus hoax Website misinformation disintermedation Hong Kong**

NIPC/DHS

April 01, Reuters — Website hoax fans virus panic.

A teenager's website hoax about a killer virus that is sweeping Hong Kong sparked panicked food buying and hit financial markets on Tuesday, forcing the government to deny it would isolate the entire territory. "We have no plan to declare Hong Kong an infected area," Director of Health Margaret Chan told reporters. "We have adequate supplies to provide (for) the needs of Hong Kong citizens, and there is no need for any panic run on food." In Hong Kong, 685 people are infected by severe acute respiratory syndrome, also known as SARS, and 16 have died from the virus. The fake website scare fueled dismay in the territory adjoining China's Guangdong province, where the virus is believed to have originated four months ago. The hoaxer copied the format of the public Internet portal of the Mingpao, one of Hong Kong's leading newspapers, and posted a message saying the government would declare the city of seven million "an infected place."

Category 16.6 *Disinformation, PSYOPS*

2003-04-03 **Iraq Information Ministry war disinformation propaganda US attack**

NIPC/DHS

March 31, salon.com — Iraq goes offline.

U.S. Tomahawk cruise missiles aimed at destroying Saddam Hussein's propaganda machine reportedly destroyed several satellite dishes and an Internet server housed at Iraq's Ministry of Information building Saturday. Local phone service in the city was also reportedly disrupted by separate missile strikes on two telecommunications switching centers. Yet Babil Online, the home page of an Iraqi newspaper run by Saddam Hussein's son Uday, was still reachable following the bombing. Babil Online may have escaped the attacks because of its physical location — the site appears to be hosted on a server not in Baghdad but in Beirut, Lebanon. Some observers have speculated that the United States left Iraq's Internet infrastructure untouched for the first week of the war in order to maintain communications with potential defectors in the high ranks of Iraq's government and military personnel. But Peter W. Singer, a fellow at the Brookings Institute, said he doubted that preserving Iraq's Internet capabilities was high on the priority lists of U.S. military planners. "Internet access is still limited mostly to elites in the country. The U.S. is mostly concerned about protecting things like water and electricity and bridges," said Singer. He said the mission of Iraq's Information Ministry has been not only to fire up nationalism but also to manipulate world opinion and to raise international protests against the war.

Category 16.6 *Disinformation, PSYOPS*

2003-04-04 **biological virus hoax SARS Website misinformation disintermedation Hong Kong SMS text message**

NIPC/DHS

April 03, Associated Press — Six million mass text messages avert SARS panic.

When a false Internet story about Asia's mystery illness sent fears through Hong Hong, authorities used a fast and simple way to shoot down the rumor: they sent a blanket text message to about 6 million mobile phones that denied the territory had been declared an "infected city." Severe Acute Respiratory Syndrome, or SARS, has killed at least 78 people and sickened more than 2,200 worldwide. The government used the text message on Tuesday after the "infected city" hoax report appeared online, prompting panic among some residents who thought the territory would be shut down. The government's text response said: "Director of Health announced at 3pm today there is no plan to declare Hong Kong as an infected area." The hoax story was allegedly posted by a 14-year-old boy who was quoted as saying he did it for fun, and didn't think anybody would believe the story. A telecommunications professor said mass text messaging - or SMS messaging - was justified in emergencies, but could potentially be abused. "It's very important for phone operators to identify where the information comes from," said KL Ho, who teaches at the Department of Electrical and Electronic Engineering at the University of Hong Kong. "It's also very important to remind users not to believe just one single source," Ho said.

Category 16.6 *Disinformation, PSYOPS*

2003-04-16 **CNN information filtering operation propaganda Iraq**

NewsScan

CNN DEFENDS ITSELF AGAINST NEWS-FILTERING CHARGES
In a memo to his staff, CNN top news executive Eason Jordan has denied that his motive for failing over a 12-year period to report horrors of the Saddam Hussein regime was to keep the CNN Baghdad bureau open. "A number of people have told me CNN should have closed its Baghdad bureau, helped everyone who told me the horror stories flee Iraq, with me thereafter telling those stories publicly long before now. While that is a noble thought, doing so was not a viable option." He says that such victims would not have left their country simply to be able to share their stories with the world. "So we reported on Iraq's human rights record from outside Iraq and featured many interviews with Iraqi defectors who described the regime's brutality in graphic detail. When an Iraqi official, Abbas al-Janabi, defected after his teeth were yanked out with pliers by Uday Hussein's henchmen, I worked to ensure the defector gave his first TV interview to CNN. He did." (Atlanta Journal-Constitution 16 Apr 2003)

Category 16.6 *Disinformation, PSYOPS*

2003-07-29 **Disinformation HIV Internet**

NewsScan

IS HIV AN INTERNET PROBLEM?
A presentation made at the 2003 National HIV Prevention Conference suggests that online chat rooms and Web sites are partly responsible for the fact that a growing number of U.S. gay and bisexual men are engaging in risky activities with partners they met on the Internet. New HIV diagnoses among those groups have jumped more than 17% since 1999, and 850,000 to 950,000 Americans have the AIDS virus. Dr. Ron Valdiserri of the Centers for Disease Control in Atlanta says: "It's clear we need to reach gay and bisexual men with appropriate messages, not only in traditional high-risk settings but also online. (Washington Post 29 Jul 2003)

Category 16.6 *Disinformation, PSYOPS*

2003-12-05 **psychological operations disinformation false news propaganda military**

NYT
http://www.nytimes.com/2003/12/05/politics/05STRA.html?th=&pagewanted=p
rint&position=

In December 2003, analysts raised the alarm upon discovering a modest $300K contract from DoD to SAIC for a study of how to "design an 'effective strategic influence' campaign combat global terror….[Eric Schmitt, NY Times] Schmitt continued his report with an explanation that Pentagon spokespersons assured questioners that although establishing a "road map for creating an effective D.O.D. capability to design and conduct effective strategic influence and operational and tactical perception-management campaigns" might be a poor choice of words, it was not a call for a propaganda machine. "We're asking for a menu of thoughts on how to approach this," one official explained. "This is not a secret document on how we're going to change the Arab world's perception of the U.S."

Category 16.6 *Disinformation, PSYOPS*

2003-12-07 **Google bomb linking search engine information warfare psyops**

BBC http://news.bbc.co.uk/2/hi/americas/3298443.stm

Pranksters deliberately agreed to link the words "miserable failure" on their Web pages to the biography of George W. Bush, resulting in "Google Bombing" as his site climbed to the number one position on the search engine's listing for — wait for it — "miserable failure." Responding to the attack, conservatives used the same technique to link the insulting words to sites about Jimmy Carter, Michael Moore and Hillary Rodham Clinton. The phenomenon is yet another wrinkle in the evolution of psychological operations and information warfare, although a minor and amusing one. Google declined to interfere.

Category 16.6 *Disinformation, PSYOPS*

2006-04-02 **authenticity fake forged e-mail political scandal government resignation Japan**

RISKS; AP http://209.157.64.201/focus/f-news/1606953/posts 24 23

FAKE E-MAIL TOPPLES JAPANESE OPPOSITION PARTY

Japan's opposition party suffered a fresh humiliation Friday [March 31, 2006] when its leadership resigned en masse over a fake e-mail scandal, handing Prime Minister Junichiro Koizumi an uncontested grip on power in his last six months in office. … Party leader Seiji Maehara and his lieutenants stepped down after the party's credibility was torpedoed by one of its own lawmakers, who used a fraudulent e-mail in an apparent attempt to discredit Koizumi's ruling Liberal Democratic Party.

[Abstract by Peter G. Neumann]

Category 16.6 *Disinformation, PSYOPS*

2006-05-05 **criminal hackers data integrity electronic advertising boards access control failure design flaw**

RISKS 24 29

SUBWAY SIGNS ACCUSE CANADIAN PRIME MINISTER OF CANNIBALISM

Criminal hackers using a $25 remote control device reprogrammed several electronic message boards in Toronto's GO Transit subway cars to read "Stephen Harper Eats Babies" in endless loops. A colleague of the Prime Minister said, "I worked with Stephen Harper for five years and never once did he, in that time, eat a baby."

[MK adds: Note the qualifier, "in that time."]

Category 16.6 *Disinformation, PSYOPS*

2006-05-05 **Islamic militants US video game recruitment terrorism technology**

DHS IAIP Daily; http://news.zdnet.com/2100−1040_22−6068963.html 23

ISLAMIC MILITANTS RECRUIT USING U.S. VIDEO GAMES.

The creators of combat video games have unwittingly become part of a global propaganda campaign by Islamic militants to exhort Muslim youths to take up arms against the U.S., defense officials said on Thursday, May 4. Tech-savvy militants from al-Qaeda and other groups have modified video war games so that U.S. troops play the role of bad guys in running gunfights against heavily armed Islamic radical heroes, Department of Defense officials and contractors told Congress. The sites use a variety of emotionally charged content, from images of real U.S. soldiers being hit by snipers in Iraq to video-recordings of American televangelists making disparaging remarks about Islam. The underlying propaganda message, officials say, is that the U.S. is waging a crusade against Islam in order to control Middle Eastern oil, and that Muslims should fight to protect Islam from humiliation.

---

17 Penetration, phreaking, cramming, uncapping (entering systems, stealing telephone or other services)

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1997-02-13 **penetration management**

EDUPAGE

Computer Science Corporation warned that many organizations are being attacked by ex-employees or by ex-employees of outsourced computing services. Some experts are urging large organizations to implement single-logon systems with centralized control of every user's passwords. According to EDUPAGE's summary, "One ex-employee of a Big Six accounting firm continued to use the company's e-mail and voice-mail systems a year after he left, and even accessed the company's internal network occasionally, although by that time he was employed by a competitor."

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1997-02-19 **intrusion penetration hackers**

RISKS, Reuters

Teenaged criminal hackers in Croatia may have broken into US military computers, although no classified materials were thought to have been compromised. According to Reuters reporter Laura Lui, "the U.S. Defence [sic] Department had contacted Croatian police through Interpol to demand an investigation while local police searched the youngsters' flats and confiscated their computer equipment. The damage caused by the teenagers' destruction of high-profile protection programmes could reach half a million dollars, the daily said."

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1997-03-01 **penetration hacking**

AP

A 15-year-old Croatian hacker broke into computers at Anderson AFB in Guam in January using hacking tools available free on the Internet. He tried to read through files but was surprised to see them disappearing every time he accessed one. On 97.02.05 he was arrested by Croatian police and his computers were confiscated. Vice Miskovic, whose pseudonym was "Intruder," cannot be charged with computer trespass because there are no such Croatian laws.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1997-03-04 **security management**

EDUPAGE

The Information Warfare Division of the Defense Information Systems Agency of the U.S. Department of Defense tested 15,000 Pentagon systems whose vulnerabilities had been signaled to system managers in a previous audit. About 90% of these systems were still vulnerable to common penetration techniques.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1997-03-06 **medical records penetration privacy law**

AP

The U.S. National Research Council issued a committee report urging hospitals to strengthen their information security measures to reduce the likelihood of unauthorized access to computerized medical records. The committee recommended, among other measures, thorough audit trails; effective passwords; timed-screen savers; data classification and access restrictions; firewalls to prevent access from Internet connections; and encryption of all patient data sent through the Internet.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1997-03-22 **hacker penetration**

Reuters

The Datastream Cowboy was finally convicted and fined the equivalent of $1,915 for cracking the U.S. Air Defense System computers. In 1994, the then sixteen-year-old music student Richard Pryce's intrusions were interpreted to be a major and dangerous attack on the security of Pentagon systems and were described in Senate Armed Services Committee hearings as the "number one threat to U.S. Security." Pryce broke into Griffiss Air Base in New York and a Lockheed computer network in California, among others. He explained his escapades as an attempt to impress his hacker friends: "It was more of a challenge really, going somewhere I wasn't meant to. If you set out to go somewhere and you get there, other hackers would be impressed." Pryce refused lucrative offers for book and film rights to his story and now pursues his double-bass studies, hoping to earn a place in a symphony orchestra.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1997-03-25 **infowar espionage information warfare**

EDUPAGE

Recent admissions about the US-Iraqi war suggested that criminal computer hackers from the Netherlands cracked military computers at 34 sites and stole operational information which they offered to Iraqi intelligence. Ironically, the Iraqis apparently rejected the free information, suspecting it to be false. However, the hackers named in these stories vigorously denied any such story and provided strong reason to believe that this story is an urban legend based on journalistic and sensational distortion of interviews and mistaking conjecture for fact.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1997-03-26 **intrusion joe accounts passwords penetration**

RISKS 18 94

Hungary's main ISP, MATAV, revealed that about 1,200 IDs and passwords were compromised because of its lax security. Seems the company actually published the list of IDs to which it had initially assigned billing numbers — as a warning to change the passwords.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1997-05-09 **phreaking penetration**

RISKS 19 13

The alcohol-abusing glue-sniffing youngster known as the Swedish "Demon Freaker" who placed 60,000 free calls worth $250K and linked Florida switchboards to sex lines last year was fined the equivalent of $350 and sent to a psychiatric institution. He was caught while harassing an emergency-response operator in the US with claims that his penis was glued to the wall; while he was being encouraged to continue with his story, officials traced the call to Sweden. Swedish police identified his home because it was the only one making so many calls to the US. The 19-year-old's mother said that he had a history of alcohol abuse and glue sniffing but that she had no idea of his nocturnal phone calls to the U.S.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1997-06-17 **hack penetration e-mail passwords ISP**

Ottawa Citizen

A16-year-old A+ student from a private school in Brockville, ON cracked into RipNet, a local ISP, and stole 1300 user IDs and passwords, handing them out to four of his friends. The break-in was discovered immediately and the ISP managers contacted police. The authorities decided to let the school deal with the delinquents. The ringleader was expelled from computer classes for a year; all five miscreants were ordered to write essays analyzing the moral dimensions of their actions. The ISP contacted all the victims and arranged for them to change their passwords.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1997-06-26 **hacker phreak penetration PBX voice-mail**

OTC

A 15-year-old phreak calling himself "Mr Nobody" claimed he cracked Netcom On-Line Communications Service Inc. in 1995 and listened to voice-mail messages as well as placing long-distance calls at company expense. He pointed out that the company voice-mail boxes had the same passwords as their own extension. In addition, the phreak encouraged his friends to place free calls at Netcom expense.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1997-07-14 **impersonation social engineering airport hacker**

Newsbytes

The German hacker known as "Kimble Schmitz" infiltrated Munich Airport three times in a few days by smiling at a security guard and by waving a visitor's card purchased from a stationery shop. The hacker and a friend gained access to the VIP jet area, to restricted areas with national and international planes, and to the control tower. Airport managers responded by charging the hacker with trespass. The German press generally sided with the hacker and launched critical stories about airport security. In general, it is not a good idea to test people's security without their permission!

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1997-07-21 **cellular phone cloning phreaking**

Newsbytes

In early May, AirTouch Cellular security staff identified an unusual pattern of fraudulent cell-phone calls in Salt Lake City, UT using numbers assigned to Phoenix, AZ customers. Two illegal aliens were arrested in mid-July and charged with cloning cell phones (assigning other people's electronic serial numbers, or ESNs, to new phones) and then selling the units for $200 each.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1997-07-29 **ISP hackers consortium**

EDUPAGE

In July, the International Computer Security Association (ICSA) formed the Internet Service Provider Security Consortium (ISPSEC) composed of national backbone, corporate value-add and individual dial-up service providers to promote the development of activities to make the Internet a safer place. ISPSEC will develop, implement, and maintain global measures to improve security on the Internet. Through cooperation and communication among multiple ISPs, Internet users will encounter a consistent set of policies and procedures that will prevent or mitigate malicious activity. This is a necessary evolution to build consumer trust. ISPSEC is primarily comprised of large national service providers. ICSA is expanding the ISPSEC concept to regional and local ISPs. It is anticipated and expected that the policies and procedures agreed upon between these large service providers will filter down to the smaller ISPs that are connected via backbone providers. See <http://www.ncsa.com/services/consortia/ispsec/>.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1997-07-30 **hacker phreak**

Newsbytes

A 23 year-old hacker, Leon Fitch of Manchester, was charged in London with three offenses under the Computer Misuse Act. Details of the case were unavailable due to restrictions on reporting of cases sub judice.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1997-08-01 **spam junk e-mail lawsuit damages**

RISKS, AP 19 27

Strong Capital Management, Inc. alleges that David Smith and Glenn Canady broke into SCM's computers to send 250,000 ads with fraudulent headers for "cyberstripping," computer equipment and sports betting. SCM demands penalties of $5,000 per message — about $125M in all. SCM has added mechanisms to stop further transmission of such messages. [The use of civil litigation to attack hackers is one of the most powerful tools available to fight them. This will be an interesting and possibly landmark case with implications not only for the growing displeasure over fraudulent REPLY-TO addresses but also for penetration in general.]

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1997-08-10 **crackers hoax forgery university**

EDUPAGE

Prosecutors in Fairfax County, Virginia, have filed criminal charges against two George Mason University students for hacking their way into university computers and sending derogatory e-mail under the names of random students and staff members. (from summary by EDUPAGE editors John Gehl and Suzanne Douglas).

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1997-09-02 **AOL hacking criticism parody satire criticism**

ZDNN

AOL repeatedly tried to shut down the Inside AOL site, which allegedly posts tips on breaking AOL security as well as the usual criticism and satire of the giant VAN. The anonymous Webmaster insisted on continuing to publish graphical objects taken without permission from AOL, claiming Fair Use.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1997-09-18 **war dialing hacker**

ZDNET

Peter Shipley, a computer security expert in Berkeley, CA, dialed 1.4 million telephone numbers, day and night, to count the number of modem lines. He found 14,000 of the numbers to be modems; the article did not report on the 99% (around 1,386,000 phone numbers) of calls that didn't have modems connected. Next time you are awaked at 3 in the morning by a silent phone call, perhaps you should call Mr Shipley to find out if he was testing _your_ line to see if it was a modem.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1997-09-19 **hacker juvenile**

Vancouver Sun

A 14-year-old hacker from the Burlington, ON area was arrested in September after over 500 attempts to enter computer systems all over North America and, according to news reports, evidence of malicious hacking. The child's attacks on US military computers caused his downfall, since according to Sgt. Terry Dickie, one of the fraud squad investigators, "This young fellow did try the military sites and that is part of the reason he got caught. They take a dim view and they are prepared to attack back — to hack the hacker."

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1997-10-01 **password policy penetration identification authentication**

RISKS 19 40

Mike Jeays of Statistics Canada wrote in RISKS, "The CBC [public broadcaster in Canada] aired an article on improvements to the health care system in Manitoba on 24 Sep 1997. Viewers were assured that the security software was `the finest that money can buy.' The technically literate might have been discouraged by the use of a 3-character password in part of the demonstration.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1997-10-06 **hacker vandal intellectual property industrial espionage**

OTC

In Tokyo, a hacker broke into the Nippon Telegraph and Telephone Corporation's (NTT) computer network and stole programs used in software development. According to NTT officials (as reported by OTC news wire), "The culprit is thought to have gained access to the network through the use of an internal identification number after uncovering the telephone number of the modem adapting the phone line to NTT's computer network."

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1997-11-10 **phone phreaking fraud prevention detection**

The Dominion (Auckland, NZ)

The New Zealand Telecom fraud unit saved the company several $M in its first four month in 1997. Using an HP computer to spot unusual calling patterns, the system helps staff notify subscribers if calls seem to be outside their usual usage of the telephone system. Some of the frauds were costing $K per day. The proactive approach to spotting fraud has paid off in reduced complaints from customers and avoidance of disputes over expensive calls.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1997-11-11 **fraud theft credit card**

Reuters

According to police in San Carlos, a city south of San Francisco, four teen-agers hacked their way into an on-line auction house, stole credit card numbers and fraudulently obtained $20,000 of computer equipment which they arranged to have delivered to an empty house in their neighbourhood. Police caught up with the juvenile gang when one of the children had stolen goods delivered to his own home.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1997-11-14 **phreak phone hacker default canonical password**

RISKS 19 46

Phone phreaks have exploited canonical (default) passwords on PBXs, allowing unlimited international calls from the Macedonian Foreign Ministry. The PBX was left with its DISA (direct inward service access) enabled, allowing the intruders to exploit the system by using a well-known standard password.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1997-11-26 **hacking penetration survey**

RISKS 19 47

The US Senate Permanent Investigations Subcommittee found evidence that "Worldwide, hackers cost businesses an estimated $800 million in 1995 through break-ins to computer systems at banks, hospitals, and other large businesses."

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1998-02-08 **access control QA**

EDUPAGE

A widely-used physical access-control system has a design flaw: people can dial into the control system and make changes. Airport security officers were particularly concerned about this problem.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1998-02-26 **criminal hacker cracker penetration theft bank international**

RISKS, COMPUTERGRAM 19 61

Vladimir Levin was convicted to three years in prison by a court in New York City. Levin masterminded a major conspiracy in 1994 in which the gang illegally transferred $12M in assets from Citibank to a number of international bank accounts. The crime was spotted after the first $400K were stolen in July 1994 and Citibank cooperated with the FBI and Interpol to track down the criminals. Levin was also ordered to pay back $240,000, the amount he actually managed to withdraw before he was arrested.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1998-03-22 **penetration hacking international information warfare**

Denver Post

Joshua Gregory Pearson, 18, a computer science major at University of Colorado, was arrested for allegedly providing stolen passwords and access codes to an Israeli hacker called "Heavy Metal" who broke into the U.CO. computer system in March. Apparently Pearson may have used a packet sniffer to intercept passwords and access codes needed to sign on to university computers. The outside criminal hacker also seems to have caused a denial of service by causing unauthorized programs to flood university e-mail accounts with error messages.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1998-04-22 **criminal hackers penetration attack DoD networks satellites**

RISKS, EDUPAGE 19 69

A new MOD (Masters of Downloading this time instead of the older Masters of Deception) criminal hacker group claimed to have broken into a number of military networks, including the DISN (Defense Information Systems Network) and the DEM (DISN Equipment Manager) that controls the military Global Positioning Satellites (GPS).

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1998-05-16 **penetration criminal hacker cracker student**

RISKS 19 74

Peter G. Neumann, editor of RISKS, provided the following summary of a trans-border hacking case: "21-year-old Jason Mewhiney was arrested by the Canadian RCMP on 27 charges related to using a computer in his home to access computer systems of the U.S. government (including NASA and NOAA, the National Oceanic and Atmospheric Administration), as well as Canadian and U.S. universities. In one case he allegedly caused `extensive damages'."

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1998-05-31 **social engineering penetration misrepresentation Web vandal**

EDUPAGE

The ACLU site on AOL was vandalized by an intruder who simply asked an AOL help-desk staffer — now an ex-employee — for a new password for the ACLU account. The success of this ancient trick may be in part a function of the sheer size of the help-desk organizations for large ISPs; with thousands of people staffing the help desks, many of them relatively new and poorly trained, even a very low probability that any one employee will hand out passwords like party favors leads to a very high probability that at least one gullible person will give away the store. For probability freaks, this "birthday formula" is P{at least one failure} = 1 - (1-p)^n where p=probability of one failure and n=number of independent units subject to failure.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1998-06-10 **penetration criminal hacker cracker**

RISKS 19 80

Peter Neumann reported, "The Stanford Linear Accelerator Center (SLAC) computer system was the victim of an intrusion on 2 Jun 1998 that touched about 50 files. The intruder logged in with a password (guessed? sniffed? borrowed?), and left as evidence only a new zero-length file (perhaps set up with write privileges?). In response, SLAC cut its computers off the Internet until yesterday while they tried to figure out what had happened, with 30 people working overtime." A later posting indicated that the attackers used LAN sniffers, which implies an inside job.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1998-07-07 **voice mail penetration intrusion espionage data leakage**

EDUPAGE

The Privacy Rights Clearinghouse warned that voice mail is often an insecure system liable to penetration by outsiders. In May, Michael Gallagher, a reporter for the Cincinnati Enquirer, broke into the voice mail system of Chiquita fruits. The fruits of his espionage were stories in the paper accusing Chiquita of illegal activities. The reporter was fired; the Enquirer eventually paid $10M to Chiquita in damages and published front-page apologies three days in a row to forestall a legal contest.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1998-08-16 **intrusion cracking penetration hacker passwords decrypt**

EDUPAGE

Someone (or several people) broke into sites around the world and copied files containing encrypted passwords. Peter Neumann (the RISKS moderator) reported, "Michael Kleber, a UC Berkeley Sys Admin, discovered that someone had cracked his password, and was using his account — having already successfully cracked about 48,000 passwords from a list of 186,126 encrypted passwords. From Berkeley, the cracker broke into systems at "a noted Silicon Valley company", an Indiana ISP, other UC Berkeley systems, Caltech, MIT, and Harvard, having used a Swedish ISP Telenordia, and coming through computers in England, Denmark, and South Korea. He was finally detected on 29 Jun 1998. [Source: Henry K. Lee, *San Francisco Chronicle*, 13 Aug 1998, A21]" The FBI was investigating the break-ins.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1998-11-08 **hackers penetration FBI DoD Pentagon**

EDUPAGE, RISKS

In mid-February, criminal hackers increased the frequency of attacks on unclassified DoD computers. Two teenaged (16, 15) criminal hackers from Cloverdale, CA (north of San Francisco) broke into 11 military computer systems, those of several universities and federal laboratories. They were caught with the cooperation of their ISP in late February. The ISP provided facilities for FBI monitoring of the miscreants' activities. In November, the "Cloverdale Two" were sentenced to three years probation during which they were forbidden to have contact with computer systems and networks without the presence of an authorized adult. In addition, said the judge, "The defendants will attend school and make their grades."

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1998-11-09 **penetration telecommunications criminal hacker teenager**

South African Independent Newspapers
http://www.inc.co.za/online/news2/south_africa/headlines/tekhack.html

A 15-year-old Pretoria boy was arrested by South African police after a series of penetrations of the S. A. Telkom networks over a two-week period. Administrators tracked the intruder carefully and he apparently did no obvious harm. The teen and an older confederate also allegedly broke into several ISPs in the country.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-01-04 **criminal hackers hacktivism sabotage information warfare**

Los Angeles Times

Maggie Farley, a Staff Writer for the Los Angeles Times, provided an in-depth review of "hacktivist" attacks on Chinese Internet sites. Groups such as Bronc Buster, Cult of the Dead Cow and the Hong Kong Blondes [a gang later found to have been a hoax] have been penetrating Chinese systems, vandalizing government or pro-government Web sites, installing back-door programs for later access and control, and sending out millions of news reports to Chinese recipients — including even head of Shanghai's Internet security division — from randomized e-mail source addresses (to escape identification and prosecution).

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-01-06 **computer crime police enforcement prosecution punishment**

Xinhua News Agency (translated by OTC)

According to the official Chinese government news agency, 1998 was a banner year for the fight against computer crime in China. After several years of 30% annual growth, there were almost one hundred cases of computer crime cases were uncovered — only a small portion of the total, according to the Public Security Ministry. One computer journal estimated that 95% of all Chinese network management centers exposed to the Internet had been attacked, whether by Chinese hackers or by foreigners. According to the Xinhua report, "In one study, Jinhua'an Information Technology Co. recently conducted tests of dozens of security agencies in Shanghai and Shenzhen, and found almost all of their network security systems were undefended. With a lap top computer hooked up to a telephone line, testers easily logged in their networks and reached restricted information in a minute."

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-01-06 **criminal hacker hospital pirated software intellectual property penetration vandalism**

Magyar Hirlap

Police in Pecs (southern Hungary) arrested a 22-year-old student in January 1999 who allegedly penetrated the databases of several hospitals and disabled their servers. He was also found in possession of illegally-copied software and may have been distributing copies. Police said this was the biggest computer hacking crime committed so far in Hungary. The student also possessed a CD from the Matav telecommunications company containing ownership of unlisted (ex-directory) telephone numbers. The student admitted breaking into the databases but did not admit disabling the hospital servers.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-01-06 **criminal hackers Trojans password stealing BackOrifice Netbus theft services police warnings**

Herald Sun (Australia)

Police in Australia warned of a rash of penetrations of ISP users' computers using Trojans such a BackOrifice and Netbus. The victims reported huge bills after criminals stole their user IDs and passwords and racked up hours of connect time in their names. The trojans were discovered in all kinds of executables, including electronic greeting cards, games, and stolen software.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-01-06 **criminal hacker teenager social engineering administrator e-mail forged headers police arrest confession theft services**

Straits Times (Singapore)

Goh Teck Hwee, 17, was arrested for posing as an official from the Singapore ISP SingNet. The top student in his class, he was impressed by the movie "Hackers"and began reading about hacking on the Internet. After learning how to alter the headers on his e-mail to pretend that he was "Dade Murphy" (a character in the movie) and told 20 SingNet users that their accounts were "corrupted." He demanded their user IDs, passwords, and billing information — and four gullible unfortunates complied. He stole ISP service at their expense for several months. He was arrested four days after one of the victims realized what was happening and reported the crime to police. Goh pled guilty to impersonation at his hearing and faced three other charges.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-01-08 **criminal hacker teenager child China Web penetration immunity**

Xinhua (PRC News Agency) via OTC

A 13-year-old middle-school student in the Inner Mongolia Autonomous Region of the People's Republic of China (PRC) managed to penetrate the Guangzhou province official Web site in southern China, where he posted a Web page entitled "Hacker." He then apparently obtained root on a multi-media telecommunication network for the Mongolian capital of Hohhot. Later he threatened to vandalize the main page of the "169"network, a major Mongolian ISP. The child was ruled immune to prosecution because of his age; the police ordered his parents to keep a closer watch on him. [Considering that some criminal hackers have been executed in China, one imagines this advice would be heeded.]

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-01-11 **police criminal hackers phreaks theft telephone service PBX PABX private branch exchange**

Newsbytes

British police began a campaign in January 1999 to crack down on theft of telephone services through subverted private branch exchanges (PBXs). Criminals, including organized crime, were reported to use direct inward services access (DISA) to place long-distance calls at the victims' expense. Since many firms also provide toll-free access to their PBXs, they end up paying for the entire theft. [MK Comment: DO NOT LEAVE DISA ENABLED! Anything you can for legitimate employees using DISA you can also do using telephone cards — and be sure that those cards do NOT show the PIN for the account number.]

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-01-21 **criminal hacker penetration home computer police**

AP

A 19-year-old Danish criminal hacker picked a home computer at random and began attacking it. Unfortunately, the computer belonged to Detective Arne Gammelgaard, head of the Copenhagen police's special computer crime unit. Gammelgaard's personal firewall informed him of the hack and he tracked down the malefactor immediately. The student admitted guilt and was convicted for "unauthorized access to another person's documents or programs." He faced up to six months in jail.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-01-26 **criminal hackers Web vandalism**

Defcon Hacker List

A tizzy in a teapot broke out when the HFG (Hackers for Girlies) vandalized criminal-hacker sympathizer Carolyn Meinel's Web site. The HTML source code included a great deal of abusive text attacking computer security celebrities such as Winn Schwartau and Fred Villella.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-02-15 **criminal hackers challenge contest penetration testing perimeter Japan**

JIJI PRESS NEWSWIRE

International Network Security Inc. of Tokyo appealed to criminal hackers to break into their company's computer systems as an employment test. The new company offered penetration testing, although how it would guarantee its customers' safety given the nature of its proposed employment strategy was not spelled out. The president of the company, Sato Hideaki, is said to be a close friend of Mark Abene, the criminal hacker who spent nearly a year in jail for his part in the depredations of the Legion of Doom and who was responsible in 1997 for accidentally broadcasting a command on the Internet that resulted in his receiving thousands of password files from computers around the world.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-03-01 **criminal hacker punishment sentence court fine damages**

RISKS 20 23

Peter G. Neumann coined a new term: "PGNed" which he modestly defined as "summarized in an abstract." In my opinion it means "brilliantly summarized." Here is a PGNed item about a criminal hacker from Rhode Island: "Sean Trifero was sentenced to one year in prison by a U.S. District Judge for intentionally damaging computer systems (Harvard, Amherst, a Florida ISP, and Alliant Technologies, including planting sniffers and denial-of-service attacks) and unauthorizedly accessing others (Arctic Slope Regional Corp. and Barrows Cable, Alaska), three years subsequent probation, 150 hours of community service, and $31,650 restitution."

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-04-22 **impersonation social engineering ISP credit card password**

RISKS

I recently received an obviously fraudulent e-mail request claiming to be from CompuServe administration and demanding that I submit my user-ID, _password_, and full credit-card information. After I forwarded it to CompuServe support I received a response with the following key text:

> There are currently numerous email messages circulating on
> the service claiming to be official CompuServe notices of account
> and/or billing problems being sent to members which contain
> a form that is supposed to be filled out and returned by email
> or a termination of the account will occur. It is an attempt
> to steal your credit card and CompuServe account information!
>
> DO NOT respond to this or any similar email!
>
> Instead forward a copy of the complete message by email
> to the CompuServe Internet address actionteam@compuserve.com.

RISKS readers may want to remind naive users of any ISP be warned never to respond to requests to reveal their passwords to anyone at an ISP or indeed, on any network. Even in the rare cases where it would be useful to log into a specific account for problem resolution, any authorized personnel who need access to an account will have the capabilities required to change its password themselves. They do not need to know the user's original password.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-04-27 **hacker confederate guilty plea law court justice**

LA Times

In April, Lewis DePayne pleaded guilty to conspiracy to defraud the Nokia Corporation in his attempt to help Kevin Mitnick steal software. He admitted having used social engineering techniques against Nokia, impersonating an employee to gain access to systems. Prosecutors dropped 13 other criminal charges against DePayne and recommended leniency in sentencing (six months of home detention or community confinement, five years of probation, 225 hours of community service and a fine of $2,000 to $5,000).

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-05-12 **criminal hacker hacktivists Web defacement alert**

ANSIR / NIPC Advisory 99-008

The National Infrastructure Protection Center (NIPC) issued an Awareness of National Security Issues and Response (ANSIR) alert in May 1999 warning that a hactivist group called F0RPAXE defaced several US military and government Web sites. The group claimed to be a Portuguese organization opposing the Portuguese government.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-05-13 **hacking contest firewalls**

Reuters

Reed Exhibition Companies of Singapore launched a one-week hacking contest in May 1999. Successful hackers who could vandalize three Web sites protected by various firewalls would win prizes of U$10,000 and S$10,000 (U$1=S$1.70). Critics disapproved of rewarding what would otherwise be criminal activity and complained that such "hack-off"contests reveal little of value about the security systems under attack.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-05-19 **insider sabotage forgery fraud witness-tampering lawsuit dismissal investigation**

AP

In April 1998, Christian Curry was fired by Morgan Stanley Dean Witter, ostensibly for abusing his expense account. Mr Curry claimed at the time that he was fired because he is black and because his employers thought he was a homosexual (he isn't). While waiting for a response to his claim for wrongful dismissal, Curry talked to an old college buddy of his, C. Joseph Luethke, about planting forged e-mail in the company system to demonstrate homophobia and racism. Luethke reported the conversation to the company and sent Curry to a private detective who pretended to be a criminal hacker. Curry paid the "hacker" $200 for insertion of the forged e-mail and was then arrested on charges of forgery, coercion and tampering with physical evidence. However, the lurid story wasn't over yet: it turned out that Morgan Stanley paid Luethke, the "friend," $10,000. In May 1999, all charges against Mr Curry were dropped and he and his lawyers were contemplating a lawsuit against Morgan Stanley, accusing the firm of libel, conspiracy and violating Curry's human rights.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-05-28 **criminal hacker subculture gang group Russia**

Unknown source, Moscow Times

A Russian criminal hacker gang calling itself Chaos Hackers Crew has been wiping out home pages around the world. They steal access codes for ISPs and appropriate services for their nefarious hobby; their criminality made AOL and CompuServe decide to abandon Russia altogether.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-05-28 **criminal hackers attack government Web sites down unavailable vandalism defaced**

AP, New York Times, Newsbytes

Criminal hackers attacked several US government Web sites, including those of the US Senate and the FBI, apparently in retaliation for FBI actions against Eric Burns ("Zyklon"), who was indicted in May on three counts of illegal computer intrusions. The FBI shut down its Web site to increase security. The Senate Web site included the following hacker-lingo: "The FBI may be all over the other groupz, like those gH and tK queerz, cl00bagz gal0re. M0D make th0se m0ronz l00k like a gr0up of special-ed st00dentz! FBI vs. M0D in '99, BR1NG IT 0N FUQRZ! (BTW NIPC IZ ALS0 0WNED)... S0METIMEZ U G0TTA G0 WITH A NAME U CAN TRUST. 4 S0ME, REGULAT10N IZ JUST A WAY 0F L1FE. 0wned (0wn'3d) : the art of showing how stupid a sysadmin can be, see sekurity." Global Hell (gH) was thought to be the criminal-hacker gang that attacked the FBI. The vandals signed their masterpiece, "Mast3rz 0f D0wnl0ading."

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-05-31 **criminal hacker gang syndicate organized crime Asia police arrests**

Newsbytes

In one of the first successful crackdowns on organized computer-crime syndicates, Hong Kong police arrested ten men accused of stealing and reselling illegal access to ISPs. They allegedly stole account information from at least 200 victims and then sold the accounts to thieves who wanted unlimited access to the Net. The gang also sold CDs with pirated music.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-06-01 **criminal hackers Web sites extortion defaced attacks vandalism political government**

AP

The Portuguese criminal hacker group F0RPAXE defaced Web sites of the US Department of the Interior and of the Federal Supercomputer Laboratory in Idaho Falls, ID. The vandals left a note boasting that unless the FBI stopped investigating criminal-hacker gangs in the US, they would destroy government systems.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-06-02 **criminal hacker investigation Web vandalism defacement seizure**

New York Times

The FBI raided several suspected criminal hackers in late May in connection with the wave of attacks on US government Web sites. Paul Maidman, 18, of Waldwick, NJ denied that he was involved in the attacks. However, he admitted, "I got into other servers. I'd look around, read some e-mail, and that would be it." The FBI seized his computer, some diskettes and CD-ROMs. According to reports posted on the Internet, the FBI obtained warrants to require several ISPs to release information about dozens of criminal hacker gangs, pseudonyms and hacking tools.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-06-03 **criminal hacker probes attacks intrusion detection**

Computing (UK)

Howard Schmidt, Director of Information Security at Microsoft, told the Infowar 99 conference in London that the giant software company has detected up to 22,000 probes an hour in attacks on one of its data centers. He said that most of the attacks were from "ankle-biters" (children) trying to raise their status in the criminal hacker underground. He made a special point of warning managers to protect their PBXs against penetration by updating passwords regularly. Microsoft uses the Info.Safe method of having constant challenges to their own networks by Red Teams; employees who detect the attacks win special tee-shirts.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-06-11 **criminal hacker hactivist attacks Web vandalism**

UPI

F0RPAXE, the supposedly Portuguese criminal hacker gang, continued its attacks on governments and universities in the US. They apparently penetrated the Web site of the Illinois State Comptroller's Office, where they vandalized the home page and ridiculed the FBI.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-06-12 **Web attack criminal hackers government**

AP

A new criminal hacker group calling itself Varna Hacking Group (Varna is the name of a Bulgarian province) successfully attacked the Web site of the US Senate — the second hack in two weeks. The criminals hijacked visitors to the site, redirecting them to a Web site on a Florida hosting service where a modified version of the official site was located. The copy of the Web page included ridicule of the FBI; an obscene, anonymous message on the real Senate Web site claimed that the attack was motivated by the desire to stop FBI investigations of criminal hacker groups.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-06-17 **criminal hacker ISP account abuse theft services stealing password**

New Zealand Herald

A 24-year-old Auckland NZ man was arrested and charged with stealing more than $600 of ISP services using a victim's account. The theft was discovered when the victim switched from an unlimited-usage account to a less expensive 10-hour a month account. The thief was identified with the help of ISP log files.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-06-26 **criminal hacker penetration theft embezzlement transfer bank Russia sentence imprisonment prison fines**

RIA (Russian news agency) monitored by BBC

In June, two young Russian hackers were imprisoned for 6.5 and 7 years for having stolen a large amount of money (the news reports are unclear on the exact amount) using a computer program to embezzle the funds from the Berezniki branch of Sberbank in 1997. Igor Chupin and Igor Chernyy [sic] transferred the funds into their own bank account. They took out cash from banking machines in Perm, Moscow and St Petersburg over the next three days. That money was never recovered. The court sentenced these criminals to 7 and 6.5 years in prison, respectively. In addition, the young men are supposed to pay restitution and fines amounting to R2,782,000 (U$28,869), a sum so vast by Russian standards that the Moscow news report ended with the comment, "Judging by everything, they will have to pay the bank as long as they live." [Mind you, in the Russian prison system, that may not be very long.]

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-08-10 **criminal hacker court case law judgement punishment prison fines restitution parent father morality ethics upbringing self-pity excuses rationalization**

SJ Mercury News, Los Angeles Times, Guardian (London), Reuters

Criminal-hacker icon Kevin Mitnick finally negotiated an agreement with prosecutors in California. Mitnick, imprisoned for the last four years much to the disgust of criminal hackers and their sympathizers everywhere, agreed to an additional year of imprisonment and a three-year period thereafter during which he would not use computers. At his sentencing hearing in August 1999, he was also ordered to pay a token $4,125 in restitution and to turn over all profits from any books he may write or interviews for which he may be paid. Mr Mitnick's father said he was proud of his son, whom he said had a lot of talent and was unfairly targeted by prosecutors. "A lot of people made their fortunes off his name," said Alan Mitnick. "He was made to be a poster boy. They wanted to scare other hackers in the future. They also want to control the information superhighway."

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-08-11 **criminal hacker probes Trojans back door**

Bangkok Post (Thailand)

A question-and-answer column in the Bangkok Post, Thailand in August 1999 showed how widespread criminal hacking has become in this Internet-assisted age. Howie Mirkin wrote, "In the past two weeks I have experienced about three to four "back orifice" hacking attempts per day. I have a small program called anti-BO, which detects such attempts. I have been notifying the appropriate ISPs after doing a WhoIs ISP Lookup and a trace route to help them determine the user.
The anti-BO program gives the time and host id. I have had a couple of ISPs come back and tell me that they throw hackers off their connection, but we know that nothing will stop them if they want to hack. . . . It is a real pain to keep getting these hits and have to stop working and gather data to report them. Are there any laws about this? What I really wonder is how many people are getting hacked without knowing it because they have no detection program."

Craig Emmott, Director of Support Services of Internet Thailand, responded, "Unfortunately, scanning for backdoor programs such as Back Orifice is very common these days. If ISPs are informed of the time and origin-IP of the scanning they can contact the owner of the account being used at the time. However, this will often turn out to be a hacked account or the owner will deny all knowledge of the incident. Until the TOT and TA provide caller-ID on modem access lines, there is little ISPs can do other than advise these account owners to change their password." He added, "Generally, these would-be hackers don't target any specific individual. Instead, they scan whole blocks of dialup lines belonging to target networks. The main objective is to steal passwords and use them to get some free Internet access at other users' expense." Finally, he commented, "There are now over 100 backdoor/Trojan programs available on the Internet, but Back Orifice and NetBus are still the big favourites in Thailand. The most practical defence against them is to only run software from trusted sources and to use one of the major anti-virus products, all of which can detect the most widely used Trojans."

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-08-18 **criminal hacker hoax lie manipulation press gullible evidence investigation fraud spoof media**

IT Daily (AsiaTech)

Investigation of the supposed depredations of the "Hong Kong Blondes" strongly suggested that the criminal hacker gang supposedly led by "Blondie Wong" was a hoax by the Cult of the Dead Cow.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-08-31 **back door e-mail script Web confidentiality bug**

PA, Wired http://www.wired.com/news/news/business/story/21490.html

In August, two serious security holes were demonstrated on the HotMail servers run by Microsoft and claimed to be the biggest free Web-mail system in the world, with millions of subscribers affected. The problems were as follows:
(1) An error in the code for entering data into a form allowed a user login without any password at all;
(2) An undocumented back door allowed anyone to log in to any HotMail account using the canonical password "eh."
These problems meant that all unencrypted HotMail e-mail was readable to anyone who used the exploits and that such people could also impersonate their victims through e-mail. The holes caused Microsoft to shut down access to HotMail for a day while the vulnerabilities were removed.

The perpetrators, calling themselves "Darkwing" and "Hackers Unite," took responsibility for the hack. The criminal hacker spokesperson was Swedish computer expert Lasse Ljung, who said, "Hackers Unite hacked Hotmail because they wanted to show the world how bad the security is on Microsoft. . . . It is a big company on the net, so it wasn't to destroy it for others, it was to show the people how bad the security is."

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-09-02 **criminal hacker denial of service punishment jail prison China vandalism**

Xinhua

Lu Xuewen, 24-year-old high school graduate in Guanzhou (formerly known as Canton) in the PRC, penetrated the mainframe of government-owned ISP Chinanet and also a BBS server using stolen account numbers in January and February 1998. He created additional accounts for himself on the system and crashed the system for 15 hours. He was jailed for 18 months under the Criminal Law of 1997 that updated statutes to make unauthorized access to computer systems a crime.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-09-10 **Y2K criminal hacker quality assurance tests electricity power**

Wall Street Journal

According to a report in the Wall Street Journal, the successful Y2K-compliance tests carried out in early September by the North American Electric Reliability Council (NERC) with the involvement of over 500 utilities, electric cooperatives, power pools and power plants were marred by a criminal-hacker penetration of the Bonneville Power Administration center, where the Secretary of the Department of Energy, Bill Richardson, was observing the tests.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-09-17 **criminal hacker gang disruption penetration**

New Straits Times (Malaysia)

According to a spokesperson for the Malaysian ISP, Jaring, a group of users based in a Malaysian university were responsible for breaking into at least 18 organizations and controlling more than 38 servers. The criminal hackers were among a large worldwide group causing harm to Undernet, one of the world's larges IRC channels. The Malaysian CERT put up recommendations for improving security on its Web site at <http://www.mycert.mimos.my>.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-09-20 **magazine hacking contest quality assurance encourage criminal hackers legitimize hacking**

PR

PC Week Labs staged an unfortunate quality assurance contest pitting criminal hackers and others against a servers running LINUX Windows NT. The magazine challenged anyone to break into the Web site, as if such a test could be a reasonable demonstration of the security characteristics of the two operating systems. Those who successfully "mark up the home page and steal user information from the classified-ads engine" would be rewarded with computer equipment and gift certificates for about $1,000.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-09-24 **criminal hackers hactivisits political Web site defacement vandalism propaganda**

Detik (Jakarta) via BBC Monitoring Service

Indonesian Web sites were hacked by pro-Timorese hactivists starting in September 1999. The Antara Web site was defaced, with the following message left in place of the anodyne commercial text: "Indonesian Military Sponsors Mass Genocide 250,000 DEAD since 1975. How can you condone this? Your leaders have no respect for human rights. Will they have respect for yours? Your army has supported armed and trained anti-independence DEATH SQUADS in East Timor. Indonesia itself gained independence. Why has Indonesia then destroyed East Timor's dream of freedom? It is better to live one day in freedom and die than live a lifetime in the yoke of an oppressor."

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-09-29 **criminal hacker bank financial transactions penetration credit card confidentiality**

Scotsman

Frans De Vaere admitted breaking into the Web site of a Belgian bank in mid-August. He stole logon IDs and passwords and successfully accessed the account balances of many customers; luckily he was unable to effect any transactions. The bank, identified as "Generale de Banque" in a report by Alex Blair in _The Scotsman_ newspaper, refused to take legal action against the criminal hacker. However, the Skynet ISP run by the state telecom company, Belgacom, was not so accommodating. The criminal hacker broke into more than 1,000 Web sites on Skynet and stole the credit-card numbers of about 20 clients. Police began an investigation, but unfortunately Belgium has no specific law addressing computer crime and so the intruder is still unpunished.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-10-14 **criminal hacker ISP theft of service vulnerability**

SMH

In an odd twist, the Australian ISP FreeOnline treated a criminal hacker respectfully after he claimed in the Oz version of _2600_ magazine that it was possible to use the ISP without registering for a userID and password. Members of the criminal hacker magazine's club affirmed that the exploit was in fact being used successfully despite the denials of the ISP's technical staff that there was a vulnerability. The company's CEO, Sydney Low, said, "If Pho can show us that there is a flaw we'll pay him $100 an hour, because we're happy to support behaviour that increases the smarts of the industry. While we don't want to stifle this kind of activity, we don't think he should have posted the hack to a Web site without confirming its legitimacy with us first." [This kind of statement gives succour to the enemy and feeds the propaganda engine of the criminal underground. There is no place for acceptance of people who break into systems, steal services, and then boast about their exploits in detail so that other criminals — and children — can imitate their behavior.]

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-10-14 **criminal hacker threats vulnerability critical infrastructure electric power utilities damage**

Dow Jones

"Mudge" (Peiter Zatko), a member of the L0pht, claimed in mid-October 1999 that he would release a report on security vulnerabilities at about 30 electric power utilities in the US whose grids he claimed he could shut down easily. In a welcome change from other cases involving unauthorized probes of networks, Zatko said that the L0pht would give the utilities a chance to see the report and fix the vulnerabilities before they were posted in public.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-10-18 **hacking contest quality assurance test trial exposure**

Reuters

The Shanghai Waigaoqiao Free Trade Zone Network Development Co. offered anyone who could break into their Web site 5,000 Yuan (U$600) in mid-October 1999 during a one-week trial.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-10-20 **criminal hacker punishment prison appeal sentence judgement government**

Straits Times (Singapore)

Muhammad Nuzaihan Kamal Luddin, a 17-year-old high school student in Singapore, hacked into Swiftech Automation and Singapore Cable Vision and was sentenced to 2-1/2 years on probation by a district dourt in June 1999. However, the government appealed the sentence and won a stricter penalty for the young man's criminal activities: four months in jail. The decision sparked a vigorous debate about the suitability of imprisonment as a punishment for criminal hacking by young people.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-10-21 **criminal hackers Israel politics police law enforcement prosecution court phreaking theft of services telephone long-distance calls**

Wall Street Journal

In October 1999, the Israeli government finally began the trial of two blind Israeli Arab brothers, Munther and Muzhir Badir. The two were suspected of a series of major attacks on telephone systems for call-sell operations, fraudulently selling other people's land, and credit-card fraud. The indictment included 47 different counts of criminal activity. The flamboyant brothers became celebrities in Israel, with regular interviews in the media. The bitter intercommunal relations of Jews and Arabs in Israel complicated the case, with many opponents of the Israeli government claiming that the brothers were abused in the notoriously rough Israeli jails. In one interesting wrinkle, Munther Badir claimed that he worked for the Labor Party in 1998; he said he had sabotaged the party's system and then repaired it, blaming the crash on the Prime Minister's political opponents. However, Labor Party officials denied any record of Badir's working for them.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-11-03 **criminal hacker penetration ISP passwords**

AAP, Courier Mail (Brisbane)

Someone broke into the Australian Optus Internet ISP on 1999-11-03. The ISP contacted its 100,000 customers and told them to change their passwords for Internet logon. Police were investigating.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-11-11 **criminal hacker prison penetration vandalism Web passwords theft**

AP

In Singapore, Pang Soon Chen, 19, and David Kok, 22, were sentenced to 15 and 8 months in prison respectively for breaking into 54 Internet users' computers and stealing their passwords. The two also posted the passwords to a Web site in the US.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-11-17 **information warfare attack criminal hacker contest challenge firewalls**

Xinhua (Beijing)

In October, a Shanghai company issued a challenge to hackers to test its Web site security. The site was attacked 76,250 times in the first two weeks of the challenge, with peak rates of 1,253 attacks per second. No known penetration occurred.

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-11-23 **criminal hacker punishment conviction trial Web vandalism**

AP

Eric Burns, 19, pleaded guilty in September was convicted in November 1999 of criminal hacking and admitted that he had vandalized many other Web sites, including the White House site, in May. Despite his sentence of 15 months in prison and three years of supervised probation along with restitution of $36,240, the lad said, "I didn't really think it was too much of a big deal." Cost of recovering the government sites was estimated at $40,000. Burns, who called himself "Zyklon" after the gas used by Nazis to murder Jews in death camps, said he thought his penalties were too severe and vowed not to identify his two confederates. "I don't really agree with the kind of sentencing range there is for the crime."

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-12-06 **inside job criminal hackers hactivists political penetration information warfare INFOWAR**

Daily Telegraph (UK)

Criminal hackers (or possibly insiders) penetrated the computer systems of the Palestine Liberation Organization in December 1999. The unknown assailants published secret information about Chairman Yasser Arafat's billions of dollars of savings in secret Swiss numbered bank accounts and extensive land holdings in various European cities. Daily Telegraph writer Tom Gross reported, "The computer security breach is believed on the West Bank to have been carried out by PLO officials disgruntled with Mr Arafat's leadership."

Category 17 *Penetration, phreaking, cramming, uncapping (entering systems, stealing teleph*

1999-12-08 **criminal hacker gang telephone services abuse phreaking credit-card theft fraud plea court trial**

UPI

In 1995, FBI agents raided a ranch in a rich neighborhood north of San Diego and confiscated Jonathan Bosanac's computer. In December 1999, the now-27- year-old criminal hacker pleaded guilty to what police were calling the largest computer hacking scheme in US history. The gang led by Bosanac (aka "The Gatsby") broke into computers at AT&T, MCI and Sprint (among others) and stole thousands of calling card numbers which they sold to other criminals at $2 each. The cards were then used to make thousands of illegal long-distance phone calls. The gang also forwarded an FBI telephone number to a phone-sex line, racking up $200,000 in embarrassing phone bills. At one point, they harassed a victim by automatically sending his phone number to thousands of pagers. in September, the courts sentenced two other criminals in what the FBI called the Phonemasters to jail terms: Corey "Tabbas" Lindsley got 41 months in prison and Calvin "Zibby" Cantrell received a 24 month term. Seven other defendants in the case had already pleaded guilty in federal court and were awaiting sentencing. Bosanac was to be sentenced on 2000-03-02.

17.1 Penetration

Category 17.1 Penetration

1999-02-25 **criminal hackers Internet spam virus denial of service**

BBC translation of Bulgarian BTA report

On January 26, criminal hackers attacked the Internet site of the Bulgarian Telecommunications Company in Sofia. The attackers used the site to send virus-infected e-mail [possibly Trojan attachments] to several thousand victims via a US server. On February 5, attackers repeated the spam attack, sending infected e-mail to "a prestigious US college." A few days later, reported the Bulgarian radio service, the BTC e-mail server was subjected to a denial of service spam attack. Luckily, the spam attacks were of sufficiently low volume that users were not inconvenienced.

Category 17.1 Penetration

1999-03-11 **information warfare social engineering penetration**

RISKS 20 24

An experienced Internet user who happens to use AOL for convenience was shocked to find an e-mail message in his in-basket that contained his AOL password. Moments after opening that e-mail, he as contacted by "Bob SiteOp" using Instant Messaging; this person claimed to be an AOL staff member and demanded to know the contents of the e-mail. The user refused and contacted AOL to no avail — the staff stonewalled and claimed that AOL does not keep passwords on disk (presumably only one-way encrypted passwords). Despite considerable effort on the user's part, he never received an explanation of what had happened.

Category 17.1 Penetration

1999-04-30 **Internet service provider ISP privacy surveillance scans PCs**

Reuters

An uproar broke out when Singapore Telecom scanned 200,000 computers belonging to its Internet service customers — without their knowledge or permission. At first, the company hung tough: "We are merely protecting the interest of our customers," said Paul Chong, CEO of Singapore Telecom. Staff explained that the non-invasive scans, carried out by anti-hacker personnel from the Ministry of Home Affairs, did not penetrate systems but merely noted vulnerabilities visible to any hacker. However, the company announced that 900 virus-infected computers had been found — which hardly seems non-invasive. The company apologized to its customers within a couple of days after the furore erupted.

Category 17.1 Penetration

2000-01-09 **criminal hacker sabotage vandalism sentence trial judgement**

RISKS, NewsScan, USA Today 20 73
http://www.usatoday.com/life/cyber/tech/ctg955.htm

In New Rochelle, NY, a former volunteer for AOL technical support was sentenced to one year in jail for breaking into AOL and causing $50K in damages. Jay Satiro, 19, was described by his own lawyer as, "a disturbed young man." After pleading guilty of computer tampering, he was barred from having a computer in his room or computer access in his home. Judge M. Perone's severity may have been influenced by Satiro's having committed the latest offence while on probation for having used forged money orders to buy computers.

Category 17.1 Penetration

2000-01-12 **criminal hacker penetration intrusion passwords theft cracking youth child adolescent**

NewsScan, Los Angeles Times
http://www.latimes.com/business/20000112/t000003535.html

A 16-year-old boy from the Global Hell gang of criminal hackers was arrested in Eldorado, CA for allegedly stealing user IDs and passwords for 200,000 accounts at an ISP run by Pacific Bell. Police reported that the boy had decrypted 63,000 of the passwords. The lad boasted about his exploits in a chat room; apparently he may have been the hacker responsible for 26 other break-ins, including a computer at Harvard University.

Category 17.1 *Penetration*

2000-03-23 **criminal hacker informer vandal sabotage government**

NewsScan

Twenty-seven-year-old Max Ray Butler of Berkeley, California, has been indicted on charges of breaking into and causing damage to government computers belonging to such agencies as NASA, the Argonne National Labs, the Brookhaven National Lab, the Marshall Space Center, and various facilities of the Department of Defense. Butler (also known as "Max Vision") has in the past been an FBI source, helping the Bureau solve computer crimes. (AP/San Jose Mercury News 23 Mar 2000)

Category 17.1 *Penetration*

2000-07-13 **criminal hacker penetration misuse misappropriation arrest complain charges court credit-card theft gang**

RISKS 20 95

Keith Rhodes contributed the following summary to RISKS: >A 20-year-old man was arrested Wednesday for allegedly breaking into two computers owned by NASA's Jet Propulsion Laboratory and using one to host Internet chat rooms devoted to hacking. Raymond Torricelli of New Rochelle, N.Y., was named in a five-count complaint that also charged him with sending unsolicited advertisements for a pornographic Web site and intercepting passwords and usernames traversing networks of computers owned by Georgia Southern University and San Jose State University. He was also accused of stealing credit card numbers that were used to make more than $10,000 in unauthorized purchases. Court papers, which were unsealed in Manhattan federal court, alleged Torricelli was the head of a hacker group known as "#conflict" and that he used the name ``rolex." [Source: Reuters, 12 Jul 2000]<

Category 17.1 *Penetration*

2000-09-11 **penetration credit card information theft Web site**

RISKS 21 04

Peter G. Neumann wrote, "Western Union warned thousands of online customers on 9 Sep 2000 that hackers had broken into the company's Web site. Although no fraudulent transactions or breaches of personal information had been discovered, the penetration could have affected on-line users. More than 10,000 customers were being alerted, suggesting they cancel their credit and debit cards. The Web site was out of service that evening, and was expected to remain that way for several days."

Category 17.1 *Penetration*

2000-09-22 **criminal hacker penetration damage trusted computing base trial punishment sentence judgement juvenile**

NewsScan, New York Times
http://partners.nytimes.com/2000/09/22/technology/22AP-HACK.html

A sixteen-year-old Florida boy . . . [was] sentenced to six months in a federal detention center for having used the Internet to break into government computers, including ones operated by NASA and the Pentagon. Attorney General Janet Reno said, "Breaking into someone else's property, whether it's a robbery or a computer intrusion, is a serious crime." (AP/New York Times 22 Sep 2000)

Category 17.1 *Penetration*

2000-10-04 **penetration fraud spoofing Web insider bank theft arrest wiretap**

RISKS 21 08

In Sicily, police arrested 21 alleged cyberthieves who were in the process of stealing half a billion dollars (2 trillion lira) from the Banco de Sicilia. According to news reports, the gang included members of the Mafia, computer specialists and bank employees. Thanks to wiretaps, the perpetrators were stopped before they could complete their money transfers. Their plans were reported to include attacking the bank of the Vatican.

Category 17.1 *Penetration*

2000-12-06 **hospital medical records confidentiality privacy intrusion penetration hack**

RISKS, SecurityFocus http://www.securityfocus.com/news/122 21 14

Kevin Poulson, writing in SecurityFocus, broadcast a report about a catastrophic failure of security, a criminal hacker from the Netherlands was able to penetrate the admissions records for over four thousand cardiac patients at the University of Washington Medical Center in Seattle. The records were exposed to the Internet without firewalls or any other defenses. Compounding the problem, administrators who discovered the hack penetration in mid-July, a month after they began, were apparently unaware that the records had been copied and failed to notify law enforcement officials. Despite initial refusal by UWMC technical staff to believe the reports, Poulson provided them with irrefutable evidence of the penetration: their own data.

Category 17.1 *Penetration*

2000-12-23 **penetration public relations response open frank**

RISKS 21 16

Egghead.com discovered a potential breach of their customer databases during a hacker penetration of their system. The company immediately published a warning to its customers as a precaution.

[MK comments: The frank, open response was a refreshing change from stonewalling and concealment that unfortunately characterizes so much of corporate and government reactions to security breaches.]

Category 17.1 *Penetration*

2001-01-26 **criminal hacker indictment trial intrusion**

NewsScan

HACKER INDICTED FOR NETWORK VANDALISM
Twenty-one-year-old Jerome Heckenkamp has been indicted by federal prosecutors for allegedly hacking into computers at eBay, Exodus, Juniper, eTrade, Lycos, and Cygnus and causing a total of more than $900,000 in damage, in events that took place in 1999 while he was a student at the University of Wisconsin. He has pleaded innocent of all charges and says the break-ins were done by someone else using his computer. (AP/San Jose Mercury News 25 Jan 2001)
http://www.mercurycenter.com/svtech/news/breaking/ap/docs/786396l.htm

---

Category 17.1 *Penetration*

2001-04-05 **government audit security systems failures critical operations vulnerability fraud misuse disruption availability penetrations**

RISKS 21 36

A report by the U.S. General Accounting Office on security at 24 agencies found widespread security failures. A brief summary by Peter G. Neumann in RISKS stated, "During the year 2000, 155 federal computer systems (some with sensitive information) were taken over by unauthorized users who gained full administrative privileges. The military recorded 715 serious attacks in that period."

Category 17.1 *Penetration*

2001-04-11 **appropriate use confidentiality MS-Word document history data leakage QA quality assurance modem penetration**

RISKS 21 35

Tsotomu Shimomura revealed that there was a back door in the Alcatel ADSL modem that would allow anyone to "penetrate a computer system linked to the Internet by Alcatel 1000 ADSL and Speed Touch Home modems." The interesting consequence was that Alcatel posted a statement about the problem on their Web site. Unfortunately for Alcatel, someone chose to post a MS-Word document in which all the changes were still accessible, including the following embarrassing dialog reported to RISKS by Mike Bristow:

> (When and where will the firewall software be available? CERT has
> said that they don't believe that installing a firewall is the
> answer. What are you doing to provide a legitimate fix?)

Category 17.1 *Penetration*

2001-06-12 **power station grid criminal hacker critical infrastructure vulnerability risk**

RISKS 21 46

Peter Neumann wrote in RISKS, "Reuters reported on 11 June 2001 that the California Independent System Operator's flow-control computer systems had been hacked for at least 17 days before it was detected on 11 May 2001 -- in the midst of the ongoing power crisis. Although they attacks did not noticeably disrupt operations, they apparently came quite close -- and exposed some vulnerabilities that demonstrably need to be fixed. The main attack was seemingly from someone in China's Guangdong province, via China Telecom, and exploited Internet servers in Tulsa OK and Santa Clara CA."

Category 17.1 *Penetration*

2001-07-03 **criminal hacker ISP Internet service provider international court lawsuit prosecution trial judgement penalties fines**

RISKS 21 50

Dave Stringer-Calvert summarized a case of hacking gone drastically wrong in the UAE: "A computer whizzkid has been fined £2,000 ($2,600) for hacking into the United Arab Emirates' only Internet provider and causing the whole country's system to crash. Lee Ashurst, 22, originally from Oldham in Greater Manchester, was convicted of misusing equipment, services or facilities provided by Emirates Telecommunications Corp Etisalat. Ashurst, who works for a construction company in the Gulf, is now facing a compensation claim of more than £500,000 ($650,000) from Etisalat after the Dubai Court of First Instance transferred his case to the civil courts. He was working as a computer engineer at a Dubai construction firm in May last year (00) when he began hacking into Etisalat's systems. According to the Gulf News newspaper, the court was told the entire United Arab Emirates internet system crashed on several occasions over a month."

http://63.108.181.201/2001/07/03/eng-wenn/eng-wenn_001056_76_4245186652988.html

---

Category 17.1 *Penetration*

2001-11-20 **Web confidentiality penetration disclosure compromise criminal hacker credit card pornography**

RISKS 21 78

The Playboy.com Web site was penetrated by a criminal hacker who stole some customer information, including credit card data. According to an article in CNET News, "Playboy.com also said it reported the incident to law enforcement officials and hired a security expert to audit its computer systems and analyze the incident."

Category 17.1 *Penetration*

2001-12-05 **court ordered penetration financial system trial judge hacker intrusion data diddling modification account alterations**

RISKS 21 82

Under court order, an expert security specialist easily penetrated a financial system run by the US Department of the Interior and was apparently never detected when he created a false account and modified an existing account. The hack was authorized by U.S. District Judge Royce C. Lamberth as part of a lawuit against the DoI for mishandling 300,000 trust accounts for American First People.

Category 17.1 *Penetration*

2002-01-20 **database vulnerability contest advertising hackers attack testing penetrations vulnerabilities**

Security Wire Digest 4 5

ORACLE "UNBREAKABLE" BOAST BEING TESTED
Oracle's "Unbreakable" advertising campaign is about to be broken, say industry experts. Following Oracle's boastful marketing campaign that kicked off in September, hackers began blasting away at the company's code, resulting in a tenfold surge in hacking attempts. Though Oracle says none of the attempts were successful so far, a presentation scheduled for early February may soon change that. According to SecurityFocus, U.K. security researcher David Litchfield will reveal "a suite of at least seven vulnerabilities currently in the company's patch pipeline." Some security experts have said that these vulnerabilities change the claim of "unbreakable" from marketing hype to a false sense of security.

Category 17.1 *Penetration*

2002-02-20 **physical security Windows share network compromise confidentiality control penetration**

RISKS 21 92

Greg Searle posted a cautionary note warning novice users about the importance of preventing access to their workstations when they step away from their desks. He pointed out that it takes only seconds to set the share property of a drive to allow total access from anywhere in the network. No one would ever know that the share had been changed or who changed it. Lock down your machine before leaving it. On a Windows 2000 or Windows NT machine, it's as simple as hittling CTL-ALT-DEL and clicking on LOCK.

Category 17.1 *Penetration*

2002-02-27 **penetration confidentiality cracking criminal hacker consultant Social Security Number SSN vulnerabilities holes demonstration ethics professional standards**

NewsScan

SECURITY CONSULTANT SAYS HE HACKED NYT COMPUTERS [27 Feb 2002]
Adrian Lamo, a 20-year-old part-time security consultant in San Francisco, claims to have hacked the Web site of the New York Times and browsed through the names and Social Security numbers of the newspaper's employees, customers, and editorial contributors. Lamo says he notified the newspaper of what he had done -- and that the Times has patched up the security holes but has not acknowledged that he penetrated its system. (AP/San Jose Mercury News 27 Feb 2002)
http://www.siliconvalley.com/mld/siliconvalley/2752998.htm

In September, an article in the New Scientist reported, "A computer security expert has revealed how he altered news articles posted to Yahoo!'s web site without permission. The incident highlights the danger of hackers posting misleading information to respected news outlets. Freelance security consultant Adrian Lamo demonstrated that, armed only with an ordinary Internet browser, he could access the content management system used by Yahoo!'s staff use to upload daily news. He added the false quotes to stories to prove the hole was real to computer specialist site Security Focus. Yahoo! has issued a statement saying the vulnerability has been fixed and security is being reviewed. But experts say that the incident demonstrates a serious risk. "Just think how much damage you could do by changing the quarterly results of a company in a story," says J J Gray, a consultant with computer consultants @Stake."
http://www.newscientist.com/news/news.jsp?id=ns99991329

Category 17.1 *Penetration*

2002-04-22 **criminal hackers fraud penetration data corruption**

RISKS 22 04

Peter G. Neumann wrote:

>A group of Chicago Web site operators say they will break into school, government and corporate computers and alter records, for fees starting at $850. But at least one security expert thinks the operation probably is a scam. Among the services promised by Chicago-based 69 Hacking Services, is changing bad grades and other records on elementary, high school or college computer systems. [Source: Brian McWilliams, Newsbytes,
http://www.newsbytes.com/news/02/]<

Category 17.1 *Penetration*

2002-04-22 **Internet banking penetration data theft confidentiality Web breakin crackers criminal hackers**

Security Wire Digest 4 31

FLORIDA BANK BREACH NETS ONLINE BANKING DATA
A cracker managed to breach a Florida bank's firewall and steal the personal data of 3,600 online-banking customers. Officials at Republic Bank--among the first in the state to offer Internet banking in 1996--discovered the incident a few weeks ago but kept it from customers until April 17. The theft came to light after the attackers contacted the bank, whose main Web site runs Microsoft's IIS 4.0 and is hosted by Advances.com of Fort Lauderdale. No accounts were accessed during the attack, the bank reports. The FBI is investigating and Republic Bank has contracted a team of security consultants to review its systems.

Category 17.1 *Penetration*

2002-04-25 **crimina hacking bank penetration data theft automated teller machine ATM trial conviction prison sentences**

Security Wire Digest 4 32

RUSSIAN ATM CRACKERS SENT TO PRISON
Two leaders of a Russian hacker group received five-year prison sentences for their roles in stealing almost a million dollars from foreign bank accounts after manipulating automatic teller machines (ATM) in Moscow. More than 6,000 people were victims of the thefts, according to a news report. Zviadi Beria and Vladimir Medvedov, who adamantly denied their guilt, were each sentenced to five years in prison. The group's main organizer, Yuri Levashov, cooperated with authorities and received a three-year sentence, with immediate release due to a special arrangement. Four others were given three-year suspended sentences.

Category 17.1 *Penetration*

2002-05-05 **penetration confidentiality data leakage Web defacement management response**

RISKS 22 05

Midwest Express Airlines distributed the following announcement about a hack:

On the morning of Monday April 22, Midwest Express Airlines was informed that customer profile data had been published on the Internet, specifically on the U.S. Space and Naval Warfare Systems Command Web site. The data published contained a handful of user profiles including names and e-mail addresses. This screenshot of data was captured from the Midwest Express test server, not the actual Web site. This test server is used for testing new enhancements to www.midwestexpress.com.

Midwest Express has always taken steps to ensure security. As a result of this situation, a number of additional precautionary measures were taken to ensure that customer data was protected:

* The U.S. Space and Naval Warfare Web site immediately removed the defaced Web page from the Internet.

* A security company was contracted to eliminate any vulnerability to our test server.

* All customer passwords to Web profiles were changed to protect and restrict access to the customer data.

Since all passwords have been changed, the next time you visit midwestexpress.com and login to your profile, you will be prompted to change your own password upon successfully answering a challenge/response question that you created.

While Midwest Express is confident in the security of its Web site, we are always assessing our Web site for potential vulnerabilities and taking appropriate steps when needed. We assure you that your customer information, purchases and other transactions are secure.

Category 17.1 *Penetration*

2002-05-17 **credit report confidential personal data identity theft penetration criminal hackers**

NewsScan; http://www.nytimes.com/2002/05/17/technology/17IDEN.html

CREDIT REPORTS STOLEN FROM EXPERIAN DATABASE
Network vandals have stolen 13,000 credit reports in recent months from Experian, a national reporting agency. An Experian executive said, "I've never seen anything of this size. Privacy is the hallmark of our business. We're extraordinarily concerned about the privacy issue here, and the trust factor." The intruders used an authorization code from Ford Credit to obtain the reports, which gave the intruders access to each victim's personal and financial information, including address, Social Security number, bank and credit card accounts and ratings of creditworthiness. Ford has sent letters via certified mail to all 13,000 people, urging them to contact Experian and the two other major credit reporting companies, Equifax and TransUnion, and to report any evidence of abuse to the FBI. (New York Times 17 May 2002)

Category 17.1 *Penetration*

2002-05-27 **criminal hackers penetration state database financial information SSN**

RISKS, FINDLAW 22 10

Computer hackers have cracked into the California state personnel database and gained access to financial information for all 265,000 state workers, including Governor Gray Davis, officials said Friday [May 2002]. The database, housed at state's Teale Data Center in Rancho Cordova, holds names, Social Security numbers, and payroll information for everyone from office workers to judges. Authorities said that so far they have found no evidence that the information has been used illegally. <http://www.sfgate.com/cgi-in/article.cgi?file=/chronicle/archive/2002/05/25/MN179392.DTL>

Category 17.1 *Penetration*

2002-08-14 **criminal hacking university officials industrial espionage penetration policy punishment ethics**

NewsScan

YALE ACCUSES PRINCETON OF HACKING INTO ADMISSIONS RECORDS
Princeton University has admitted that its admissions personnel hacked into rival Yale's computer system to check on the applications status of 11 students who also had applied to Princeton. The university has suspended with pay its associate dean and director of admissions, and a spokeswoman expressed deep regret "that information provided by students in good faith to the university was used inappropriately by at least one official in our admissions office." The perpetrator(s) apparently were easily able to access the students' records via the publicly available Yale.edu Web site because they already had the students' passwords -- the names, Social Security numbers and dates of birth they had provided on their Princeton applications. The site had been set up with a feature that enabled students to check on the status of their applications themselves. The founder of one electronic-rights group noted that while Princeton's actions clearly were wrong, it was foolish of Yale to rely on Social Security numbers and birth dates to secure student data. "It's not enough to have a weak Web site and depend on the good ethical behavior of others not to penetrate it," he said. "Similarly, it is not adequate to say that just because you found the weak Web site you should go ahead and penetrate it." (Wall Street Journal 26 July 2002)

PRINCETON'S PUNISHMENT FOR COMPUTER VANDALS
Princeton University has decided on the punishment for two Admissions Office officials responsible for the invasion of Yale University's computer system to obtain applicant files: the one who actually did the breaking in will be transferred to another job, and the dean to whom he reported will be allowed to retain his position until his scheduled retirement next June. Princeton president Shirley M. Tilghman says the university has learned from this episode of computer vandalism: "One of the lessons of this experience is that even individuals with a high degree of sensitivity to ethical principles in traditional settings can fail to be equally sensitive when technology is involved," she said, "as when someone who would never open a sealed envelope addressed to another person enters a secured Web site." (New York Times 14 Aug 2002)

Category 17.1 *Penetration*

2002-08-23 **penetration criminal hackers stupidity legal liability unauthorized access computer fraud abuse investigation**

NewsScan

SECURITY FIRM SEEKS ATTENTION, GETS MORE THAN IT HOPED FOR
ForensicTec Solutions, a new computer security company in San Diego, sought publicity by bragging to the Washington Post that it had used free software to break into Army, Navy and NASA computers to demonstrate their security vulnerabilities. Big mistake, because when the FBI learned of the intrusions it raided the firm's offices. Mark Rasch, the Justice Department's former top computer crimes prosecutor, explained: "Just because you can break into Army computers doesn't mean you either should do it, have a right to do it, or can avoid criminal liability for doing it. They thought they were doing a public service. What they did, at best, was exercise a monumental lack of judgment." (AP/Washinton Post 22 Aug 2002)

Category 17.1 *Penetration*

2003-02-19 **penetration data theft fraud credit card**

NewsScan

VANDALS BREAK INTO SYSTEM HOLDING MILLIONS OF CREDIT CARD NUMBERS
A third-party processor of Visa and MasterCard credit card accounts was invaded by network vandals, but Visa and MasterCard executives say that none of the credit information was used for fraudulent purposes. In any event, no customer will be liable for any charges that might fraudulently be made to their accounts. A statement from Visa says that its fraud team "immediately notified all affected card-issuing financial institutions and is working with the third-party payment card processor to protect against the threat of a future intrusion. This is not something regional, it was throughout the nation and could be any bank." (Reuters/CNet News 18 Feb 2003)
http://news.com.com/2102-1017-984842.html

Category 17.1 *Penetration*

2003-02-24 **criminal hackers hacking America Online AOL customer database private personal sensitive information disclosed**

NIPC/DHS

February 21, Wired — Hackers compromise security at AOL.

Hackers have compromised security at America Online, potentially exposing the personal information of AOL's 35 million users. The most recent exploit, launched last week, gave a hacker full access to Merlin, AOL's latest customer database application. Merlin, which runs only on AOL's internal network, requires a user ID, two passwords and a SecurID code; hackers obtained all of these by spamming the AOL employee database with phony security updates, through online password trades, or by "social engineering" attacks over AOL's Instant Messenger (AIM) or the telephone. Another hole has allowed hackers to steal AIM screen names, even those of AOL staff members and executives. Most at risk are screen names that hackers covet, like Graffiti, or single-word names like Steve. While many of these hacks utilize programming bugs, most hackers are finding it far easier and quicker to get access or information simply by calling the company on the phone. These social engineering tactics involve calling AOL customer support centers and simply asking to have a given user's password reset. Logging in with the new password gives the intruder full access to the account.

Category 17.1 *Penetration*

2003-03-07 **criminal hacker hacking penetration theft sensitive private data university students Austin**

NIPC/DHS

March 06, American Statesman — Hackers steal vital data about university students and staff.

Computer hackers have obtained the names, Social Security numbers, and e-mail addresses of about 59,000 current and former students, faculty members and staff at the University of Texas at Austin in one of the largest cases of potential identity theft ever reported. Authorities do not know whether the information has been put to illegal uses such as obtaining credit cards or withdrawing money from financial accounts. Law enforcement officials were expected to obtain and execute search warrants late Wednesday in Austin and Houston at homes where computers are thought to have been used in the cyberspace break-in. UT officials said the computer breach could easily have been prevented with basic precautions, adding that the incident will prompt them to redouble security measures and to accelerate a plan to phase out most uses of Social Security numbers on campus. The university has set up a Web site - www.utexas.edu/datatheft - where it plans to post information. A telephone hot line will also be established, possibly staffed round the clock seven days a week, said Don Hale, vice president for public affairs. The university has reported the theft to the FBI, the Austin Police Department, the Travis County district attorney's office and other authorities.

Category 17.1 *Penetration*

2003-03-18 **hacking penetration theft conviction University Texas Austin sensitive private information**

NIPC/DHS

March 15, Washington Post — Student charged with hacking at U-Texas.

Federal prosecutors charged a University of Texas student Friday with breaking into a school database and stealing more than 55,000 student, faculty and staff names and Social Security numbers in one of the nation's biggest cases of data theft involving a university. Christopher Andrew Phillips, 20, a junior who studies natural sciences, turned himself in at the U.S. Secret Service office in Austin. He was charged with unauthorized access to a protected computer and using false identification with intent to commit a federal offense. Authorities had announced the cyber-theft last week. There is no evidence that Phillips disseminated or used the information, officials said. Phillips was released without bail and will have "limited access to computers," Johnny Sutton, U.S. attorney for western Texas, said at a news conference. If convicted, Phillips faces as many as five years in prison and a $500,000 fine, Sutton said.

Category 17.1 *Penetration*

2003-03-19 **hacking compromise Army Web server Windows 2000 vulnerability exploit Microsoft CERT CC**

NIPC/DHS

March 18, Federal Computer Week — Army Web server hacked.

A hacker last week exploited a previously unknown vulnerability in Microsoft Corp.'s Windows 2000 operating system to gain control of an Army Web server. Russ Cooper of security services company TruSecure Corp. said that on March 10 the hacker used an attack code to operate the Army system as if he or she had the highest security clearance and therefore was able to gain complete control of the system. The Army identified the problem after performing a network scan and finding data output from a port on one of its internal servers to an "unspecified region," he said. Both Microsoft and Carnegie Mellon University's CERT Coordination Center issued security warnings about the "buffer overflow" vulnerability and Microsoft has developed a patch, available on the Microsoft Web site, to fix it. The vulnerability affects systems running Microsoft Windows 2000 with Internet Information Server (IIS) 5.0 enabled and the code exploits an unchecked buffer in the WebDAV protocol. Exactly which Army computer was attacked, the sensitivity of the data contained on the system, and the attacker's intentions are still unknown. Compounding the surprising nature of an attack on a Defense Department system is the fact that this was a previously unknown vulnerability, or "zero-day exploit," which are extremely rare in the computer security arena. Vendors often issue patches before hackers have infiltrated a system.

Category 17.1 *Penetration*

2003-03-24 **criminal hackers hacking penetration National Security Agency NSA US**

NIPC/DHS

March 20, SecurityFocus — Hackers claim NSA breach.

Hackers claim to have compromised a computer at the National Security Agency (NSA). However, instead of obtaining a cache of highly-classified documents about the NSA's global surveillance work, the purported hackers mostly found biographies of agency personnel, and a handful of routine, correspondences between NSA spokespersons and media outlets. Journalist and NSA expert James Bamford says the apparent breach probably isn't a threat to national security. "I certainly don't think that it's acceptable that even unclassified computers can be hacked into there, but it doesn't sound like they've gotten beyond the non-classified computers in public affairs," said Bamford. An e-mail message sent to the hackers' address in Switzerland was not immediately answered Thursday. The group signed their message "Nescafé Open Up", the slogan of an ad campaign for flavored instant-coffee. The hackers' motives are unknown at this time.

Category 17.1 *Penetration*

2003-04-02 **hacking criminal hacker penetration theft sensitive private information credit card social security**

NIPC/DHS

March 28, The Atlanta Journal-Constitution — Hackers strike Georgia Tech computer, gain credit card data.

Computer hackers invaded a computer at Georgia Tech and copied names, addresses and — in some cases — credit card information for 57,000 patrons of the Ferst Center for the Arts in Atlanta. Tech said the database held credit card records for about two-thirds of the 57,000 people. The hackers had access to the computer between February 4 and March 14, when the attack was discovered. There's no evidence any credit card numbers have been used by hackers. Tech sent letters to patrons this week warning of "a potentially serious security breach." Tech's computer security experts discovered the attack through internal monitoring, said Bob Harty, a Tech spokesman.

Category 17.1 *Penetration*

2003-04-09 **criminal hacking Russia hacker hospital systems Al-Jazeera Trojan access**

NIPC/DHS

April 07, Associated Press — Ely hospital hacker traced to former Soviet Union.

A hacker who invaded the computer system at William Bee Ririe Hospital in Ely, Nevada, has been traced to the former Soviet Union, authorities said. The FBI said the hacker used the Web site of Al-Jazeera, the Arab news network, as a conduit to the hospital. Officials at the hospital said patient records are safe, but added that the cyber intruder may have accessed employee Social Security and bank information. Jim Crosley, information technology manager for the Ely hospital, detected the Ely break-in on March 20. He said the system seemed to be protected from attacks, but the FBI lab's analysis of the hospital's hard drives showed a game program, "Blaster Ball," contained a Trojan horse, a hidden code that acted as a beacon and let hackers into the hospital's system. "Two employees admitted downloading the game from the Internet and installing it at a work station," Crosley said. "The Trojan horse reported back to the hackers, and the system was compromised."

Category 17.1 *Penetration*

2003-05-28 **student break-in systems high school santa cruz California internet service parents credit card information grades e-mail**

NIPC/DHS

May 28, Santa Cruz Sentinel — Hackers threaten confidential student records.

Some Santa Cruz County, CA schools and many nationwide use online systems that allow parents to monitor their children's assignments, attendance and marks over the Internet. However, the expulsion of two students who allegedly hacked into the computer system of the county's San Lorenzo Valley High School exposes the the vulnerability of online record systems. Sheriff's investigators allege that in November 2000 and January 2001, the students broke into the school's computer system using stolen passwords. They allegedly changed grades, read staff e-mail and stole credit card information. Students also allegedly carried out "denial of service" attacks on the school's computer system in August and September 2002.

Category 17.1 *Penetration*

2003-07-30 **Kentucky government computers french hackers user password files computer security Ed Hatchett**

NIPC/DHS

July 30, Associated Press — French hackers break into Kentucky government computers.

State investigators in Kentucky believe French hackers have been using the Transportation Cabinet's computers to store pirated computer files including newly released movies and video games. State auditor Ed Hatchett said he believed the hackers entered the system on April 2, and have been using it since. Because they also gained access to the system's administrator and user password files, they could be able to manipulate any state file on the infected network, Hatchett said. Based on the Internet addresses investigators were able to trace, they suspect the hackers were from France, said B.J. Bellamy, chief information for the auditor's office. Other Internet addresses they found were based in Canada and Croatia, he said. Transportation Cabinet inspector General Bobby Russell said the department had already been working to tighten its computer security system before the auditor's findings.

Category 17.1 *Penetration*

2003-08-04 **Telecast Fiber Systems hacker worker computer deleting valuable files John Corrado remote location modem**

NIPC/DHS

August 04, Boston Business Journal — Former Telecast Fiber worker pleads guilty to hacking.

A former employee of Telecast Fiber Systems Inc. in Worcester, MA, pleaded guilty Friday, August 1, in federal court to breaking into the company's computer system and deleting valuable files, according to the U.S. Attorney's office. John Corrado, 35, agreed to pay $10,360, the estimated financial loss suffered by the company. His formal sentencing is scheduled for October 7 where he faces a maximum penalty of one year imprisonment and a fine of $100,000. The U.S. Attorney's office says that in July 1999, about one month after Corrado had stopped working for the company, he accessed the company's network server using a modem from a remote location. The files he deleted included those used for research and development as well as those used by sales reps to demonstrate company products.

Category 17.1 *Penetration*

2003-08-07 **hacking hacker attack 2000 computers Stanford University Cedric Bennett infected machines campus**

NIPC/DHS

August 07, The Mercury News — Hacker attack damages 2,000 computers at Stanford.

Officials at Stanford University scrambled Thursday, August 7, to repair the damage from a hacking attack that has infected thousands of campus computers. Cedric Bennett, Stanford's director of information security services, said unknown hackers had exploited a newly discovered vulnerability in Microsoft's Windows operating system. About 10 percent of Stanford's 20,000 desktop computers that run Windows were affected. The attack placed a mysterious bit of computer coding on each of the infected machines, which Bennett said the hackers could later activate. University technicians have disconnected the infected machines, used by students, faculty and staff, from the campus network.

Category 17.1 *Penetration*

2003-08-07 **Acxiom customer information hacker private files clients credit card companies identity theft computer**

NIPC/DHS

August 07, Associated Press — Hacker gets Acxiom customer information.

A computer hacker gained access to private files at Acxiom Corp., one of the world's largest consumer database companies, and was able to download sensitive information about some customers of the company's clients, the company said Thursday, August 7. Jennifer Barrett, the company's chief privacy officer, said about 10 percent of the company's customers were affected and that, "it would include some of our larger customers." Acxiom's Website says the company serves 14 of the top 15 credit card companies, seven of the top 10 auto manufacturers and five of the top six retail banks. The individual in police custody is a former employee of one of Acxiom's clients and gained access by hacking encrypted passwords from clients who access the server. Barrett said much of the information taken from the server was encrypted and that the risk of identity theft is slim.

Category 17.1 *Penetration*

2003-08-07 **e-vote hacker break security web server largest electronic voting sensitive information**

NIPC/DHS

August 07, Wired — New security woes for e-vote firm.

A hacker has come forward with evidence that he broke the security of a private Web server operated by Diebold Election Systems and made off last spring with the company's internal discussion-list archives, a software bug database and software. The company is one of the largest electronic voting systems vendors, with more than 33,000 machines in service around the country. Director of Communications John Kristoff said the stolen files contained "sensitive" information, but he said Diebold is confident that the company's electronic voting system software has not been tampered with.

[MK asks, "Why? Why is is confident?]

Category 17.1 *Penetration*

2003-08-21 **Navy purchase cards hackers Department Defense DoD cancelled accounts Citibank gained access Criminal Investigate**

NIPC/DHS

August 21, Government Computer News — Hackers compromise Navy purchase cards.

Hackers recently broke into a Navy system and gained access to 13,000 Navy purchase cards, according to Department of Defense (DoD) officials who are investigating the incident. The DoD Purchase Card Program Management Office has issued a release stating that the Navy has cancelled all of its purchase card accounts-about 22,000-to minimize the number of unauthorized purchases, and is working closely with the issuing company, Citibank. "Emergency purchases are being handled on a case-by-case basis to fully support Navy requirements," according to the statement. A DoD team is working to determine how hackers gained access to the system and what needs to be done to fix the breach. A Defense Criminal Investigative team is also pursuing the investigation.

Category 17.1 *Penetration*

2003-11-12 **criminal hacker hacking penetration Australian Defense top-secret data information file**

NIPC/DHS

November 10, Australian Associated Press — Hackers reach Australian Defense files.

Hackers have reportedly accessed top-secret files inside the Australian Department of Defense. "There have been three incidents in which an external security breach has led to unauthorized access to computer systems," Senator Hill had told an inquiry into computer security in the public service. According to the minister, the Defense Department also reported 13 cases since 2000 of its own staff trying to hack into computer systems without authorization. A review of electronic security inside commonwealth agencies has reportedly uncovered a culture of theft and lax security inside the public service. The inquiry comes amid a series of thefts of computers containing classified information from a customs office at Sydney Airport and the Transport Department in Canberra. Submissions by the major departments to the Joint Committee of Public Accounts and Audit has found that more than 1600 computers have vanished since 1998. Senator Hill said three computers stolen in the past two years contained information classified as "secret", but they had been recovered and the risk to national security had been assessed as low, he told the inquiry in a memo.

Category 17.1 *Penetration*

2003-12-29 **election break-in computers intruder indentified VoteHere Inc. Bellevue**

NewsScan

BREAKING-IN: NOT AN ACCEPTABLE DEBATING TACTIC
VoteHere Inc., a Bellevue, Washington company that markets a security technology for electronic voting, says that U.S. authorities are investigating a break-in of its computers months ago, when someone roamed its internal computer network. VoteHere chief executive Jim Adler says: "We caught the intruder, identified him by name. We know where he lives. We think this is political. There have been break-ins around election companies over the last several months, and we think this is related. I have no problem debating the merits of electronic voting with anyone, but breaking and entering is not an appropriate forum for technology debate." (AP/Washington Post 29 Dec 2003)

Category 17.1 *Penetration*

2004-03-17 **hacking attack penetration announcement California disclosure law**

NIPC/DHS

March 12, Security Focus — Hosting company reveals hacks, citing disclosure law.

Citing California's security breach disclosure law, Texas-based Allegiance Telecom notified 4,000 Web hosting customers this week of a March 3 computer intrusion that exposed their usernames and passwords. The law, called SB 1386, took effect July 1, 2003. It obligates companies doing business in California to warn their customers in "the most expedient time possible" about any security breach that exposes certain types of information: specifically, customers' names in association with their social security number, drivers license number, or a credit card or bank account number. Attorneys have warned that SB 1386 applies to e-commerce companies nationwide if they house information on residents of California. The intrusion did not directly expose information covered by the law, according to the company. Instead, the intruder pilfered thousands of passwords protecting customers' Web hosting accounts. Because many of those accounts are held by e-commerce companies, Allegiance issued the notice anyway, informing clients that SB 1386 may now oblige them to pass on the warning to their California customers if they accept personally identifiable information.

Category 17.1 *Penetration*

2004-03-25 **security breach source code penetration Gnome project Linux open-source operating system desktop**

NIPC/DHS

March 23, CNET News.com — Server breach likely to delay Gnome.

The Gnome Project administrators said Tuesday, March 23, that its servers have apparently been breached, potentially delaying the latest release of its desktop system for Linux. Gnome provides one of the two major desktop systems used on computers running the Linux operating system. "We are investigating further and will provide updates as we know more," Owen Taylor, a member of the Gnome system administration team said. The message also stated that the administrators believed the source code repository, which contains the current development work on Gnome software, was unaffected by the breach. The next version of the software, Gnome 2.6, will likely be delayed a few days while the project members investigate the breach. The software was scheduled to be released on Wednesday.

Category 17.1 *Penetration*

2004-04-13 **network computer attack vandals TeraGrid Unix security incident National Science Foundation NSF**

NewsScan

UNIVERSITY SUPERCOMPUTERS ATTACKED BY VANDALS

Network vandals have infiltrated supercomputers at as many as 20 colleges, universities and research institutions in recent weeks, disrupting the TeraGrid, a network of computers funded by the National Science Foundation and used in support of such scientific projects as weather forecasting and genome sequencing. The vandals have not been identified. None of the systems was permanently damaged, but the intruders gained the ability to control the various networks for short periods of time, prompting TruSecure security expert Russ Cooper to warn, "This could be a wake-up call to what should be very, very secure computing environments, because these machines should never have been compromised." The attacks were made against Unix machines. Stanford University computer security officer Tina Bird comments: "This incident is definitely giving us an opportunity to reevaluate the maintenance and protection we provide to our Unix systems. When you're completely focused on widespread attacks on Windows systems, it's certainly startling." (Washington Post 13 Apr 2004)

Category 17.1 *Penetration*

2004-09-30 **US government govt. Department of Energy DoE cybersecurity penetration hacking cracking report**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/27489−1.html

September 30, Government Computer News — DOE cybersecurity penetrated.

Weaknesses in the Department of Energy (DOE) cybersecurity allowed hackers to penetrate its systems 199 times last year, affecting 3,531 systems, the DOE's inspector general (IG) said. DOE continues to have difficulty finding, tracking and fixing previously reported cybersecurity weaknesses quickly, the IG said in a report, "The Department's Unclassified Cyber Security Program—2004."

Category 17.1 *Penetration*

2004-10-21 **Purdue University computer system penetration hack password changes information disclosure**

DHS IAIP Daily; http://www.indystar.com/articles/7/188156−5277−102.html

October 21, Associated Press — Purdue computer system hacked.

Someone gained unauthorized access to Purdue University's computers, prompting school officials to urge all students, staff and faculty to change their passwords. "We have confirmed that some computer passwords have been obtained by unauthorized users accessing a number of computer systems," said Scott Ksander of Purdue's information technology office. The school has not been able to determine whether personal information was copied by the hacker.

Category 17.1 *Penetration*

2005-01-11 **hacker penetration T-Mobile wireless product manufacturer customer private information disclosure**

DHS IAIP Daily; http://www.securityfocus.com/news/10271

HACKER PENETRATES T-MOBILE SYSTEMS.

A sophisticated computer hacker had access to servers at wireless giant T-Mobile for at least a year. Twenty-one year-old Nicolas Jacobsen was charged with the intrusions last October, after a Secret Service informant helped investigators link him to sensitive agency documents that were circulating in underground IRC chat rooms. The informant also produced evidence that Jacobsen was behind an offer to provide T-Mobile customers' personal information to identity thieves through an Internet bulletin board, according to court records. Jacobsen could access information on any of the Bellevue, Washington-based company's 16.3 million customers, including many customers' Social Security numbers and dates of birth, according to government filings in the case. He could also obtain voicemail PINs, and the passwords providing customers with Web access to their T-Mobile e-mail accounts. Jacobsen faces two felony counts of computer intrusion and unauthorized impairment of a protected computer in a federal case in Los Angeles, currently set for a February 14th status conference.

Category 17.1 *Penetration*

2005-01-12 **penetration George Mason GMU college grades confidential data**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A5188-2005Jan12.html

SECURITY I: VANDALISM OF COLLEGE NETWORKS

Early this month an intruder penetrated a central computer at George Mason University and attempted to access GMU's 130 other servers -- which hold such information as grades, financial aid, and payrolls. In the past two years, similar attacks have occurred at the universities of Georgia, Texas, Missouri, and California. To resist such attacks, some schools are beginning to use software that scans individual computers before they are allowed to connect to campus networks, and other institutions are setting up multiple smaller networks that house sensitive data, keeping them separate from the main networks. (Washington Post 12 Jan 2005)

Category 17.1 *Penetration*

2005-01-12 **T-Mobile data theft Secret Service Jacobsen e-mail files customers vandal penetration breakin trespass criminal hacker**

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/10633193.htm

SECURITY II: ATTACK ON T-MOBILE

A network vandal broke into the network of wireless carrier T-Mobile over a seven month period and read e-mails and personal computer files of hundreds of customers -- including those of the Secret Service agent investigating the hacker himself. The online activities of the vandal, 21-year-old computer engineer Nicolas Lee Jacobsen of Santa Ana, were traced to a hotel where he was staying in Williamsport, N.Y. Although Jacobsen was able to view the names and Social Security numbers of 400 customers (all of whom were notified in writing about the break-in), customer credit card numbers and other financial information never were revealed, and T-Mobile says it "immediately took steps that prevented any further access to this system." (AP/12 Jan 2005)

Category 17.1 *Penetration*

2005-02-04 **Federal Bureau of Investigation FBI unclassified e-mail system shut down penetration hacking compromise fear**

DHS IAIP Daily;
http://story.news.yahoo.com/news?tmpl=story&cid=528&ncid=528&e=3&u=/ap/20050204/ap_on_hi_te/fbi_computers

FBI SHUTS DOWN UNCLASSIFIED E-MAIL SYSTEM.

The FBI said Friday, February 4, it has shut down an e-mail system that it uses to communicate with the public because of a possible security breach. The bureau is investigating whether someone hacked into the www.fbi.gov e-mail system, which is run by a private company, officials said. "We use these accounts to communicate with you folks, view Internet sites, and conduct other non-sensitive bureau business such as sending out press releases," Special Agent Steve Lazarus, the FBI's media coordinator in Atlanta, said in an e-mail describing the problem. The FBI computer system that is used for case files, classified and sensitive information, and internal communications is unaffected, Lazarus said.

Category 17.1 *Penetration*

2005-02-15 **data theft confidentiality control identity fraud consumer records social engineering Social Security Numbers SSN credit reports**

RISKS; http://news.com.com/2100-1029-5577122.html 23 72

SCAMMERS ACCESS CHOICEPOINT DATA ON 35,000

ChoicePoint confirmed on 15 Feb that criminals recently accessed its database of consumer records, potentially viewing the personal data of about 35,000 Californians and resulting in at least one case of identity fraud. The unidentified individuals posed as legitimate businesspeople in order to [breach]* its defenses. Chuck Jones, a company spokesman, said that roughly 50 fraudulent accounts were set up by the schemers, through which they could view the data of California residents.

News of the crime first surfaced when ChoicePoint sent an e-mail to individuals potentially affected by the attack last week. Among the data available through the company's services, and possibly accessed by the criminals, are consumers' names, addresses, Social Security numbers and credit reports.

(Matt Himes in news.com , relayed via RISKS by Monty Solomon)

* Prof Kabay notes: The original article used "breech." DON'T DO THAT. If you mean a breakin, the word is "breach."

Category 17.1 *Penetration*

2005-03-09 **confidentiality hacking cracking security failure data leakage punishment student applications ethics rejection consequences questions problems**

RISKS; http://tinyurl.com/6k3zs; http://tinyurl.com/du52h 23 78

UNIVERSITIES REJECT STUDENTS WHO CHECKED THEIR ADMISSION STATUS ONLINE

[In early March 2005, some students tried to check the status of their applications to various graduate schools by using information published in an online forum on how to find their records. Several schools responded by rejecting those candidates, provoking some controversy about whether the students had done anything wrong in the first place and whether the response was draconian. Mony Solomon summarized the university response and Peter Neumann summarized some of the controvery in the following RISKS posting.]

Sloan School of Management has joined Carnegie-Mellon and Harvard in rejecting applications from prospective students who hacked into a website to learn whether they had been admitted before they were formally notified. 32 MIT applicants reportedly took a peek, along with 1 at CMU, 119 at Harvard, and 41 at Stanford. The Web site is run by ApplyYourself, and also used by other business schools. Its access was compromised by a posting on a BusinessWeek Online forum. [PGN-ed from Robert Weisman, *The Boston Globe*, 8 and 9 Mar 2005]

[Dave Farber's IP list had several responses. Rejected applicants considered their treatment excessive. One candidate saw only a blank page at ApplyYourself, but was rejected for having accessed the site. Dave Lesher wrote

> What's the B-schools' culpability in contracting out a process to a company with inadequate security? [Presumably] the schools demanded SSN's and other financial data from the applicants. Was there informed consent by the applicants to have their data shared with, in effect, a data broker? Could they apply WITHOUT so agreeing?

Joe Hall wrote

> What strikes me is how constructing a URL that is available to students without any further authentication or protection is considered "hacking". That's inevitably diluting any geek cred. held by any of us who are even crappy hackers!

Joe also noted Ed Felten's post on this subject at http://www.freedom-to-tinker.com/archives/000780.html

PGN wonders what if a competing candidate had masqueraded as other candidates to see if others had been accepted, and thereby wound up getting them all rejected! Could that be a suitable defense for the rejected students? PGN]

Category 17.1 *Penetration*

2005-03-17 **Boston College alumni database Social Security Numbers information disclosure virus data leakage**

EDUPAGE; http://news.zdnet.com/2100-1009_22-5623084.html

VIRUS INFECTS BOSTON COLLEGE ALUMNI DATABASE

A computer at Boston College with access to an alumni database has been found to be infected with a virus that may have exposed personal information on more than 100,000 individuals. According to officials at the college, the computer was operated not by the college but by a third-party IT service, which officials declined to name. Although no evidence has so far surfaced that any of the information in the database was in fact accessed by hackers, officials decided to notify anyone who might have been affected. Jack Dunn, spokesperson for Boston College, said, "We thought it was necessary to send out the precautionary advisory to alert the alumni and to offer them steps that they could take to ensure their privacy." Dunn also noted that Boston College will hereafter delete Social Security numbers from its records, despite their usefulness in maintaining accurate records. Social Security numbers have lately been highlighted as one of the pieces of personal information that pose the greatest risk for identity theft. Members of Congress have recently proposed strict restrictions for how and when Social Security numbers can be gathered and sold. ZDNet, 17 March 2005

Category 17.1 *Penetration*

2005-03-18 **penetration hacking Dartmouth admissions Website penalize applicants**

EDUPAGE; http://www.post-gazette.com/pg/05077/473361.stm

DARTMOUTH DECIDES TO PENALIZE, BUT NOT ELIMINATE, HACKERS

Applicants to the Tuck School of Business at Dartmouth College who used a hacker's tips to try to access admissions records were not automatically disqualified, though their actions were considered by school officials in their admissions decisions. The decision to consider applications of those involved in the hacking was made after consultations with faculty and staff and with the appliants themselves. Unlike officials at Harvard University, Duke University, MIT, and Carnegie Mellon University, administrators at Dartmouth decided that the hacking, while serious, "did not reach the level that would necessarily bar a person from being a valued member of the Tuck community," according to Paul Danos, dean of the school. Attempting to access restricted records was viewed by the school as "a very important negative factor" in considering the applications, but ultimately the school's decision did not rest on that single factor. Of the 17 applicants involved, some were admitted, and those who enroll will be monitored and counseled. The incident will also become a part of their files. Pittsburgh Post-Gazette, 18 March 2005

Category 17.1 *Penetration*

2005-03-18 **criminal hackers Web site vulnerability exploit consequences university admissions ethics**

http://www.post-gazette.com/pg/05077/473361.stm

APPLY YOURSELF TO BREAKING INTO … APPLYYOURSELF, INC.

Criminal hackers posted instructions on March 2, 2005 on how to break into the ApplyYourself Inc. database online, a repository of applications used by many universities to track applicants.

About 150 candidates did break into the database and were identified because they looked at their own applications. Most of the six top business schools involved in the breakin rejected the applicants outright. However, Dartmouth College's Tuck School of Business decided to count the breakins as a factor detracting from an applicant's suitability but not absolutely barring their admission. Stanford University's business school had not yet decided on a firm policy by mid-March. Ethicists pointed out serious problems with the laissez-faire attitude of these schools.

Category 17.1 *Penetration*

2005-03-19 **Social Security Numbers SSN data loss theft compromise criminal hackers**

RISKS; http://news.zdnet.com/2100-1009_22-5623084.html 23 80

BOSTON COLLEGE LOSES THOUSANDS OF SSNs

[Same case as one in VIRUS INFECTS BOSTON COLLEGE ALUMNI DATABASE entry]

Geoff Kuenning summarized yet another after-the-fact response to a breach of confidentiality:

Hackers have invaded a Boston College database of alumni, compromising data on up to 100,000 people. The data includes Social Security Numbers. In a choice quote, Jack Dunn of BC ``noted that Boston College will hereafter delete Social Security numbers from its records, despite their usefulness in maintaining accurate records."

Question: If every organization that currently stores SSNs waits until *after* they are hacked before they decide that maybe it's not smart to expose sensitive data, how many Americans will be left with uncompromised SSNs?

Liability laws are desperately needed.

Category 17.1 *Penetration*

2005-04-24 **criminal hacker data theft penetration**

RISKS; http://www.post-gazette.com/pg/05111/491836.stm 23 85

HACKER(S) BROKE INTO CMU COMPUTERS

Monty Solomon summarized another attack on university data:

A hacker [or hackers] who tapped into business school computers at Carnegie Mellon University may have compromised sensitive personal data belonging to 5,000 to 6,000 graduate students, staff, alumni and others. The breach confirmed by officials in the Tepper School of Business is the latest in a recent string of campus computer break-ins nationally and the second since early March affecting Tepper. There is no evidence that any data, including Social Security and credit card numbers, have been misused, officials said. But they have begun sending e-mails and letters alerting those affected. They include graduate students and graduate degree alumni from 1997 to 2004, master's of business administration applicants from September 2002 through May 2004, doctoral applicants from 2003 to this year, and participants in a conference that was being arranged by the school's staff.…

Bob Heuman commented:

Another case of not knowing how long the exposure existed and therefore how much exposure the personal information really had. Once again we have Social Security Numbers, credit card data, etc. exposed for an indeterminate amount of time. I have gone to the university's own web site and the Tepper School web site and neither has any mention of this report as of the time I checked, which is Apr 21 at 4:45PM EDT.

Category 17.1 *Penetration*

2005-05-11 **computer security attack FBI thwart Cisco routers government university computers NASA NCSA San Diego Supercomputer Center Sweden teenager**

EDUPAGE; http://online.wsj.com/article/0,,SB111569768679229042,00.html

FBI THWARTED COMPUTER ATTACKS

An investigation into the theft of part of the operating system software for Cisco routers has prevented network attacks on government and university computers, according to the FBI. In May 2004, a hacker was able to access Cisco's software and reportedly used that information to compromise networks at several military installations and at the National Aeronautics and Space Administration. Computers at the Argonne National Laboratory, the National Center for Supercomputing Applications, and the San Diego Supercomputer Center were also compromised. The FBI said that law enforcement action has apparently ended the break-ins. As part of the investigation, authorities in Sweden detained a teenager thought to be involved in the malicious activity, though it remains unclear whether U.S. authorities will be able to prosecute that person.
Wall Street Journal, 11 May 2005 (sub. req'd)

Category 17.1 *Penetration*

2005-05-26 **hackers hacking penetration Stanford University Career Development Center CDC personal information disclosure Social Security Numbers**

EDUPAGE; http://software.silicon.com/security/0,39024655,39130758,00.htm

HACKERS HIT STANFORD

Officials at Stanford University and the FBI are investigating a computer breach at the university's Career Development Center (CDC) earlier this month that may have exposed personal information on as many as 10,000 individuals. Most of those affected are students, though a small number are recruiters who had registered with the CDC. Information that might have been improperly accessed includes names, Social Security numbers, financial information, and, in some cases, credit card numbers. The university is notifying those possibly affected by the breach, in compliance with the 2003 Security Breach Information Act. That law requires organizations to inform California residents any time their personal information might have been accessed without authorization. Silicon.com, 26 May 2005

Category 17.1 *Penetration*

2005-06-17 **data theft penetration criminal hacker credit burea**

RISKS; http://www.cbc.ca/story/business/national/2005/06/17/equifax-050617.html 23 91

EQUIFAX (CANADA) HACKED

A computer hacker has accessed the files of about 600 consumers at Equifax Canada, one of Canada's major credit bureaus. Most of the files are for consumers from British Columbia. Equifax Canada uses data provided by banks to compile credit records on Canadian consumers. Those records include personal information such as social insurance numbers, bank account numbers and up to six years of credit and banking history … Equifax said all affected customers in this latest breach have been contacted. The RCMP is investigating.

[Abstract by R. S. "Bob" Heuman]

Category 17.1 *Penetration*

2005-06-22 **customer pharmacy medical data privacy controls penetration leakage compromise Web access identification authentication I&A response**

RISKS; http://www.pbn.com/contentmgr/showdetails.php/id/115431 23 92

CVS FIXES PRIVACY HOLE

The CVS Corp.has cut off Web access to ExtraCare card holders' detailed purchase information after a consumer group showed reporters how easily an intruder could log into the system and find out, say, how many condoms or enema kits someone's bought. CVS has issued about 50 million of the loyalty cards, which allow the drugstore chain to track each customer's purchases and, in exchange, provide a 2-percent rebate on those purchases, along with customized coupons. To log into your account on CVS.com, all you need is the card number, your ZIP code, and the first three letters of your surname. Even now, anyone with that information can easily find out the card holder's home address, phone number, and total purchases each quarter. But until last week, the Web site also allowed customers to request a detailed purchase report to be e-mailed to them -- to any address they put in….

[Excerpt from article by Marion Davis]

Category 17.1 *Penetration*

2005-07-15 **data theft confidentiality credit card hack**

Crypto-Gram

CARDSYSTEMS SOLUTIONS HACKED -- 40M PEOPLE AFFECTED

Bruce Schneier wrote, "The personal information of over 40 million people has been hacked. The hack occurred at CardSystems Solutions, a company that processes credit card transactions. The details are still unclear. The New York Times reports that "data from roughly 200,000 accounts from MasterCard, Visa and other card issuers are known to have been stolen in the breach," although 40 million were vulnerable. The theft was an intentional malicious computer hacking activity: the first in all these recent personal-information breaches, I think. The rest were accidental -- backup tapes gone walkabout, for example -- or social engineering hacks. Someone was after this data, which implies that's more likely to result in fraud than those peripatetic backup tapes.

CardSystems says that they found the problem, while MasterCard maintains that they did; the New York Times agrees with MasterCard. Microsoft software may be to blame. And in a weird twist, CardSystems admitted they weren't supposed to keep the data in the first place."

Category 17.1 *Penetration*

2005-07-22 **hacker hacking penetration perimeter breach University of Colorado information disclosure Social Security Numbers**

EDUPAGE; http://www.thedenverchannel.com/technology/4757407/detail.html

CU COMPUTERS HACKED

Officials at the University of Colorado said hackers gained access to two servers at the university, possibly exposing personal information on nearly 43,000 students and employees of the institution. One server, at the College of Architecture, contained data on 900 individuals; the other, at the university's health center, included information for another 42,000 people. The servers included names, Social Security numbers, addresses, and dates of birth, according to the university, but neither included credit card information. Still, university officials are advising those affected to monitor their credit reports for suspicious activity, and the university has set up a Web site and a hot line to answer questions. Investigators looking into the situation said that one hacker came through a server in France, while the other came through a server in Eastern Europe. University officials have no information so far that any of the personal data on the servers has been misused. The Denver Channel, 22 July 2005

Category 17.1 *Penetration*

2005-07-25 **Hackers spyware Website hosting ISPs malicious worms viruses spyware hosting**

DHS IAIP Daily; http://www.techweb.com/wire/security/166402258

HACKERS SPREADING SPYWARE FROM FREE PERSONAL WEBSITES

Attackers are using free personal Web hosting sites provided by nationally- and internationally-known ISPs to store their malicious code, and to infect users with worms, viruses, and spyware, a security firm said Monday, July 25. Websense, a San Diego, California-based Web security and content filtering vendor, has detected a big jump in the use of personal hosting sites, said Dan Hubbard, the company's senior director of security and technology research. "Attackers don't have to go to the trouble to find a compromised machine, search for one with a vulnerability they can exploit to turn into a zombie," said Hubbard. "Plus, they're reliable. Since they're offered up by national and international Internet service providers, they're built on a lot of infrastructure. Third, they often offer quite a bit of storage space, in some cases up to 500MB." The problem is that too few free hosting services offer even the most basic security tools, Hubbard said. None of the services found hosting malicious sites use a graphics-based question to make sure that a human, not a bot, registers for the service, he said.

Category 17.1 *Penetration*

2005-08-03 **hacker hacking penetration perimeter breach University of Colorado information disclosure Social Security Numbers**

EDUPAGE; http://www.denverpost.com/news/ci_2909173

CU SUFFERS ANOTHER HACK

Hackers broke into a server at the University of Colorado (CU), marking the third security breach in the past six weeks. The latest attack targeted servers that held information for the school's ID card, known as the Buff OneCard. Those servers included names, Social Security numbers, and photographs but not financial information. Potentially exposed in the attack is personal information for 29,000 students, some former students, and 7,000 staff members. Students who will be entering the university in the fall were not affected. Dan Jones, IT security coordinator, said it was not clear whether this attack was perpetrated by the same people who compromised two other servers recently. In April, CU had decided to move away from using Social Security numbers as identifiers for students, based on security problems at other institutions and the risk of identity theft. Some systems on campus, however, still use Social Security numbers to track students, according to Jones. Officials at the university said they will hire an independent auditing firm to assess the institution's security measures and will also evaluate some 26,000 computers to determine which could be placed behind a firewall. The Denver Post, 3 August 2005

Category 17.1 *Penetration*

2005-08-09 **Sonoma State University California hacker penetration personal information disclosure Social Security Numbers**

EDUPAGE; http://sfgate.com/cgi-bin/article.cgi?f=/c/a/2005/08/09/BAGLJE50C81.DTL

HACKERS HIT ANOTHER UNIVERSITY

Sonoma State University, an hour north of San Francisco, has become the latest in a growing list of universities to suffer a hacker attack that put personal information of students and staff at risk. At Sonoma State, hackers in July gained access to several computer workstations, which allowed them to access a number of other computers before university staff detected and put an end to the intrusion. In all, the hackers had access to names and Social Security numbers of nearly 62,000 students, applicants, or employees of the university between 1995 and 2002. A spokesperson for the university said the hackers did not have access to financial information and noted that there is currently no evidence that any of the information has been misused. Nevertheless, the university is required by state law to contact individuals whose personal information has been compromised, and the university is working to do just that. The university has set up a Web site with information and is advising affected individuals to contact credit-reporting agencies to be on the lookout for possible identity fraud. San Francisco Chronicle, 9 August 2005

Category 17.1 *Penetration*

2005-09-29 **hacker attack penetration University of Georgia personal sensitive information disclosure Social Security Numbers**

EDUPAGE; http://www.ajc.com/metro/content/metro/0905/29ugabreach.html

HACKER HITS UNIVERSITY OF GEORGIA

The University of Georgia has revealed that a hacker was able to access a computer system that contained personal information for employees of the College of Agricultural and Environmental Sciences as well as people who are paid from that department. Social Security numbers were in the accessed database, though no credit card information was exposed. In all, 2,400 Social Security numbers for about 1,600 people were compromised, and the university is working to contact those affected. According to Tom Jackson, spokesperson for the university, names and Social Security numbers in the database were not connected, but an experienced hacker would likely be able to correctly match them up. The university suffered another computer hack in January 2004. No arrests have been made in that incident. The Atlanta Journal-Constitution, 29 September 2005

Category 17.1 *Penetration*

2005-11-18 **hacking penetration malicious network activity Indiana University IU**

EDUPAGE;
http://www.fortwayne.com/mld/fortwayne/news/local/13202338.htm

HACKER HITS IU

Officials at Indiana University reported that a routine scan of computer systems turned up malicious software on the computer of a faculty member at the Kelley School of Business. According to James Anderson, the school's director of information technology, the software could have been used to access the personal information of about 5,300 current and former students at the university, though no reports have surfaced that the information was used illicitly. The school has notified the students who are possibly affected and encouraged them to monitor their credit reports for suspicious activity. Daniel Smith, dean of the Kelley School, said all of the institution's computers are being audited to ensure they are free of malicious software and have current antivirus and system patches installed.
Associated Press, 18 November 2005

Category 17.1 *Penetration*

2005-12-20 **data theft security breach Encase Guidance software criminal hackers financial personal data customer database law enforcement response credit card Secret Service investigation**

EDUPAGE; http://www.washingtonpost.com/wp-dyn/content/article/2005/12/19/AR2005121901525.html

HACKERS HIT SECURITY COMPANY DATABASE

Hackers gained access to the financial and personal data of 3,800 law enforcement and network security professionals when they broke into the customer database of Guidance Software in Pasadena, California. Guidance Software is a leading provider of software to diagnose hacker attacks, and its EnCase product is used by hundreds of security researchers and law enforcement agencies worldwide, including the U.S. Secret Service and FBI. The break-in took place in November and was discovered December 7. The company alerted its customers within two days after the discovery and assured them it would no longer store customer credit card data. The company is working with the Secret Service on a detailed investigation of the incident.

Category 17.1 *Penetration*

2006-01-16 **criminal hacker US Navy base California penetration arrest Spain**

DHS IAIP Daily; http://today.reuters.com/news/newsArticleSearch.aspx?storyID 23
=210818+16−Jan−2006+RTRS&srch=hacker

SPAIN ARRESTS HACKER AFTER BREACH AT U.S. NAVY BASE

Spain's Civil Guard said on Monday, January 16, they had arrested a man who hacked into a U.S. Department of Defense computer, breaching security at a U.S. naval base in California. The man was part of a group of hackers which attacked more than 100 computer systems, including one at the U.S. Navy's Point Loma base in San Diego where nuclear submarines are maintained in dry docks. U.S. security services found someone had illegally accessed the computer and subsequently traced the link to Spain. Spanish authorities pinpointed the group in the southern city of Malaga and arrested one man. Many of the group were students though all were over 18. "They did it for the challenge, there's no implication of terrorism," a Civil Guard spokesperson said, adding that the man would face unspecified charges. The Guard did not say when the arrests or the hacking took place.

Category 17.1 *Penetration*

2006-01-23 **British parliament attack WMF exploit Microsoft Windows**

DHS IAIP Daily; http://news.com.com/British+parliament+attacked+using+WMF+ex ploit/2100−7349_3−6029691.html?part=rss&tag=6029691&subj=news 23

BRITISH PARLIAMENT ATTACKED USING WMF EXPLOIT.

The British Parliament was attacked late last year by hackers who tried to exploit a recent serious Microsoft Windows flaw, security experts confirmed on Friday, January 20. MessageLabs, the e-mail-filtering provider for the UK government, said that targeted e-mails were sent to various individuals within government departments in an attempt to take control of their computers. The e-mails harbored an exploit for the Windows Meta File (WMF) vulnerability. The attack occurred over the Christmas period and came from China, said Mark Toshack, manager of antivirus operations at MessageLabs, who added that the e-mails were intercepted before they reached the government's systems. The vulnerability with the way that WMF images are handled by Windows was discovered in November 2005. In a WMF attack, exploit code is hidden within a seemingly normal image that can be spread via e-mail or instant messages. The attack was individually tailored and sent to 70 people in the government, MessageLabs said. It played on people's natural curiosity by purporting to come from a government security organization. The Trojan was hidden as an attachment called "map.wmf".

Category 17.1 *Penetration*

2006-01-30 **AMD Website forum hacker compromise malicious software infection WMF Windows vulnerability**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/hacking /story/0,10801,108195,00.html 23

HACKERS LURK IN AMD WEBSITE.

Advanced Micro Devices (AMD) Inc.'s customer support discussion forums on the forums.amd.com site have been compromised and are being used in an attempt to infect visitors with malicious software, an AMD spokesperson confirmed Monday, January 30. The problem was first reported Monday in a blog posting by Mikko Hypponen, manager of antivirus research at F-Secure Corp. in Helsinki. According to F-Secure's Hypponen, attackers are exploiting a widely reported flaw in the way the Windows operating system renders images that use the WMF (Windows Metafile) graphics format. This flaw was patched on January 5, so users who are running versions of Windows that have the latest patches installed are not at risk, he said. Attackers have figured out a way to use AMD's forums to deliver maliciously encoded WMF images to visitors, which are then used to install unauthorized software on the unpatched systems, he said. "Most of the tool bars show pop-ups, follow your search and other keyword activity, and use that to target ads to you," Hypponen said. "It's for-profit hacking. Somebody is making money from each machine that is hit by these tool bars."

Category 17.1 *Penetration*

2006-02-13 **Olympic computer network attack threat Turin winter**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/content/article/2006/02 /13/AR2006021300387.html 23

MAN THREATENS TO ATTACK OLYMPIC COMPUTERS.

A would-be hacker was being investigated by police Monday, February 13, after threatening to attack the internal computer network of the Turin, Italy, Olympics organizing committee. The man -- a technical consultant for the Turin Organizing Committee -- illicitly gained access to off-limits sections of the network, police officer Fabiola Silvestri said. "This consultant -- who is now a former consultant -- said in a very strong way that he could do certain things to the network," Turin Organizing Committee spokesperson Giuseppe Gattino said. "Nothing has happened and all the passwords have been disabled."

In a separate case, police found that a Turin antiques dealer had acquired five Internet domains that had similar names to Olympic Websites. If accessed, the domains redirected users to the dealer's Website, which also carried Olympic logos and other copyrighted material, Silvestri said. Once he had been told that what he was doing was illegal, the dealer deleted the material and redirected users from his domains to Olympic Websites, she said.

Category 17.1 Penetration

2006-02-14 **hacker break in penetration University of Arizona journalism computers**

DHS IAIP Daily; http://www.azstarnet.com/metro/115789 23

ROMANIAN HACKER BREAKS IN TO UNIVERSITY OF ARIZONA JOURNALISM COMPUTERS.

Hackers broke into the computer system of the University of Arizona journalism department, and students were unable to use the computers Monday, February 13. All of the department's Apple Macintosh computers were affected and have been logged off the server and the Internet until the problem is solved, said Jacqueline Sharkey, head of the department. No information has been lost so far, she said. It was unclear Monday how long it would take to fix the security leak, she said. Department officials uncovered the problem during the weekend when they ran a security check on the computers. The computers are protected by a password, and Sharkey said she suspects that the hackers got through by trying "again and again and again." The security check showed that in other unrelated cases, hackers from Korea and Indonesia had tried to gain access to the system but were unsuccessful, she said.

Category 17.1 Penetration

2006-03-06 **hacker penetration Georgetown University server personal information disclosure**

EDUPAGE; http://www.computerworld.com/ 23

HACKER ACCESSES GEORGETOWN SERVER

An external hacker has accessed a server at Georgetown University, according to officials from the Washington, D.C., institution. The server contained personal information on more than 41,000 individuals being tracked by the District of Columbia's Office of Aging. The office was working with the university as part of a grant to manage the information. According to the university, the breach was discovered on February 12. Although the server was immediately taken off line, the Office of Aging was not notified until February 24 because school officials did not understand the scope of the exposure for some time. The Secret Service was then notified and is working with the university to try to identify the hacker. David Lambert, CIO at Georgetown, said the university would undertake a thorough review of its computer systems, "focused on enhancing the security of confidential information contained on campus and departmental servers."

Category 17.1 Penetration

2006-04-16 **computer breaches intrusion security attention Iowa State University**

DHS IAIP Daily; 23
http://www.businessrecord.com/main.asp?SectionID=8&ArticleID
=2656&SubSectionID=9

HIGH-PROFILE COMPUTER BREACHES DRAW ATTENTION TO SECURITY.

In December, an intruder breached the security of two Iowa State University computers containing encrypted credit card numbers of athletics department donors and Social Security numbers of more than 3,000 university employees. An investigation determined that the intruder hacked into the computers to store and distribute pirated movies or music. The incident prompted efforts over the past four months to tighten security around sensitive information and a greater awareness among students, faculty and non-information technology staff that the threat of an attack exists and it is up to the entire university community to prevent another incident. Incidents such as the one at Iowa State have created greater awareness nationwide of the widespread threat of computer security breaches. According to a recent FBI survey of more than 2,000 businesses in Iowa, Nebraska, New York and Texas, nearly nine out of 10 suffered from a computer virus, spyware or other online attack in 2004 or 2005. Though most companies use security software, computer hacking techniques are also far ahead of what they were 18 months ago, according to Loras Even, managing director of RSM McGladrey Inc.'s Integrated Technology Solutions.

Category 17.1 *Penetration*

2006-04-23 **University of Texas UT Austin computer breach hacking penetration sensitive data disclosure Social Security numbers**

EDUPAGE; 23
http://news.yahoo.com/s/ap/20060424/ap_on_hi_te/ut_computer_breach

UT SUFFERS ANOTHER COMPUTER BREACH

Officials at the University of Texas at Austin (UT) said a hacker broke into a computer system at the university's McCombs School of Business and may have accessed sensitive data on nearly 200,000 students, faculty, and alumni. The breach is the second major incident for the university after a former UT student was found to have hacked into a university computer system in 2003. In that incident, the hacker accessed about 40,000 Social Security numbers. William Powers Jr., president of UT, said that the current incident, which may have begun as early as April 11, appears to have been limited to the business school. The university has set up a hotline for those whose information may have been compromised.

Category 17.1 *Penetration*

2006-04-25 **confidentiality privacy control SSNs Social Security Numbers university criminal hacking penetration**

RISKS 24 26

ANOTHER SECURITY/PRIVACY BREACH AT THE UNIVERSITY OF TEXAS

Nearly 200,000 electronic records at the University of Texas at Austin's business school have been illegally accessed, including SSNs and possibly bio info on faculty, students, staff, and alums. The previous breach occurred in 2003, resulting in a former UT student receiving five years of probation and having to pay $170,000 in restitution for accessing almost 40,000 SSNs. Last year, a former UT student received five years probation and was ordered to pay $170,000 in restitution for hacking into the school's computer system in 2003 and accessing almost 40,000 Social Security numbers.

[Abstract by Peter G. Neumann]

17.2 Web vandalism

Category 17.2 *Web vandalism*

2000-01-17 **Web site vandalism defacement criminal hackers**

AP

In mid-January 2000, the "Lamers Team" criminal hackers claiming to be from Europe defaced the "Thomas" Web site of the Library of Congress, one of the most popular government sites among journalists and others needing information about pending legislation in the House and Senate of the USA.

Category 17.2 *Web vandalism*

2000-01-18 **Web defacement vandalism criminal hackers**

Irish Times

Cybervandals damaged the Web site of the University of Limerick; the perpetrators left electronic graffiti with the initials of Trinity College Dublin prominently displayed, perhaps in an attempt to implicate that institution in the crime.

Category 17.2 *Web vandalism*

2000-03-07 **Web defacement vandalism impersonation spoofing**

RISKS 20 83

In early March, someone attacked two victims in one case of Web vandalism. The Gallup Organization's Web site was defaced and AntiOnline's John Vranesevich was fraudulently indicated as the defacer. This case supports the view that it is unwise to assume that the apparent attacker really has caused the damage at hand; it makes immediate vigilante revenge action ever less reasonable.

Category 17.2 *Web vandalism*

2000-04-05 **Web attack law enforcement deterrence arrest search warrant seizure evidence ISP**

RISKS 20 87

Ulf Lindqvist reported in RISKS that the operators of the Web site for the Swedish National Board of Health and Welfare (Socialstyrelsen) reported an attack to the National Police Computer Crime Squad so promptly that the police were able to find the perpetrator's home phone number from the ISP involved. Armed with a search warrant, they arrested a 16 year-old boy and seized his and his parents' computers. Lindqvist wrote, "What I personally find noteworthy in this story is how quickly the police reacted and that it could be a sign of the trend to treat computer crimes no differently than "low-tech" crime. When organizations see that it actually helps to call the police in cases like this, maybe they will be less reluctant to do so. The deterrent effect on would-be criminals by likely detection and immediate response should not be underestimated."

Category 17.2 *Web vandalism*

2000-09-13 **Web site vandalism hactivism**

RISKS 21 05

Mike Hogsett reported in RISKS as follows: >Someone identified as "fluxnyne" cracked into the OPEC Web site, posting this message: "I think I speak for everyone out there (the entire planet) when I say to you guys to get your collective a**es in gear with the crude price. We really need to focus on the poverty-stricken countries, who don't even have enough money for aspirin, let alone exorbi[t]ant prices for heating oil. I think the lives of children are paramount to your profits."<

Category 17.2 *Web vandalism*

2001-05-03 **Web server vulnerability exploit criminal hacker international defacement**

NIPC Daily Report

Computer intruders managed to gain control of three international Microsoft home pages on 3 May, replacing the company's data with a simple message taunting the software giant. Microsoft s UK, Mexico and Saudi Arabia sites were replaced with messages from the hacker group Prime Suspectz. The defacements come two days after Microsoft revealed its flagship Web server software had a serious vulnerability, but it is not known if the intruders used that vulnerability to attack the Microsoft sites. In a related development, a computer hacker published code on 2 May that makes taking advantage of the new Microsoft flaw easy for any ill-intentioned computer programmer. (Source: MSNBC, 3 May)

Category 17.2 *Web vandalism*

2001-05-04 **information warfare criminal hacker attacks Web sites defacement probing scanning international vulnerabilities**

NIPC Daily Report

According to the Xinhua News Agency, Chinese Internet operators and administrators have been warned to be aware of hacker attacks and reminded of the need for Internet security by an official with the Computer Network and Information Security Management Office. Nearly 14% of all hacker attacks that happened in April across the world were targeted at Chinese mainland Web sites, said the official. Among the several hundreds of Chinese Web sites attacked, 54% were commercial, 12% official and 19% education and scientific research Web sites. According to Internet experts, in April, there was an increase in reports of probing and scanning by would be intruders seeking to find security cracks in systems that could be compromised. An average of 100 sites a day have seen some form of attack. A Xinhua Web report said as many as 700 official and non-governmental Web sites from both countries were hacked from 30 April to 1 May, 600 were from the Chinese mainland and Taiwan, and the other 100 or so were from the U.S. (Source: Beijing China Daily, 4 May)

Category 17.2 *Web vandalism*

2001-05-05 **Web defacement criminal hacker gang group**

NIPC Daily Report

A hacker group calling itself Prime Suspectz defaced three Microsoft sites on 3 May, although the software company managed to get the sites back to normal within hours. That makes nine times that Microsoft Web sites have been hacked in the last 20 months. The latest Microsoft sites to be defaced- Microsoft Mexico - join previously defaced Microsoft sites in Brazil, New Zealand and Slovenia.incidents. COMMENT: Please remember that these sites are hosted by ISPs within the victim country and not maintained by Microsoft. (Source: Newsbytes, 5 May)

Category 17.2 *Web vandalism*

2003-05-02 **internet radio station site hacker damage Denver Colorado Larry Nelson w3w3 FBI e-mail**

NIPC/DHS

May 02, Rocky Mountain News — Hackers damage Internet radio site.

Hackers broke into the Web site of an Internet radio station in Denver, CO that's sponsoring a Denver conference next week aimed at thwarting computer break-ins. The attack is believed to have caused more than $50,000 in damage. Larry Nelson of the w3w3 network, the target of the attack and sponsor of the conference dubbed "Cyber Security Super Bowl," said the hackers got away with up to 1,000 names and e-mail addresses for people attending the conference. The conference will bring together industry and government experts from around the nation to discuss homeland defense and cybersecurity - a growing field that aims to protect computer systems from hackers. Nelson said the FBI and two cybersecurity firms probing the attack plan to use the case as a model to underscore the threat of Internet-based break-ins.

Category 17.2 *Web vandalism*

2003-06-26 **cyber thief web addresses los angeles county pornographic e-mail junk Atriva bogus company hijacker**

NIPC/DHS

June 26, Pasadena Star News — Cyber-thief nets 65,000 county Web addresses.

An Internet hijacker stole 65,000 Web site addresses belonging to Los Angeles County between April 3 and May 1. The addresses were then sold and used to send pornographic material and junk e-mail, and to try to hack into other computers. No harm was done to the county during the scam. It apparently only took a phone call and follow-up e-mail to the American Registry of Internet Numbers for the hijacker to change ownership of the county's Web addresses into another name, according to the county's Chief Information Officer Jon Fullinwider. The registry, according to county officials, put the addresses into the name of Atriva, which turned out to be a bogus company. An investigation is continuing to find the hijacker.

Category 17.2 *Web vandalism*

2003-07-02 **warning message 6000 websites hackers challenge.com Critical Infrastructure necessary measures security server**

NIPC/DHS

July 02, Associated Press — Warning of massive hacker attacks.

Hackers plan to attack thousands of Web sites Sunday in a loosely coordinated "contest" that could disrupt Internet traffic. Organizers established a Web site, defacers-challenge.com, listing in broken English the rules for hackers who might participate. The Chief Information Officers Council cautioned U.S. agencies and instructed experts to tighten security at federal Web sites. The New York Office of Cyber-Security and Critical Infrastructure Coordination warned Internet providers and other organizations that the goal of the hackers was to vandalize 6,000 Web sites in six hours, and urged companies to change default computer passwords, begin monitoring Web site activities more aggressively, remove unnecessary functions from server computers and apply the latest software repairs. The purported "prize" for participating hackers was 500-megabytes of online storage space, which made little sense to computer experts who said hackers capable of breaking into thousands of computers could easily steal that amount of storage on corporate networks.

Category 17.2 *Web vandalism*

2003-07-07 **hackers web vigilante-style attacks break-ins online vandalism small internet sites disrupted**

NIPC/DHS

July 07, Associated Press — Hackers limit disruption to small Internet sites.

A battle among hackers erupted on the Internet yesterday as some factions disrupted a loosely coordinated effort among other groups trying to vandalize Web sites around the world. Unknown attackers for hours knocked offline an independent security Web site that was verifying reports of online vandalism and being used by hackers to tally points for the competition. U.S. government and private technology experts warned last week that such vandalism was likely. After three such vigilante-style attacks, the hacker organizer extend the contest until 6 p.m. yesterday. With continued attacks disrupting the ability of vandals to claim credit for their break-ins, some experts said it could be later this week before damage from the weekend's hacking would be known. There were no reports of vandalism involving larger, more well-known Internet sites, which may be a testament to improved online security at large companies, government agencies and organizations.

Category 17.2 *Web vandalism*

2003-07-14 **ten internet sites hacker destroy Sudanese major corporations Airlines Al-Sahafa Khartoum University Aptec Computers revenge**

NIPC/DHS

July 14, Arab Times — Hacker destroys ten Internet sites.

A Sudanese hacker claimed to have destroyed the Internet websites of 10 major corporations, one of which is the Sudanese Airlines, Al-Sahafa newspaper said Sunday. The hacker sent an e-mail to Sudanese Airlines saying that by hacking the company webpage he is taking revenge for the families of victims of the plane crash that took place last Tuesday killing 115 passengers. The hacker claimed to have destroyed the websites of Khartoum University, Aptec Computers and the Sudanese Internet Company. He said he is working on the destruction of more websites.

Category 17.2 *Web vandalism*

2003-12-02 **domain name Website registry .name hacked Global Name Registry GNR**

NIPC/DHS

December 01, The Register — Website .name registry hacked.

The Website of the .name registry was hacked over the weekend through an Apache exploit. London-based Global Name Registry (GNR) was updating its Apache and PHP system when hackers broke into the system and replaced the frontpage index file. The hackers didn't manage to access the system and no data was lost, GNR's president Hakon Haugnes said. The site was taken offline and was back up by Sunday, November 30 with added security. "We were adding patches but in spite of that someone managed to get to the index file," said Haugnes. The .name domain—one of seven approved by ICANN in 2001—now has around 100,000 registrants.

Category 17.2 *Web vandalism*

2003-12-19 **NASA Websites hacked Brazilian defacement vandalism Netcraft PHP**

NIPC/DHS

December 18, ComputerWorld — NASA sites hacked. Thirteen NASA Websites were defaced Wednesday by a Brazilian crew dubbed drwxr, according to a statement from Zone-H, an organization that monitors hacking. Zone-H said the defacer apparently modified the index pages on the sites to express his opinion about the Iraq war. The main NASA Web site did not appear to be among those hit by the attack. Zone-H, citing Netcraft Ltd., a British Internet consultancy, said the sites were running the Apache 1.3.27 Web server with PHP (an open-source scripting language often used to create dynamic Web pages) and several Apache modules on a Linux system. "We can suppose that the server was remotely compromised using a vulnerability in a PHP script, then the defacer probably gained root privileges using the local root exploit for the Linux kernel 2.4.22 published by iSEC Security Research last week." NASA spokesman Brian Dunbar confirmed that the sites had been hacked and defaced and said the agency had taken them offline. The hacked NASA Web sites include its Computing, Information and Communications Technology Program site; the NASA Advanced Supercomputing Division; the NASA Information Power Grid; and the NASA Research & Education Network.

Category 17.2 *Web vandalism*

2004-06-19 **Web vadalism network hacking al-Qaeda hostage beheading video**

NewsScan

NETWORK VANDALS POST TERROR VIDEOS ON INNOCENT WEB SITE

Network vandals invaded the Web site of a San Jose mapping and land-surveying company last week to post videos of the American engineer Paul Johnson, who was captured and later beheaded by al-Qaeda terrorists in Saudi Arabia. Tim Redd, owner of Silicon Valley Land Survey, said: "The
usage at the Web hosting company went sky-high. We're saddened by the events that provoked all this activity." Redd didn't know that vandals were using his Web site until a reporter from German magazine Der Spiegel contacted him. The FBI is investigating. Ira Winkler of the security firm CSC thinks it will be difficult to trace the invaders because they "will break into a series of networks and use them to disguise their tracks." (AP/USA Today 19 Jun 2004)

Category 17.2 *Web vandalism*

2004-06-21 **hacker Web vandalism South Korean defense site Trojan Horse attack**

NewsScan

HACKER HITS SOUTH KOREAN DEFENSE

A network vandal has broken into computers at sensitive South Korean research institutes and government agencies, infecting more than 60 PCs with a variation of the Peep Trojan program. The National Cyber Security Center (NCSC) said the hacker had broken into computers at the Agency for Defense Development, which develops weapons, the Korea Atomic Energy Research Institute, the Korea Institute for Defense Analysis and three other government agencies. (The Australian 21 Jun 2004) Rec'd from John Lamp

---

Category 17.2 *Web vandalism*

2005-06-03 **Web vandalism hacking Microsoft Network MSN Website South Korea password stealing victim outsourced hosting**

DHS IAIP Daily; http://www.washingtonpost.com/wp−
dyn/content/article/2005/06 /02/AR2005060201604.html?nav=hcmodule

MICROSOFT SAYS MSN WEBSITE HACKED IN SOUTH KOREA

Microsoft acknowledged Thursday, June 2, that hackers booby-trapped its popular MSN Website in South Korea to try to steal passwords from visitors. The company said it was unclear how many Internet users might have been victimized. Microsoft said it cleaned the Website, http://www.msn.co.kr and removed the dangerous software code that unknown hackers had added earlier this week. A spokesperson, Adam Sohn, said Microsoft was confident its English-language Websites were not vulnerable to the same type of attack. The Korean site, unlike U.S. versions, was operated by another company Microsoft did not identify. Microsoft's own experts and Korean police authorities were investigating, but Microsoft believes the computers were vulnerable because operators failed to apply necessary software patches, said Sohn, an MSN director. MSN Korea said the only site affected by the hacking was the MSN Korea news site: http://news.msn.co.kr

---

Category 17.2 *Web vandalism*

2005-06-10 **Web vandalism hacking defacement Korean Mozilla Website Simiens Crew Brazilian organization**

DHS IAIP Daily; http://www.internetnews.com/security/article.php/3512081

HACKERS DEFACE KOREAN MOZILLA WEBSITE

The Korean language Mozilla Website was hacked and defaced last week, prompting calls from some corners of the open source community to gain control of the independent site. The job was likely the work of the notorious Simiens Crew, a Brazil-based outfit, and while the main page was not affected, other pages were replaced by the message "Simiens Crew ownz u viva os macacos." The phrase "os macacos" means "the monkeys" in Portuguese. It could be that the hackers simply have misspelled their own name, according to MozillaZine, a Web-based forum for the browser's enthusiast. The proper spelling is "Simians" and means apes. The crew has attacked several high-profile sites, often exploiting a vulnerability in the AWStats log file analyzer, according to MozillaZine. While Mozilla Europe, Mozilla Japan and Mozilla China have an official affiliation with the foundation, the Korean language Website has no official connection. Channy Yun, leader of Mozilla Korean Community, said the hack happened because there was not a patch for a PHP vulnerability for the company hosting mozilla.or.kr. He assured users he would backup and fix the problem with the ISP.

Category 17.2 *Web vandalism*

2005-07-06 **The Register Micrsoft UK hacking defacer Apocalypse Rafa GIF Microsoft institutions government Aponte World of Hell**

DHS IAIP Daily; http://www.theregister.co.uk/2005/07/06/msuk_hacked/

MICROSOFT UK DEFACED IN HACKING ATTACK

Microsoft's UK Website was defaced by well-known defacer Apocalypse Tuesday, July 5, with a message in support of Venezuelan hacker Rafa. The site has since been restored to normal operation and the offending GIF removed. A Microsoft spokesman said it was aware of the attack, which technical staff are investigating. "There is no reason to believe customer data or any other sensitive information has been compromised," he said. Apocalypse has been targeting U.S. institutions and the government sites for months, always posting messages in support of Rafa Nunez-Aponte, a suspected member of the World of Hell hacking crew. Rafa is in custody in the U.S. following his arrest in Miami, FL, in April over a series of alleged attacks on U.S. Department of Defense servers dating back to 2001. Previous targets of DHS IAIP DHS IAIP Daily; DHS IAIP Daily; Daily; Apocalypse's "digital graffiti" attacks have included Stanford University and U.S. Navy Websites.

Category 17.2 *Web vandalism*

2006-05-03 **hacker attack train signs Canadian Prime Minister Stephen Harper Eats Babies**

DHS IAIP Daily; http://www.theregister.co.uk/2006/05/03/canadian_train_sign_ 23
hack/

HACKERS LIBEL CANADIAN PRIME MINISTER ON TRAIN SIGNS.

Bewildered Toronto, Canada, train passengers were left scratching their heads after a hacker altered advertising signs in order to mock Stephen Harper, the country's prime minister, on the westbound Lakeshore GO Transit train. Scrolling LED signs on several trains repeated the message "Stephen Harper Eats Babies" every three seconds during the duration of the attack. Security specialists told the Toronto Star that the attack was probably carried out by a remote control device that can be used to program scrolling electronic signs. The kit can be bought over the counter at electronic hobby stores, such as Sam's Club.

17.3 Phreaking, cramming, uncapping, theft of services

Category 17.3 *Phreaking, cramming, uncapping, theft of services*

2000-10-12 **telephone calling card fraud personal identification number PIN keyspace brute-force cracking**

RISKS 21 09

Peter Reith, a minister in the government of Australia, repaid $950 in calls placed by his son using an official government calling card. The minister had foolishly given his son the personal identification number (PIN) for the card. However, he expressed surprise at the 11,000 phone calls made from 900 locations around the world (e.g., the US, Singapore, Malaysia, Hong Kong, Thailand and China) which generated over A$50,000 in charges. Fergus Henderson commented in RISKS, "in order to make phone calls billed to the card, you only need to know the 8-digit card number and the 4-digit pin number."

Category 17.3 *Phreaking, cramming, uncapping, theft of services*

2002-03-05 **phone phreaking fraud unauthorized charges**

RISKS, http://www.computerworld.com/cwi/story/0,1199,NAV47-74_STO68446,00.html 21 93

As mentioned in RISKS by Anthony W. Youngman and summarized by Peter G. Neumann, Nicholas Petreley suffered from phone phreaking and reported on it extensively in his _Computerworld_ column <http://www.computerworld.com/cwi/story/0,1199,NAV47-74_STO68446,00.html >. Neumann wrote, "After noticing the frequent calls to Germany, Nick canceled his calling card and switched his long-distance carrier. The person who had been piggybacking on his old card then managed to switch his new account back to the old carrier and make more calls. It turns out that person had created a Web account for him, so that he no longer received statements. The entire saga is a real horror story, and very well worth reading. Lots of lessons to be learned."

Category 17.3 *Phreaking, cramming, uncapping, theft of services*

2002-05-14 **cell phone wireless clone fraud differential cryptanalysis**

NewsScan

ATTACK OF THE PHONE CLONERS
A team of engineers from IBM and the Swiss Federal Institute of Technology have found a way to capture the data necessary to "clone" a cell phone in 60 seconds. Previous methods used to copy the identifying data that enables calls to be charged to another person's phone took about eight hours. The researchers found that they could gain valuable information about the numerical "key" a phone uses to uniquely identify its owner by timing how long the phone's chip took to complete certain tasks and by measuring changing current flows across the chip. Taken together, the information revealed what was being done to the numerical key. The researchers say that chips can be protected against this type of espionage by making sure all computational tasks take the same amount of time, or by changing the way a chip carries out certain computations. (BBC News 14 May 2002) http://news.bbc.co.uk/hi/english/sci/tech/newsid_1984000/1984887.stm

---

Category 17.3 *Phreaking, cramming, uncapping, theft of services*

2003-02-18 **telephone PBX phone fraud hacking Taiwan credit card information stolen scam**

NIPC/DHS

February 14, SC Infosecurity News — Taiwanese telco virtual operator system hacked.

Chungwa Telecom of Taiwan has issued warnings about its virtual telephone operator service, which allows the company's staff to act as PBX operators for those Taiwanese companies without their own operator staff. Hackers have been taking advantage of companies that had not changed their control PIN from the default settings of 0000, 9999 or 1234. The result has been that hackers have been able to intercept calls originally destined to be handled by Chungwa's operators, routing to their prepaid (and anonymous) mobile phones. The hackers are said to have taken card details from callers and used the information to swindle them. Taiwan's Morning Post newspaper says that Chungwa Telecom has not revealed the scale of the problem, or the names of the companies affected, although the paper says the firms are known to be in the courier and allied business markets. The paper adds that affected customers' claims have been settled, while police are investigating the scam. The firms affected by the scam are said to have suspended their use of the virtual operator facility, switching back to using their own staff to answer calls.

Category 17.3 *Phreaking, cramming, uncapping, theft of services*

2003-05-16 **New Jersey company illegal advertising pornographic internet charging telephone connection dial-up**

NewsScan

13 STATES SUE OVER POP-UP ADS
Thirteen states have sued a New Jersey company that allegedly billed Internet users who tried to close pop-up windows advertising p*rnographic Web sites. The lawsuit maintains that Alyon Technologies automatically connected users to its toll telephone number when they tried to close the ads, and then charged them $5 a minute, resulting in bills ranging from $14 to more than $1,000. "The way this organization has allegedly been doing business is illegal, irresponsible and an outrageous misuse of Internet technology," said Wisconsin Attorney General Peg Lautenschlager. Joining Wisconsin in the suit are California, Connecticut, Florida, Illinois, Kentucky, Missouri, New Jersey, Ohio, North Carolina, Nebraska, Texas and West Virginia. (AP 16 May 2003)

Category 17.3 *Phreaking, cramming, uncapping, theft of services*

2003-06-10 **compromising PBX Private Brach Exchange systems voice mail internet service providers overseas Bill Murray FBI 911 center**

NIPC/DHS

June 10, Washington Post — Phone networks open doors for hackers.

Federal law-enforcement officials said last week that they are tracking numerous reports of hackers who gain access to corporate voice mail and telephone systems to launch Internet attacks. The hackers, according to the Department of Homeland Security (DHS), tap into corporate phone systems, or private branch exchange (PBX) systems, using them to make long-distance calls to Internet service providers in other cities or overseas. Hackers compromising PBX systems can use them as entryways into computer systems, said Lisa Pierce, a research fellow for the Giga Information Group. From there they can steal corporate information, eavesdrop on conversations and create havoc on the system because no one knows where the attacks are coming from, she said. FBI cyber division spokesman Bill Murray said poorly secured PBX systems also present a serious national security threat. A hacker could use a compromised PBX system to route dozens of calls simultaneously to an emergency 9-1-1 center, overloading the emergency call center and preventing real emergency calls from getting through. A tutorial on locking down PBX and voicemail systems is available from the National Institute of Standards & Technology at: http://www.csrc.nist.gov/publications/nistpubs/800-24/sp800- 24pbx.pdf

---

Category 17.3 *Phreaking, cramming, uncapping, theft of services*

2003-06-20 **Indian cellular fraud Hutchison Essar telecommunications company New Delhi**

NIPC/DHS

June 20, SC Infosecurity News — Four men charged in major Indian cellular fraud.

A U.S.-based IT professional and three Indian citizens have been arrested, charged with defrauding Hutchison Essar, an Indian telecommunications company, of around $200,000. Delhi Police arrested two of the men in the city of New Delhi, while the other two, including the U.S. citizen originally from India, were arrested in the city of Kochi at the start of June. The losses were incurred after the men conspired to activate and use 19 GSM SIM cards in the U.S., making significant volumes of calls back to India and other countries. The case highlights the delays that some cellular carriers experience before forwarding roaming call data on to other networks in other countries. While all GSM networks authenticate roaming SIM card accounts with their home network before each roamed call is connected, information on the actual value of the call is not shared in real time.

Category 17.3 *Phreaking, cramming, uncapping, theft of services*

2003-06-25 **phone phreaking victims pay AT&T**

NIPC/DHS

April 21, New York Times — AT&T trying to collect bills from the victims of hackers.

The city of East Palo Alto, CA, is battling with AT&T over who is responsible for a $30,000 long-distance phone bill that resulted from voice mail hacking. Last summer, hackers in the Philippines and Belgium penetrated the agency's voice mail system, operated by SBC Communications, the local phone service provider, by figuring out system pass codes. AT&T wants the city to pay the bill for the fraud, which it says was the customer's responsibility to prevent. It offered a settlement in which it would pay 30 percent of the charges, but the city says the company should pay the whole thing. Voice mail hackers have discovered that if voice mail customers do not change their default pass code when the system is set up, they can sometimes break in by figuring out assigned pass codes. Hackers breaking into the system then change the outgoing message to one that automatically accepts collect calls. Once connected, the hackers can leave the line open for hours, charging up enormous bills. AT&T now requires that individuals accepting collect calls, besides having to respond "yes" when prompted, also enter a three-digit number.

June 25, SecurityFocus — AT&T lets phone fraud victims off the hook. AT&T said Wednesday that it would forgive all of the outstanding long distance charges that the company had been trying to collect from victims of the so-called "Yes-Yes" voicemail subversion fraud. Last year fraudsters began cracking weak and default PINs on individual and small business voice mail boxes provided by local phone companies, then changing the outgoing messages to say "yes, yes, yes" over and over again. The newly-agreeable voice mail could then be used for third-party billings. The scam left scores of victims holding liable for thousands of dollars of long distance calls they never made-typically between $8,000 and $12,000. AT&T insisted that the victims pay up, arguing that it was the consumer's poor voice mail security that was at fault. When pressed, the company sometimes offered to absorb 35% of a fraudulent billing. The company announced Wednesday that it's will abandon those collection, but the amnesty offer only applies to past victims of this particular type of fraud.

Category 17.3 *Phreaking, cramming, uncapping, theft of services*

2003-09-11 **Voice mail hijacked passwords small businesses outgoing messages protection accept collect calls Yes positive**

NIPC/DHS

September 11, KIRO TV (Seattle, WA) — Voice mail hijacked to accept collect calls from crooks.

The words "Yes, Yes, Yes" usually mean something positive, but not in this case. A new con uses these three words to rip off voice mail users. Maureen Claridge says she got stuck with a large phone bill because someone hijacked her voice mail. Maureen's voice mail usually sounded like this: "This is Maureen; I'm in the office, but on the other line, leave a number and I'll get back to you as soon as I can." But a crook hacked into it and recorded the words "yes, yes, yes." The crooks target people who have simple voice mail passwords. They use the password to hack into the system and change the message to accept collect calls. Then they ask you a series of questions, usually three, and the answer is "yes, yes, yes." The voice mail telephone company says small business people are often targeted, because they don't answer their phones on the weekend. To protect yourself, check your outgoing message from time to time and change your password to something only you would know.

Category 17.3 *Phreaking, cramming, uncapping, theft of services*

2004-02-05 **cable modem hacking firmware flash Motorola coders uncappers bandwidth limitations breach of contract illegal theft services**

RISKS; http://www.securityfocus.com/ news/7977 23 18

CABLE MODEM HACKERS CONQUER THE CO-AX
(Kevin Poulsen, SecurityFocus)

A small and diverse band of hobbyists steeped in the obscure languages of embedded systems has released its own custom firmware for a popular brand of cable modem, along with a technique for loading it -- a development that's already made life easier for uncappers and service squatters, and threatens to topple long-held assumptions about the privacy of cable modem communications. The program, called Sigma, was released in its final version last month, and has reportedly been downloaded 350 to 400 times a day ever since. It's designed to be flashed into the nonvolatile memory of certain models of Motorola's Surfboard line, where it runs in parallel with the device's normal functionality. It gives users almost complete control of their cable modem -- a privilege previously reserved for the service provider. The project is the work of a gang of coders called TCNiSO. With about ten active members worldwide, the group is supported by contributions from the uncapping community -- speed-hungry Internet users who rely on TCNiSO's research and free hackware to surmount the bandwidth caps imposed by service providers, usually in violation of their service agreement, if not the law. To them, Sigma is a delight, because it makes it simple to change the modem's configuration file -- the key to uncapping, and, on some systems, to getting free anonymous service using "unregistered" modems. "I've known TCNiSO for two years now and I've done a lot of things with their techniques," wrote a Canadian uncapper in an e-mail interview. "Sigma is the greatest one I've seen." …

Category 17.3 *Phreaking, cramming, uncapping, theft of services*

2004-02-12 **organized crime cramming fraud telephone bills**

RISKS; http://www.nytimes.com/2004/02/11/nyregion/11MOB.html 23

OFFICIALS SAY MOB STOLE $200 MILLION USING PHONE BILLS

Peter Neumann wrote, >New York organized crime figures reportedly bilked millions of unsuspecting consumers out of more than $200 million over five years by piggybacking bogus charges on their telephone bills ("cramming"). <

Category 17.3 *Phreaking, cramming, uncapping, theft of services*

2004-07-13 **penetration criminal hacking phreaking**

NYT http://www.nytimes.com/2004/07/13/nyregion/13hacker.html

Julia Preston of the New York Times wrote:

"A Westchester County man illegally infiltrated an internal computer at Verizon more than 100 times this year, forcing the telecommunications company to spend at least $120,000 to retool its security system, prosecutors charged in a federal indictment yesterday [Monday 12 July 2004].

The man, William Quinn, 27, of Eastchester, obtained many passwords to a central computer that Verizon technicians use in repairing telephone lines, according to the indictment, filed in the Southern District of New York in Manhattan. . . . ."

Category 17.3 *Phreaking, cramming, uncapping, theft of services*

2004-07-20 **phone phreaking Phillipines hacking telecommunications Manila raids**

NewsScan

THREE HELD ON PHREAKING CHARGE IN PHILLIPINES

Eight people, including two Indians, a Bangladeshi, and five Filipinos, have been arrested for allegedly hacking into Philippines telecommunications systems to make unauthorized long-distance calls. The suspects, who were arrested in a series of raids in and around Manila, will be charged with
using computer equipment to break into the systems of corporate subscribers of dominant carrier Philippine Long Distance Telephone Co. and then selling long-distance calls to other people, charging the costs to the unwary corporate subscribers. (The Age 20 Jul 2004) Rec'd from John Lamp

---

Category 17.3 *Phreaking, cramming, uncapping, theft of services*

2005-04-05 **New York state law target modem hijacking consumer international phone calls phreaking service theft**

DHS IAIP Daily; http://www.nytimes.com/aponline/technology/AP−Modem−Hijackin g.html

NEW YORK LAWMAKERS TARGET MODEM HIJACKING

New York state lawmakers unveiled a bill Monday, April 4, that is believed to be the first in the nation to target modem hijacking, a practice in which thieves tap into people's computer modems to make international phone calls. If passed, the law would allow telephone companies and the state attorney general to bring lawsuits against modem hijackers and their accomplices. The hijackers tap into people's modems by luring computer users to specific Websites – sometimes through e-mails – where pop-up windows emerge inviting the user to click on them. The windows authorize the downloading of modem software that is then remotely accessed to make international calls that are charged back to the user. Consumers can fight hijacking by using a dedicated phone line for the computer dial-up connection, then blocking international calls to that line. New York Legislature: http://www.state.ny.us

---

Category 17.3 *Phreaking, cramming, uncapping, theft of services*

2005-07-31 **hotel system lap linux infrared IrDA USB TV tuner data leakage unauthorized access e-mail surveillance penetration cracking**

RISKS; http://www.wired.com/news/privacy/1,68370-0.html 23 95

HOTEL TV SYSTEM HACKED USING LAPTOP & TUNER

Adam Laurie, tech director of the London security and networking firm "The Bunker", apparently got bored on a recent trip and found the time to hack the hotel's TV system which lets customers not just watch 'normal' TV programming, but also, for a fee, provides access to not-safe-for-work flicks and access to the Internet including e-mail.

The article reports that a laptop running linux, its IrDA port and a USB TV tuner can be used to trick the TV into doing more than it was supposed to do, including gaining access to the NSFW content without being charged for it, snooping on other people's TV watching habits, their Internet browsing habits and their e-mails. Also, the "coding" system used for infrared-based access control to the hotel minibars doesn't seem to be insurmountable either.

[Abstract by Florian Liekweg]

The bill so far: Lost profit for the hotel, lost privacy for the customers, the possibility for corporate espionage. Return value: Easy network access. Good deal, eh?

[Abstract by Florian Liekweg]

Category 17.3 *Phreaking, cramming, uncapping, theft of services*

2005-12-22 **British face fines Parliament companies software hijacks connection United Kingdom fraudulent text messages voice mails applications Trojan spam**

DHS IAIP Daily; http://news.com.com/British+rogue+dialers+face+heftier+fines /2100−1037_3−6005760.html?tag=cd.lede

British "rogue dialers" face heftier fines.

British Parliament members have agreed to raise the maximum fine that can be imposed against companies that operate "rogue dialer" software that hijacks a dial-up Internet user's Web Connection. Parliament on Wednesday, December 21, agreed that, as of Friday, December 30, companies caught abusing United Kingdom premium-rate services should be liable to fines of up to $434,281, up from the existing limit of $173,998. The higher fines will also apply to fraudulent text messages and voice mails that tell people they have won a prize. Many thousands of dial-up Internet users have fallen victim to rogue dialers throughout 2005. Once installed on a dial-up user's PC, the applications can secretly dial a premium-rate number. This has led some people to run up call charges of hundreds of pounds. It's thought that many rogue dialers are spread using Trojan horses contained within spam e-mails. Last month, Ofcom warned that there was "growing evidence of consumer harm" arising from rogue dialers.

18.1 Theft of equipment

Category 18.1 *Theft of equipment*

1997-01-29 **theft ATM**

AP

Thieves bypassed fancy electronic security measures on a Portland, TN automated teller machine. They attached cables to the device and ripped it off its foundation using a tow truck. The ATM was found ripped open in a field some miles away.

Category 18.1 *Theft of equipment*

1997-02-02 **infowar intrusion theft privacy**

PA News

UK Defence Secretary Michael Portillo appears to have been the victim of a theft of computer files. The _Sunday Times_ reported to police that it was offered 7,000 confidential files on 12 floppies from the Minister's parliamentary office dating from 1987. The thieves asked for 2,000 pounds payment and said that private files from Deputy Prime Minister Michael Heseltine and Home
Secretary Michael Howard were also available for a fee.

Category 18.1 *Theft of equipment*

1997-03-25 **theft counterfeit**

RISKS 18 94

Thieves have stolen valuable equipment used to make "non-counterfeitable" drivers' licenses in Florida. The machines were left in unguarded, unprotected state offices.

Category 18.1 *Theft of equipment*

1997-04-02 **computer theft**

RISKS 19 2 ff

When the CalTrain computer used to issue tickets by mail was stolen, the company initiated cancellations for the thousands of credit cards in their unencrypted database. These cancellations were to be carried out before users were informed that their credit cards would no longer work: not much fun for travelers with only one credit card. Luckily or unluckily (you decide), a later posting revealed that the credit-card companies seem to have ignored the requests for cancellation.

Category 18.1 *Theft of equipment*

1997-05-02 **computer theft privacy**

RISKS 19 12

When a computer hard-disk was stolen from Levi Strauss, the personnel records containing personal information for 40,000 employees and former employees were compromised. A company spokesperson lamely assured the public that the data would be hard to read and that it wouldn't happen again. Moral: encrypt sensitive data on hard disks. Peter Neumann warned that the employee records would make the victims susceptible to theft of identity.

Category 18.1 *Theft of equipment*

1997-05-06 **laptop theft**

EDUPAGE

In 1996, claims the computer-insurance company SafeWare, 265,000 laptop computers were reported stolen — up 27% from 1995.

Category 18.1 *Theft of equipment*

1997-05-17 **computer theft forgery**

RISKS 19 16

In Oregon, the DMV lost its license-making equipment to thieves who stole the computer, printers, cables, and a camera. Observers expect a flood of forged drivers' licenses real soon now.

Category 18.1 *Theft of equipment*

1997-05-28 **theft hardware industrial espionage**

AP

Losses of computer components to thieves in Silicon Valley are approaching $1M per week, and the region's political representatives have asked that the FBI upgrade its San Jose satellite office to be a full-fledged center for fighting the growing problem. Thieves have lately been breaking into delivery vans rather than attacking factories, says a spokesperson for the San Jose Police Department's high-tech squad. The parts are then either shipped to Asia for inclusion in low-cost computer boards or sold right back to the victims who may be in desperate need of the components that were stolen. Another problem, according to Rep. Zoe Lofgren (D-CA), is industrial espionage. According to Richard Cole, AP Writer, "San Jose Police Chief Louis Cobarruvias sent a letter to Freeh along the same lines in March, saying Chinese and Japanese organized crime groups are taking a growing interest in Silicon Valley."

Category 18.1 *Theft of equipment*

1997-06-03 **theft hardware chips**

UP

In Los Angeles, 17 people were indicted for two military-style attacks on computer component factories. The defendants are accused of stealing $10M of chips and motherboards from Centon Electronics, Inc. on 97.05.16; in addition, 11 of the defendants are charged with theft of $400K of computer chips from Multi-Industry Technology, Inc. The alleged ring-leader, John That Luong, faces additional charges in San Francisco in connection with other computer robberies. The ring was described as being involved in Asian organized-crime syndicates.

Category 18.1 *Theft of equipment*

1997-06-05 **chip theft**

EDUPAGE

EDUPAGE editors write: "Federal prosecutors have indicted 17 individuals for their involvement with an Asian organized-crime syndicate responsible for armed robberies in May 1995 of more than $10 million worth of Intel Pentium chips from two companies in Orange County, California. (New York Times 4 Jun 97)"

Category 18.1 *Theft of equipment*

1997-06-23 **theft hardware chips**

RISKS 19 23

In Hacienda Heights, CA, five armed thieves kidnapped a businessman, took him to his factory and stole $800,000 in computer chips. Two criminals were arrested.

Category 18.1 *Theft of equipment*

1997-06-26 **theft hardware cable denial of service backhoe**

RISKS 19 23

Betty O'Hearn contributed this précis of a curious incident in the Far East (slightly edited):
>[From Reuters news wire 97.06.19 09:19 EDT] A thief removed 60 meters of cable from the center of the remote Russian city of Ulan-Ude (the capital of the Republic of Buryatiya, near Mongolia), which shut down external communications for five hours on 19 Jun 1997. "The incident . . . affected military . . . [and] other communications in the region and caused an estimated loss of 800 million rubles ($135,000)." Apparently, the criminal or criminals may have been harvesting precious metal from the lines. ("Earlier this week two thieves were electrocuted in eastern Kazakhstan as they tried to steal copper wires from a high-voltage power transmission line.") [Source: Itar-Tass news, 19 Jun 1997]<

Category 18.1 *Theft of equipment*

1997-08-15 **airport theft fraud confidence tricksters laptops security**

UPI

Air travellers should beware unusual gefuffles at security checks. Organized gangs identify victims with valuable computers and cameras. While one criminal goes quietly througy security before the victim, one or more step in front of the victim and cause delays by carrying metal objects, dropping things, or getting into mock arguments. Meanwhile, the first thief makes off with valuables. Solution: do not allow anyone to step in front of you once you have put your valuables through the X-ray machine; if you are delayed, call out clearly to the security staff to keep their eye on your belongings.

Category 18.1 *Theft of equipment*

1997-08-22 **theft medical research cancer data confidentiality**

PA News

Professor David Newell of Newcastle University suffered a grievous loss when someone stole his computer and five floppy disks containing the sole copy of his research data. The thief eventually returned the five disks; the professor politely requested the return of his computer. Had no one ever broached the topic of off-site backups to the good professor?

Category 18.1 *Theft of equipment*

1997-08-26 **credit card theft sniffer ISP FBI sting**

RISKS, EDUPAGE 19 19

Peter Neumann summarized one of the largest cyber-related FBI stings of recent years:
>Carlos Felipe Salgado Jr. ("Smak", 36, Daly City, CA) was arrested at San Francisco Airport on 21 May 1997 after he sold an encrypted diskette with personal data on more than 100,000 credit-card accounts to undercover FBI agents, who paid him $260,000, checked out the validity of the data, and then nabbed him. He reportedly had obtained the information by hacking into various company databases on the Internet or by packet-sniffing an unidentified San Diego-based ISP. He faces up to 15 years in prison and $500,000 in fines.<

In August, Salgado pleaded guilty to the charges before beginning trial.

Category 18.1 *Theft of equipment*

1997-10-31 **theft burglary privacy questionnaires Internet**

Reuters

Burglars in the UK were reported to be offering free software and sending out questionnaires asking about details of people's private life and computer equipment — and then robbing cooperative victims. Moral: think before you answer questions from strangers.

Category 18.1 *Theft of equipment*

1997-11-19 **theft robbery authentication certificates CD-ROMs computers**

Reuters, EDUPAGE

In November, four masked gunmen attacked Thompson Litho Ltd in Scotland, bound its employees and stole 200,000 certificates of authenticity, 100,000 CD-ROMs, computers and other equipment — an estimated $16 million worth of goods. The company immediately circulated the serial numbers of the authentication certificates to dealers worldwide to prevent use in pirated software.

Category 18.1 *Theft of equipment*

1998-03-05 **chip theft robbery black market**

EDUPAGE

New technology adopted by the EIA (Electronic Industries Association) allows chips to be labelled indelibly with a serial number — seriously interfering with the worldwide flourishing trade in stolen chips.

Category 18.1 *Theft of equipment*

1999-01-01 **theft computer components organized crime**

UPI

On 31 December 1998, three members of Asian organized crime syndicates were convicted in Los Angeles of the largest theft of computer components in history. According to the UPI report, "The robbers escaped with $2 million worth of hard drives in a March 25, 1995, heist at Comtrade Electronics in City of Industry, CA and nearly $400,000 in computer components from Multi-Industry Technology in Cerritos, CA on May 3. The third crime . . . took place at Centon Electronics in Irvine, CA where approximately $10 million worth of computer chips and motherboards were stolen by the armed bandits."

Category 18.1 *Theft of equipment*

1999-01-05 **denial of service theft breakin violence**

RISKS 20 15

Three armed robbers broke into a Boston-area Sprint telephone office, assaulted workers with stun guns, tied them up, and stole telephone switches. The robbery interrupted service for 75K users for 7 hours.

Category 18.1 *Theft of equipment*

1999-04-08 **theft laptop computer components equipment organized crime**

GUARDIAN

In Britain, the _Guardian_ newspaper reported on the professionalization of computer theft — the physical abduction of computers, that is. A Home Office study, called "Pulling the Plug on Computer Theft," reported the following key findings:
* many of the "second-hand" computers for sale through classified ads are stolen;
* total value of stolen computers approached £320M per year in 1996;
* 96% of a sample of 1,048 stolen items recovered by police were computers or computer-related hardware;
* professional gangs find it ridiculously easy to study unsecured targets such as universities and hospitals where there are few barriers to free access;
* any organization that has been burgled is more likely to be attacked again;
* most thefts were burglaries carried out after hours by breaking through minimal barriers, but a few were armed robberies in broad daylight.

Category 18.1 *Theft of equipment*

2000-03-24 **laptop portable computer theft law enforcement intelligence**

RISKS, BBC http://news.bbc.co.uk/hi/english/uk/newsid_688000/688814.stm 20 85

In Britain, an MI5 agent stopped to help someone at an Underground (subway) station and got his laptop stolen. Luckily, the data were encrypted. However, Steve Loughran, writing in RISKS Forum, correctly warned that file-level encryption (e.g., the encrypting file system in Windows 2000) does not necessarily encrypt file names, so some data may be revealed by induction if overly-descriptive file names are used. [An amusing detail for non-British readers was the description of the laptop in the BBC report: "The 2,000-pound laptop was snatched as the agent stopped to help. . . ." which raised eyebrows of those who were thinking of pounds Avoirdupois instead of pounds Sterling.]

Category 18.1 *Theft of equipment*

2000-05-22 **laptop computer stolen secrets confidentiality theft**

RISKS; The Mirror http://www.sundaymirror.co.uk 20 89

In early May, a British Navy intelligence officer lost a laptop computer containing "details of a top secret 250-billion-pound Anglo-US super-lethal stealth Strike fighter project. . . ." The machine was recovered by The Mirror newspaper two weeks later.

Category 18.1 *Theft of equipment*

2000-09-18 **industrial espionage information warfare theft laptop disk encryption user interface**

NewsScan, San Jose Mercury News
http://www.sjmercury.com/svtech/news/breaking/ap/docs/412258l.htm

After addressing a national business journalists' meeting in Irvine, California, Qualcomm chief executive Irvin Jacobs found that someone had stolen his laptop computer, which he left on the floor of a hotel conference room. The thief acquired not only an IBM ThinkPad but also the Qualcomm secrets it contains, because Jacobs had just finished telling the audience that the slide-show presentation he was giving with his laptop contained proprietary information that could be valuable to foreign governments. People in the area "included registrants, exhibitors and guests at our conference, hotel staff and perhaps others." Qualcomm, a leader in the wireless industry, and is the world's leading developer of a technology known as CDMA, which makes high-speed Internet access available on wireless devices. (Reuters/San Jose Mercury News 18 Sep 2000)

In a RISKS commentary on this case, encryption expert Camillo Sars of F-Secure Corporation commented on often-ignored risks from real-time encryption of disk files:
* damage to a block or an entire file from flipping a single bit in the ciphertext;
* loss of the key and therefore of all encrypted data.
Sars ended with the comment, ". . . I second Ross Anderson's view that a paradigm shift is required. Let's not only make systems that are easier to use correctly. Let's make systems that are difficult to use incorrectly."

Category 18.1 *Theft of equipment*

2001-11-14 **laptop computer theft loss airport X-ray scanner inspection confusion label**

NewsScan

PROTECTING LAPTOPS AT AIRPORT SECURITY CHECKPOINTS
Travelers going through airport security checkpoints these days need to take their computer laptops out of their cases and place them separately on the conveyor belts of the airport X-ray machines. To protect the machines from damage, airline experts suggest you take the following steps: request a plastic tub for your laptop before placing it on the conveyor belt; position the laptop in the middle of the belt and behind the carrying case, so that the case can serve as a cushion if the machine slides forward; and tape your name onto the laptop itself, so that it doesn't get confused with other laptops with the same general appearance. (Washington Post 14 Nov 2001)
http://www.washingtonpost.com/wp-dyn/articles/A25015-2001Nov13.html

---

Category 18.1 *Theft of equipment*

2001-11-29 **burglary theft physical security data loss confidentiality industrial espionage financial data insider job**

RISKS 21

In Auckland, New Zealand, sensitive data about the investments of 25,000 investment clients were stolen on magnetic tapes. News reports indicated that only the tapes were taken, with the thieves leaving behind laptop computers and other valuables. Richard A. O'Keefe, reporting to RISKS on this incident, noted, " Without knowing anything about the people involved, or having any expertise beyond that common to all readers of detective stories, I must say that it looks uncommonly like an insider job."

Category 18.1 *Theft of equipment*

2002-08-23 **laptop computer theft loss tracking software Internet**

NewsScan

FIND THAT LAPTOP! NEW TRACKING SOFTWARE FOR NOTEBOOKS
In response to an epidemic of laptop thefts, leading notebook makers IBM, Hewlett-Packard and Dell are offering software with their new machines that enable tracking as soon as their connected to the Internet. IBM, which offers ComputracePlus software from Absolute, says it's seeing growing demand from laptop customers in the education and enterprise markets. Service costs start at $49 for a 12-month license for a single computer. The tracking-agent software imperceptibly connects to Absolute's monitoring center whenever its user connects to the Internet. If the notebook is reported stolen or lost, its location is tracked and local law officials are called in to retrieve it. Although popular, this approach to laptop security does have some weaknesses. "A lot of people steal laptops for commercial espionage -- to get the data that resides on them," says an IDC analyst. "Those people will steal them without ever intending to go online." In other cases, a thief could reformat and configure the hard drive in a way that bypasses the tracking agent. "We'll survive a reformat of the hard drive, but where it gets tricky is when people reinstall operating systems on top of each other," says Absolute CEO John Livingston. Experts say this type of tracking system works best if it is part of a larger theft-prevention strategy that includes cable locks or motion-sensitive alarms. (CNet News.com 22 Aug 2002)
http://news.com.com/2100-1040-954931.html?tag=fd_top

Category 18.1 *Theft of equipment*

2003-01-10 **computer data theft military member information health care records**

NIPC/DHS

January 09, Government Computer News — DOD says system pilot not affected by TriWest thefts.

The December 14 theft of computer equipment containing information on more than 500,000 military members poses no threat to the Composite Health Care System II, the Defense Department's pilot computerized medical system still in development, a Defense health official said yesterday. The computers were stolen from a TriWest Healthcare Alliance office in Phoenix. TriWest provides managed health care to 1.1 million military personnel and their families in 16 states for DOD's health care service, known as the Tricare Management Activity. But Tricare is not part of CHCS II, the official said. "There is no relationship between those two (systems)," said Dr. William Winkenwerder, Jr., assistant secretary of Defense for health affairs. Furthermore, Winkenwerder said, CHCS II information is stored at "very secure sites" and that DOD had implemented steps to increase CHCS II security. CHCS II eventually will store the records of more than 8.5 million military personnel and their families, allowing doctors to retrieve medical histories on their patients. Defense has approved use of CHCS II at seven military hospitals across the country. The thefts at TriWest are still unsolved.

Category 18.1 *Theft of equipment*

2003-04-03 **computer data theft sensitive critical information radioactive waste details**

NIPC/DHS

April 02, Associated Press — Thieves take computers containing details on radioactive material.

Eight state-owned computers containing details on all of the New Mexico companies that use radioactive material have been stolen, officials said Tuesday. The names, addresses and phone numbers of more than 210 businesses are contained in the stolen computers, along with what radioactive materials each is licensed to have, said Bill Floyd, manager of the state Environment Department's Radiation Control Bureau. Thieves took the eight computer towers from the bureau's office in Santa Fe either Thursday night or early Friday. While the files are legally accessible to the public, anyone seeking them would need to do so under the Freedom of Information Act, Floyd said. He said he believed the culprits were seeking the machines themselves — not the data in them.

Category 18.1 *Theft of equipment*

2004-05-03 **NIC physical security theft loss of service**

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1583359,00.asp

May 03, eWeek — Network card theft causes Internet outage.

The theft of network cards from a Verizon central office in New York has caused some customers there to lose their Internet access. A handful of corporate customers were left without e-mail and Internet access Monday, May 3, after the theft of networking equipment from a New York City office Sunday, May 2. Law enforcement officials said four DS-3 cards were reported missing from a Manhattan co-location facility owned by Verizon Communications Inc. The outage affected area customers of Sprint Corp. "We found backup cards in the area," said Charles Fleckenstein, spokesperson for Sprint in Overland Park, KS. "All of the cards are now on site in New York. [They] are being installed at this moment." Service was being restored to customers as the cards were being installed, he said. Sprint officials said other ISPs were affected by the incident, but declined to identify them. Verizon spokesperson Dan Diaz would not identify which providers were affected by the theft of the equipment. Diaz said no Verizon Internet customers were affected by the outage.

Category 18.1 *Theft of equipment*

2004-05-17 **theft telecom physical security**

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1593073,00.asp

May 17, eWEEK — New York theft raises questions.

As of late last week, local and federal investigators were proceeding with their probe into a burglary at a Midtown Manhattan telecommunications office. According to the New York City Police Department, three DS-3 networking cards were stolen May 2 from a New York central office (CO) of Verizon Communications Inc. This CO, also a co-location office housing competing carriers' equipment, is one of the many hubs for the country's voice and data networks and a key component of the nation's critical infrastructure. "Everybody's overly sensitive, with reason, to the issues of terrorism or terrorists trying to sabotage the infrastructure, whether it be the Brooklyn Bridge or the Internet," Joseph Valiquette, spokesperson for the New York FBI Field Office, said about the involvement of the FBI's Joint Terrorism Task Force in the Verizon burglary. The online operations for several New York-based businesses were shut down for almost an entire business day as a result of the Verizon theft.

Category 18.1 *Theft of equipment*

2004-08-05 **hacker theft fraud indictment Romania shipment conspiracy**

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml?artic leID=26806085&tid=13692

August 05, InformationWeek — Hacker indicted on equipment theft charges.

A federal grand jury in Los Angeles on Wednesday, August 4, indicted a Romanian hacker and five Americans on charges that they conspired to steal more than $10 million in computer equipment from Ingram Micro Corp.. The 14-count indictment charges that Calin Mateias, who used the online nickname "Dr. Mengele," hacked into Ingram Micro's ordering system beginning in 1999 and placed fraudulent orders for computer equipment. When Ingram Micro subsequently blocked shipments directed to Romania, he allegedly recruited the co-defendants named in the indictment to provide U.S.-based addresses as mail drops for fraudulently ordered equipment. If convicted, Mateias faces up to 90 years in prison.

Category 18.1 *Theft of equipment*

2005-03-29 **identity data laptop theft University of California Berkeley Social Security Numbers**

EDUPAGE; http://www.insidehighered.com/index.php/news/2005/03/29/theft

THIEF GRABS LAPTOP AND 100,000 IDENTITTIES

Officials at the University of California at Berkeley said that a laptop stolen from the university's graduate division contained personal information for nearly 100,000 individuals. The computer included records for applicants to Berkeley's graduate programs from fall 2001 to spring 2004; students enrolled in the school's graduate programs from fall 1989 to fall 2003; and individuals who received doctorates from Berkeley between 1976 and 1999. Although no evidence exists that any of the stolen information has been used fraudulently, according to a statement from the university, the institution is required by a California law to disclose the breach to those affected. The statement said the university is making "every reasonable effort to notify by mail or e-mail all 98,369 individuals whose names and Social Security numbers were on the computer." Inside Higher Ed, 29 March 2005

Category 18.1 *Theft of equipment*

2005-03-29 **Social Security Numbers SSN laptop computer data theft reporting law awareness alert thief university students alumni**

RISKS 23 82

UNINTENDED CONSEQUENCES OF CALIFORNIA DATA-THEFT REPORTING LAW

A laptop computer containing names, SSNs, and some addresses and birthdates for 98,369 alumni, grad students and applicants was stolen from an office at UC Berkeley. In compliance with California's new data-theft reporting law, the breach was reported and has now been widely publicized -- although ironically, as a writeup on slashdot points out, this publicity may have alerted the thief, who was probably only interested in the hardware, to the true value of his find.

[Summary and analysis posted in RISKS by Steve Summit]

Category 18.1 *Theft of equipment*

2005-04-08 **stolen computers medical records California Security Breach Information Act law encryption confidentiality HIPAA**

SANS NewsBites; http://news.zdnet.com/2102-1009_22-5660514.html?tag=printthis

STOLEN COMPUTERS CONTAIN 185,000 PEOPLE'S MEDICAL RECORDS

Two computers containing the financial and medical records of nearly 185,000 current and former patients were stolen from the offices of the San Jose Medical group late last month. The group's vice president for information technology says he believes the thieves were interested in the computers and not the information they contained. Nonetheless, the affected patients are being notified pursuant to California's Security Breach Information Act. The company had been transferring patient data from secured servers to the PCs; some of the data were encrypted.

Category 18.1 *Theft of equipment*

2005-05-23 **data personal information theft MCI employee data Social Security Numbers**

EDUPAGE; http://online.wsj.com/article/0,,SB111680003245940129,00.html

LATEST LOSS OF PERSONAL INFORMATION: MCI

Officials from long-distance carrier MCI are investigating the loss of employee data after a laptop was stolen from the car of an MCI financial analyst. The laptop contained names and Social Security numbers for about 16,500 employees, whom the company has notified. A spokesperson for MCI said the machine was password-protected but did not say whether the employee data were encrypted. MCI is reviewing the incident to see whether the analyst violated any company policies, such as those concerning what types of information may be put on laptops and what information must be encrypted. MCI is also taking this opportunity to make sure employees who have access to sensitive information are clear on company policies. The company said that so far there have been no reports that any of the information on the laptop has been sold or misused. Wall Street Journal, 23 May 2005 (sub. req'd)

Category 18.1 *Theft of equipment*

2005-06-10 **data theft personal information disclosure Motorola Affiliated Computer Services fraud insurance offer**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=8760748

MOTOROLA EMPLOYEE DATA STOLEN

Over the Memorial Day weekend, thieves broke into the offices of Affiliated Computer Services (ACS), a provider of human resources services, and stole two computers with personal information on Motorola employees. The computers, which reportedly employed security measures to make accessing their files difficult, contained names and Social Security numbers of an unspecified number of employees but did not include any financial information, according to a Motorola spokesperson. Lesley Pool, chief marketing officer at ACS, described the theft as an "amateur burglary" and said no evidence has surfaced that any of the information has been used for illicit purposes. Most of those affected are U.S. employees of Motorola, which employs about 34,000 people in the United States. Motorola has notified all of the affected employees and offered them fraud insurance at no charge. Reuters, 10 June 2005

Category 18.1 *Theft of equipment*

2006-01-26 **Ameriprise laptop personal data theft Social Security numbers**

EDUPAGE; http://www.nytimes.com/2006/01/25/business/25cnd-data.html 23

AMERIPRISE LAPTOP WITH PERSONAL DATA STOLEN

A laptop containing information on 230,000 individuals was stolen from the car of an employee of Ameriprise Financial in December, according to the company. The computer included names and Social Security numbers for more than 70,000 financial advisors, and names and Ameriprise account numbers for 158,000 customers of the firm, which was spun off of American Express last year. Andy MacMillan, a spokesperson from the company, said that although access to the data is protected by a password, the data were not encrypted, which is a violation of written company policies. MacMillan said the company does not believe that the thief knew about the information contained on the laptop and thinks that it is unlikely any of the information will be accessed or used fraudulently.

Category 18.1 *Theft of equipment*

2006-01-29 **stolen laptop personal data leakage confidentiality control employees customers unencrypted disk**

RISKS; NYT; http://tinyurl.com/rgh5t 24 15

AMERIPRISE LAPTOP COMPUTER STOLEN WITH DATA ABOUT 230,000 CUSTOMERS & EMPLOYEES

A report mirrored on emergentchaos.com summarized another data loss through unencrypted disks on a stolen laptop:

>On Wednesday, Ameriprise Financial, an investment advisor firm, said that a company laptop stolen from an employee's parked car in December contained the personal information of some 230,000 customers and company advisors, The New York Times reports.

The sensitive information contained in the laptop included the names and Social Security numbers of roughly 70,000 current and former financial advisors, as well as the names and internal account numbers of about 158,000 customers.

Andrew MacMillan, Ameriprise spokesperson, said the culprits likely had no idea that the laptop contained sensitive information, and in turn, the potential risk of "any data being used or discovered is very low." MacMillan noted that the laptop was protected by a password, but the data was not encrypted, a blatant breach of the company's privacy regulations. Ameriprise has fired the employee involved.<

[MK comments:
1) Firing the employee seems like an empty response to the problem, which is that corporate computers were being issued without mandatory disk encryption;
2) Having a company spokesperson announce to the world that the crooks "likely had no idea that the laptop contained sensitive information" is an inherently self-defeating form of reassurance.]

Category 18.1 *Theft of equipment*

2006-05-22 **computer laptop theft confidentiality control unencrypted hard drive policy violation information warfare terrorism**

RISKS; ConsumerAffairs.Com http://tinyurl.com/loluu; USA Today http://tinyurl.com/mwugq 24 29

VAST DATA CACHE ABOUT VETERANS HAS BEEN STOLEN

Personal electronic information on up to 26.5 million military veterans, including their names, Social Security numbers, and birth dates, was stolen from the residence of a Department of Veterans Affairs employee who had taken the data home without authorization. …Comments about no evidence of data misuse (yet) and no health/financial records, but deeply embarrassing to VA. No mention of a statement that this incident was not reported for several weeks….

[Abstract by Peter G. Neumann]

Martin Bosworth, writing for ConsumerAffairs.Com, wrote "In every public case, company representatives insist the laptops are stolen simply for their resale value, as opposed to the data they contain. The more skeptical might say that as consumers get smarter about not sharing their information on the Web, enterprising hackers and data thieves are taking advantage of other holes in the security fence -- namely slipshod government and business policies. Whether it's a criminal conspiracy or good old-fashioned incompetence, public and private agencies are not adequately protecting the personal information that's entrusted to them and, in many cases, are less than forthcoming about the circumstances surrounding laptop losses."

The FirstGov.gov Web portal included an extensive Web page entitled "Latest Information on Veterans Affairs Data Security" at < http://www.firstgov.gov/veteransinfo.shtml >.

In early June, the VA revealed that the stolen data included information about 2.2 million active-duty military personnel and National Guard troops. According to an Associated Press report, a class-action lawsuit filed by a coaltion of veterans' groups demanded "that the VA fully disclose which military personnel are affected by the data theft and [sought] $1,000 in damages for each person — up to $26.5 billion total. The veterans are also seeking a court order barring VA employees from using sensitive data until independent experts determine proper safeguards." The complaint added, "VA arrogantly compounded its disregard for veterans' privacy rights by recklessly failing to make even the most rudimentary effort to safeguard this trove of the personally identifiable information from unauthorized disclosure."

Category 18.1 *Theft of equipment*

2006-06-02 **laptop computer stolen unencrypted disk drive confidentiality data leakage control credit-card numbers**

RISKS 24 31

HOTELS.COM LOSES CONTROL OF 243,00 CREDIT-CARD NUMBERS

CNNMoney reports that about 243,000 Hotels.com credit-card numbers were stolen back in February via the theft of a laptop computer. They believe that the theft was of the computer, with no idea of the information on the hard drive, and, likely as well, no intention of using the information on the hard drive. That it takes from February to June to determine what was on the hard drive is difficult to accept, however, and leaves unanswered what MIGHT have happened in the intervening three months respecting identity theft or misuse of the credit cards. Lots of unanswered questions, but typical of the problem when a laptop gets stolen.

[Abstract by Robert Heuman]

18.2 Loss of equipment

Category 18.2 Loss of equipment

2002-08-16 **laptop computer losses internal controls policies**

NewsScan

DETAILS, DETAILS: IRS LOSES COMPUTERS (EXACT NUMBER UNKNOWN)
An Inspector General's report has concluded that the Internal Revenue Service has lost (or had stolen) some unspecified number of personal computers that had been lent to volunteers who were assisting low-income, disabled, and senior citizens prepare their tax returns. IRS critic Sen. Charles E. Grassley (R-Iowa) wrote in a letter to the federal Office of Management and Budget: "I'm worried that just as clothes dryers have the knack of making socks disappear, the federal government has discovered a core competency of losing computers." An IRS spokeswoman said that the agency has been working "for some time" to improve its internal controls over the computers it lends to volunteers, and "will continue" to do so. (Washington Post 16 Aug 2002)

Category 18.2 Loss of equipment

2003-10-16 **top data loss disasters**

NewsScan

TOP 10 DATA DISASTERS
Although machine failure is at fault for the majority of lost data disasters, humans are increasingly culpable as well, according to recovery experts at Kroll Ontrack. "Despite being the easiest problem to prevent, we are seeing more cases where human error is to blame. Interestingly, we see a 15 to 20% increase in calls to recover lost data on Mondays. This could be a result of the rush to complete work and leave early for the weekend on Friday afternoons, as well as a lack of staff concentration on Monday mornings," says a Kroll spokesman. The Top 10 list of unusual data loss stories includes laptops being shot or thrown against the wall in a fit of e-rage; laptops suffering spills of red wine or latte because users were "drinking on the job," laptops falling off mopeds or car roofs, then being crushed by oncoming traffic; and PCs being thrown out a window or into a river to destroy evidence of theft or fraud. Our favorite? The laptop that slipped into the bathtub with its owner while he was working on accounts. Amazingly, Kroll Ontrack says in all these cases, it was able to rescue and restore computer files. (BBC News 16 Oct 2003)

Category 18.2 Loss of equipment

2004-05-04 **hackers theft damage data loss Taiwan**

DHS IAIP Daily;
http://www.chinapost.com.tw/taiwan/detail.asp?ID=48429&GRP=B

May 04, The China Post — Hackers cause almost one million dollar loss for banks, CIB reveals.

Hackers have invaded the computer systems of over 700 Taiwan companies and caused losses of more than USD$900,000 for banks with electronic financial services, according to an initial estimate by the Criminal Investigation Bureau (CIB). In the field of computer hacking, CIB officials said mainland China is the major source of hackers targeting Taiwan with the aim of stealing commercial secrets, technical know-how, and computer systems of government agencies in charge of military, transport, public security, and finance affairs. Other sources include the United States, Japan, and South Korea. Officials said the hackers normally implant malicious programs in the form of "Trojan Horse" viruses onto the less guarded Internet operating systems of educational institutions like schools. The virus and software programs then wait for opportunities to enter the systems of other organizations with more stringent security. Companies suffering from the attacks include information service companies, high-tech firms, enterprises in the traditional manufacturing industries, and banks with Internet services. The dozens of banks reported that over USD$600,000 million was lost in the electronic fund transfer process.

Category 18.2 *Loss of equipment*

2005-01-24 **laptops cell phones equipment loss taxis cabs data confidentiality possession control**

NewsScan;
http://www.cnn.com/2005/TECH/ptech/01/24/taxis.lost.reut/index.html

THOUSANDS OF LAPTOPS, CELL PHONES LEFT IN CABS

A new survey estimates that 11,300 laptops, 31,400 handheld devices and 200,000 mobile phones were left in taxis around the world during the last six months. The survey, which polled some 1,000 taxi drivers and extrapolated from there, indicates that four out of five cell phones and 19 out of 20 laptops were returned to their owners eventually. Geographically, Chicagoans were most likely to leave a handheld device in a cab, while Londoners were more careless than others with their laptops. Danes seemed to be most likely to forget their cell phones. Other items reportedly left in cabs include a harp, dentures, artificial limbs and a baby. (Reuters/CNN.com 24 Jan 2005)

Category 18.2 *Loss of equipment*

2005-02-25 **unencrypted data laptop computer loss confidentiality medical information blood bank**

RISKS 23 76

BLOOD BANK LAPTOP FALLS OFF TRUCK; DATA UNENCRYPTED

Delaware blood bank had sensitive donor data on disk; "Officials say they will now encrypt the information to prevent its unauthorized use or disclosure."

Category 18.2 *Loss of equipment*

2005-02-26 **bank data loss tapes Visa credit cards expenses governmental Defense Department information theft**

EDUPAGE; http://www.nytimes.com/2005/02/26/national/26data.html

BANK LOSES SENSITIVE DATA

The Bank of America has lost backup tapes containing details of Visa cards that the bank issued to 1.2 million federal employees, who use the credit cards for travel expenses and other purchases related to government business. About 900,000 of those affected work in the Defense Department, according to Alexandra Trower, a spokesperson from the bank. Trower said that following a shipment of a number of such backup tapes, it was discovered that some were missing. The Secret Service was notified and is investigating the disappearance, but according to Trower, no evidence has surfaced that any of the lost information has been put to improper use or that the loss resulted from theft. The bank does not plan to change any of the affected credit card numbers, but it has notified those individuals whose information was included on the missing tapes.

Category 18.2 *Loss of equipment*

2005-05-02 **data leakage loss backup tapes personal information employees history Social Security Numbers (SSN)**

RISKS; http://tinyurl.com/cfgfm; http://tinyurl.com/9e86u; http://tinyurl.com/7ejo3 23 86

IRON MOUNTAIN LOSES BACKUP TAPES IN FOURTH INCIDENT THIS YEAR

Peter G. Neumann reported another serious data loss:

Time Warner Inc. Data on 600,000 current and former employees stored on computer backup tapes was lost by an outside storage company. The Secret Service is now investigating. The tapes included names and Social Security information on current and former Time Warner employees, dependents, and beneficiaries, back to 1986.

In addition, the *Wall Street Journal*, 3 May 2005, noted that the tapes were lost by Iron Mountain Inc., a data-storage company based in Boston. An Iron Mountain spokeswoman said this is the fourth time this year that Iron Mountain has lost tapes during delivery to a storage facility.

Category 18.2 *Loss of equipment*

2005-05-07 **physical security data leakage equipment loss computers disk drives national laboratory sloppy procedures errors flaws mess national security**

RISKS 23 87

US IDAHO NATIONAL LAB LOSES 269 COMPUTERS & DISK DRIVES IN 3 YEARS

The U.S. federal Idaho National Laboratory nuclear-reactor research lab cannot account for more than 200 missing computers and disk drives that may have contained sensitive information. The computers were among 998 items costing $2.2 million dollars that came up missing over the past three years. Lab officials told investigators that none of the 269 missing computers and disk drives had been authorized to process classified information. But they acknowledged there was a possibility the devices contained "export controlled" information -- data about nuclear technologies applicable to both civilian and military use. [Abstract by Peter G. Neumann]

Category 18.2 *Loss of equipment*

2005-07-12 **data leakage computer loss theft government agencies UK survey report**

RISKS; http://www.egovmonitor.com/node/1843 23 94

UK GOVERNMENT LOSES AT LEAST 150 COMPUTERS IN 1ST 6 MONTHS OF 2005

Central government departments have reported to have suffered at least 150 cases of computer theft in the last six months, according to official figures. The Home Office alone recorded 95 incidents of computer items being stolen between January and June 2005 - equivalent to a theft taking place in the Department every other day.

By comparison, the Ministry of Defence reported 23 computer thefts to date in 2005, down from a total of 153 in the previous year….

In a written answer, Doug Touhig, a junior minister at the MoD, said the Ministry had also experienced 30 attempted computer hacking incidents so far in 2005, having only reported 36 for the whole of 2004. However the Minister gave an assurance that "none of the reported incidents of hacking had any operational impact". Most of these incidents were due to internal security breaches, rather than external threats. Half of the cases were classed as "internal - misuse of resources".

Instances of reported computer thefts in other departments were in single figures so far this year, and most recorded no cases of IT systems being accessed illegally.

The Department for Transport said it had experienced 71 cases of computer hacking in 2003-4, 31 in the following year and one incident since April. The Treasury, the Department for International Development and the Department for Education and Skills said their IT systems had been breached on one occasion in 2004-5. Figures from the DfES show that in the two years since 2003/4, it experienced 37 incidents of computer theft, all but one of which were "perpetrated by insiders". The Department of Health said it did not distinguish between losses and theft of IT equipment, but said there were 44 such incidents in 2004-5, costing it almost 40,000 pounds. Figures provided by Health Minister Jane Kennedy put the total sum lost by the Department over the last four years at 233,000 pounds.

[Report by Ian Cuddy]

Category 18.2 *Loss of equipment*

2006-02-24 **data loss confidentiality control unencrypted backup CD-ROM**

RISKS; News.com http://tinyurl.com/ozh5x 24 17

AUDITOR LOSES CD-ROM WITH McAFEE EMPLOYEE DATA

Jeremy Epstein wrote the following summary of YADL (Yet Another Data Loss):

It was widely reported that the names, SSNs, and other personal information for 6000 current & former McAfee employees were potentially compromised. An auditor from Deloitte had the information on an unlabeled (but unencrypted) CD that was left in an airplane seatback pocket. It's unknown whether the CD simply went in the trash as part of airplane cleaning, or whether someone picked it up. McAfee is offering employees and ex-employees two years worth of credit monitoring through Experian.

The really interesting part (which I saw in the *San Jose Mercury* article, but not elsewhere) is that the auditor "had made the CD for backup purposes, and it was their decision not to encrypt the data." McAfee's spokesperson aid they have policies to prevent such actions, but they can't control what the auditor does with the data.

So if McAfee didn't have policies in place to prevent storing sensitive data in an unencrypted form (and/or to safeguard the media), Deloitte would have flunked them on their Sarbanes-Oxley audit. But because it was Deloitte who did the dirty deed, it looks like no one will be held accountable. One hopes that the Deloitte employee who made the CD is now a former employee.

Category 18.2 *Loss of equipment*

2006-02-24 **McAfee auditor employee data loss leakage no encryption**

EDUPAGE; http://www.siliconvalley.com/mld/siliconvalley/13952271.htm 23

MCAFEE AUDITOR LOSES EMPLOYEE DATA

Deloitte and Touche, the external auditor of computer-security firm McAfee, has lost a CD containing unencrypted data on more than 9,000 McAfee employees. The CD was left in a seat pocket on an airliner on December 15, though the loss was not reported to Deloitte officials until January 8, and it took until January 30 to determine what was on the disk. A spokesperson for McAfee, Siobhan MacDermott, said auditors commonly have access to the kind of data that was on the CD and that the decision not to encrypt the data was Deloitte's. MacDermott said, "We have policies in place to prevent this from happening" and noted that McAfee and Deloitte are working to prevent such a loss from happening again. Ken McEldowney, executive director of Consumer Action, expressed dismay at the news. "How hard would it be to encrypt the data?" he said. "How hard would it be to make sure important information like that is not on CDs that are not under tight control by the company?"

Category 18.2 *Loss of equipment*

2006-02-25 **laptop computer thefts losses compromise customer employee financial tax data identity theft passwords SSN**

The Register < http://www.theregister.co.uk/2006/03/30/ey_nokia_lapop/ >

ERNST & YOUNG LOSES LAPTOP COMPUTER WITH CUSTOMER DATA

The international consulting firm Ernst & Young lost a series of laptop computers in 2006. In February, the firm admitted that a laptop with confidential customer data -- including the SSN of Scott McNealy, CEO of Sun Microsystems -- had been lost or stolen in January. McNealy reported that his identity had in fact been compromised.

Then a March report in the Miami Herald stated that some Ernst & Young auditors went to lunch on Feb 9 -- leaving their laptop computers in a conference room in the office building where they were working. Two men stole four laptops. E&Y declined to issue a public statement about these breaches of security, although they did assure the public that "password protection" sufficed to compensate for loss of control over the data.

On March 15, The Register's Ashlee Vance, indomitable reporter that she is, wrote that E&Y lost yet another laptop computer -- this one stolen in January from an employee's car. It contained financial and tax records compromising the security of "thousands" of IBM employees and ex-employees. Once again, the company refused to issue a public statement about the theft and informed the potential victims of identity theft two months after the incident. On March 23, Vance found out that E&Y had admitted to BP that 38,000 employees were included in the January laptop theft.

Category 18.2 *Loss of equipment*

2006-03-22 **laptop computer thefts losses compromise customer employee financial tax data identity theft encryption SSN**

The Register < http://www.theregister.co.uk/2006/03/22/fidelity_laptop_hp/ >

FIDELITY INVESTMENTS LOSES LAPTOP WITH CLIENT DATA

Ashlee Vance, scourge of careless laptop users, reported on March 22 in The Register that Fidelity Investments had announced the loss of a laptop computer containing detailed HP retirement plan data for 196,000 HP employees, including names, addresses, salaries and SSNs. In contrast with the disgraceful performance of Ernst & Young, Fidelity announced the loss relatively quickly and cooperated fully with the trade press. In addition, the data on the laptop were encrypted.

The same article reported that Ernst & Young were rolling out encryption software for their corporate computers. At last.

On 24 March, Vance reported that the _reason_ a Fidelity employee was carrying 196,000 records about HP employees on a laptop was… wait for it… as part of a demo intended to impress HP executives with some new software. Yep: live, highly sensitive data for a demo on a laptop computer.

Category 18.2 *Loss of equipment*

2006-05-12 **data loss computer sensitive data confidentiality SSN financial information**

The Register <
http://www.theregister.co.uk/2006/05/12/wellsfargo_computer_loss/ >

WELLS FARGO LOSES COMPUTER WITH SENSITIVE CUSTOMER DATA

Ashlee Vance, writing in The Register, reported that
>At least one poor Hewlett Packard employee compromised by Fidelity's March laptop loss has now been told Wells Fargo lost his personal data, too.

The staffer received a note this week from Wells Fargo, saying the financial institution had lost a computer packed full of sensitive data such as customers' names, addresses, Social Security numbers and Wells Fargo mortgage loan account numbers, according to a document sent to The Register. Wells Fargo has admitted the loss, telling us that it affected a "relatively small percentage of Wells Fargo customers." The company, however, has millions of customers, so it's pretty tough to tell what a "small percentage" means.

The company said that, "a computer - being transported for Wells Fargo Home Mortgage, a division of Wells Fargo Bank, N.A., by a global express shipping company between Wells Fargo facilities - has been reported as missing and may have been stolen. Wells Fargo said there is no indication that the information on the computer equipment has been accessed or misused. The computer has two layers of security, making it difficult to access the information."<

---

19 Counterfeits, forgery (including commercial software/music piracy)

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

1997-02-17 **Forgery**

RISKS 18 83

Robert Ames, victim of attacks on his reputation by forged, offensive USENET postings, found the fraudulent messages archived on DejaNews even though he had repudiated the forgeries using PGP-signed messages.

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

1997-03-09 **Chin**

EDUPAGE, COMPTEX

In Monterey Park, CA, two Chinese nationals were raided by police; their company had 23,000 counterfeits of Windows 95 software. In July, 43-year-old Zhijian Song and 38-year-old Jian Ping Zhu pleaded no contest to the charges of counterfeiting and were sentenced to 16 months in prison.

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

1997-03-26 **forgery**

RISKS 18 94

A convict was released from prison when his girlfriend sent in a pardon ostensibly from the PA governor. The same pair then tried to free the runaway's cell-mate using a forged fax claiming to be from the governor of FL. Luckily, someone checked with the governor's office before releasing the prisoner.

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

1997-08-05 **forgery spam denial of service harassment fraud e-mail porn**

C|Net news.comhttp://www.news.com/News/Item/0,4,13141,00.html

An innocent Florida businessman, Bruce Hovland, was harassed by thousands of phone calls from angry strangers who complained about junk e-mail that threatened to bill their credit cards for almost $200 in return for pornographic videos they had never ordered and did not want. Mr Hovland was the victim of a deliberate smear campaign, probably by a creep who had refused to pay rent at his marina and lost his boat as a result. The malefactor spammed the net in Hovland's name and suggested that people call his business number collect. Hovland guesses that he lost about two weeks of business because his phones were ringing off the hook. Hovland points out that his case was relatively minor; he imagines the mayhem if an emergency number were posted on the Net in such a fraud. The case illustrates the difficulty for victims in finding an agency willing to receive and follow up on complaints about such outrageous and dangerous attacks.

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

1997-08-10 **hoax rumor myth**

EDUPAGE, AP

A minor storm erupted in August when Kurt Vonnegut was credited with a clever commencement address at MIT; unfortunately, the "address" was a pirated version of a column by March Smich of the Chicago Tribune.

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

1997-08-19 **counterfeit color printers**

EDUPAGE

According to the Secret Service and the U.S. Department of the Treasury, kids have been trying to counterfeit money using PCs and color printers and copiers. Authorities are trying to get the word out to "these knucklhead kids" that counterfeiting is a serious offense, with sentences of up to 15 years in federal prison.

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

1997-08-20 **spam fraud hoax impersonation**

RISKS, Newsbytes 19 32

Someone sent an offensive e-mail message throughout the Net ostensibly from Samsung America's legal counsel. The e-mail caused a fuss, with many victims announcing that they would no longer buy from Samsung. Investigation showed that the e-mail contained forged, fraudulent headers and that Samsung and their lawyers had nothing to do with the hoax. Moral: if a professional is sending e-mail that makes it look like they have lost their senses, the message may very well be fraudulent.

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

1997-08-25 **fraud counterfeit components chips memory**

Computer Reseller News

Resellers with a sharp eye noticed funny-looking memory chips on some of the boards coming in from low-end manufacturers. Turned out the "memory chips" were dummies that were not even connected to the rest of the board. Resellers began using a test program called WhatMem from Data Depot, in Clearwater, FL. The scam died down as memory prices dropped, but resellers are still advised to run occasional quality control checks on their components.

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

1997-10-28 **fraud forgery cheating universities**

EDUPAGE

Boston University invited other universities to join its lawsuit against eight term-paper mills selling student papers over the Internet. According to EDUPAGE, the university accused the companies of "wire fraud, mail fraud, racketeering, and violating a Massachusetts law prohibiting the sale of term papers." The plaintiff dismissed claims that disclaimers advertising the papers as "research tools only" are a sham.

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

1998-01-06 **bank debit card fraud counterfeit forgery**

RISKS 19 53

Burns National Bank of Durango, CO cancelled its debit-card program because of technical problems with security. Unspecified weaknesses in the design allowed The Bad Guys to make counterfeit debit cards. Losses reached about $300K before the cards were withdrawn.

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

1998-01-29 **plagiarism forgerny**

EDUPAGE

A researcher using automated textual-analysis tools on the National Library of Medicine's online PubMed system found strong evidence of plagiarism to support accusations against a Polish engineer who claimed to have written 125 articles. A total of 59 of these seem to have been pirated. Plagiarists who publish their works online should be trembling in their stolen boots.

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

1998-03-29 **copyright fraud theft video software culture enforcement**

EDUPAGE

COPYRIGHT SITUATION IN CHINA

Pirated videodisks of the movie "Titanic" were available throughout China last November, a month before its release in U.S. theaters, and about half a million pirated disks are smuggled into China every day from Macao. Chinese officials say there is little they can do about this blatant violation of the intellectual property rights agreement that China reached with the United States in 1995. One official explains: "The profits are so great, they will take any risk. They're like drug dealers. It is very difficult to arrange a crackdown. You have to coordinate all these different departments, the copyright publication department, the police, the Industrial and Commercial Administration. We take copyright violations very seriously. But when it comes to copying a disk, most Chinese people don't see what's wrong." And one merchant who sells pirated material insists: "There's nothing wrong with selling pirated VCDs. My son loves watching them." (New York Times 28 Mar 98)

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

1998-04-28 **shoulder surfing debit cards PIN camera retail bribery**

RISKS 19 70

In Newmarket, Ontario (near Toronto), thieves in cahoots with a gas-station employee installed a miniature camera focused on the debit-card PIN pad. Videos of customers punching in their PINs, coupled with account information provided by the criminal employee sufficed to let the gang create fake debit cards to pillage accounts. The criminals got into the habit of visiting ATMs at midnight so they could steal two days' worth of maximum withdrawals. Police reported total thefts in the hundreds of thousands of dollars. The criminals were arrested just before a planned expansion to five more gas stations.

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

1998-05-07 **forged Pentium processor chips clock speed counterfeit**

RISKS 19 72

Some department stores are selling computers with overclocked mother boards and slower processors than what they claim they're selling. Clues include evidence of tampering on the mother boards. Be sure to check the characteristics of your purchase using an adequate diagnostic tool such as Norton's Nuts & Bolts [this is not an endorsement by ICSA, merely an example].

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

1998-05-21 **forgery hologram European currency theft**

EDUPAGE

A hologram intended to deter counterfeiters was lost or stolen in transit from Paris to Munich. The European Union may have to change the design of its high-denomination currency as a consequence. This case illustrates the security principle that human failings are usually a more important vulnerability than technological weaknesses.

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

1998-06-21 **software piracy copyright intellectual property lawsuits**

EDUPAGE

The Business Software Alliance and the Software Publishers Association reported that the US software industry lost $11.4B in lost sales because of national and international software piracy. The organizations vowed to crack down publicly on violators, abandoning their long-standing practice of discretely coming to settlement agreements with companies that deliberately flout the law. Current estimates of piracy rates are 27% in the US and 50% in Europe — both significant improvements. Asia still leads the world in illegal copying, though, with rates mostly above 90% and reaching as high as 98% in China.

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

1998-08-13 **software copying piracy copyright intellectual property**

EDUPAGE

It is a commonplace that schools are among the worst violators of copyright law in the US and Canada. Educators often blithely assume that they have implicit dispensation from restrictions on copying. One of the most significant cases of the year occurred when the Business Software Alliance audited the Los Angeles Unified School District and found 1400 illegal copies of proprietary software in a single school in the District. Total costs of replacing illegal software throughout the District may reach $5M.

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

1998-08-19 **debit-card fraud credit unions account number generator**

RISKS 19 93

The Transportation Federal Credit Union was robbed of over $1M by Asian crime groups which developed algorithms for generating valid debit-card numbers (with a success rate of about 50%). The fake cards were then used to extract money from the victimized accounts. Unfortunately, a software error at the Union precluded verification of the encrypted checksums on the cards' magnetic strips.

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

1998-09-01 **software copyright piracy international marketing culture**

EDUPAGE

Microsoft paid for a new CD produced in Hong-Kong with songs urging its listeners to stop copying proprietary software without a license. There were no indications that the songs would be turned into a rock video.

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

1998-10-13 **bank card forgery PIN reader ATM**

RISKS 20 3

In Finland, high-tech thieves installed a "small black card reader" on top of the regular slot for inserting debit and credit cards in an ATM. With the codes from their extra card reader plus some standard shoulder-surfing to garner PINs, the thieves were able to create 60 counterfeit cards and stole the equivalent of U$36,600.

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

1998-10-28 **forgery prison documents spoof release escape mail**

UPI

In yet another prison-escape forgery case, Tonya Hager pleaded guilty to having sent forged papers authorizing the release from prison of her friend Thurman Green. She used official county stationery and official-looking time stamps and signatures. When prison officials tried to verify the authenticity of the forged documents, their mail was intercepted (the guilty woman promises to help explain what happened) and they received a second forged document.

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

1998-12-15 **fraud forgery scanner printer color counterfeit currency**

UPI

A father and his teenaged daughter were arrested in Michigan in mid-December after allegedly using a scanner, computer, and color printer to create counterfeit U$20 bills and spending $2,800 of the fake money on Christmas presents. Donald Gill of Fairgrove, MI was held in jail pending Federal felony charges. His 17-year-old girl was released on bail and charged under state laws (minors are not subject to federal felony laws).

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

1999-02-15 **software piracy theft copyright infringement copy CD-ROM**

San Jose Mercury News

In Beijing, a court ordered two software pirates to compensate Microsoft for stealing their software and making illegal copies. This was the first case in which the Chinese justice system condemned miscreants for violations of intellectual property rights.

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

1999-02-16 **credit card counterfeit fraud organized crime Asian Triads**

PA News

According to the British National Criminal Intelligence Service, the explosion in credit-card counterfeiting and other credit fraud is largely due to increased activity by Asian Triads. Losses grew by 500% between 1991 and 1998, with total theft estimated at £25M in the UK in 1998.

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

1999-02-19 **counterfeit pirated copies intellectual property copyright violation organized crime CD software music video**

AP

According to investigative reporter Nicolas B. Tatro writing for AP, Israel is a hotbed of counterfeiting and supplies large numbers of pirated CDs with stolen software distributed with the help of Palestinian criminal organizations in the West Bank. Uncollected royalties may amount to $170M a year to US copyright holders. Other counterfeit products include millions of audio cassettes selling for a fraction of the legal cost. Some Israeli musicians are withholding new music, hoping to pressure their government into cracking down on the pirates. The Israeli government announced plans to increase the severity of sanctions against copyright infringement and created a new 10-member police team to attack the problem.

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

1999-02-23 **software piracy theft copyright infringement illegal copying**

UPI

According to a study by Microsoft Corp., software piracy in Virginia alone in 1997 caused the loss of nearly 5,000 jobs and more than $900 million in combined wages, tax revenues and retail sales.

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

1999-03-25 **lawsuit intellectual property music copyright infringement**

Financial Times

The Norwegian company FAST makes software that can download MP3 files. The International Federation of the Phonographic Industry (IFPI) lodged a complaint that resulted in criminal prosecution of FAST for facilitating the theft of illegally posted copyrighted music from the Web. The IFPI was also contemplating a complaint against Lycos, whose search engine catalogs these illegal snippets of intellectual property.

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

1999-04-29 **software theft copyright intellectual property piracy**

AP via OTC

Microsoft sued 15 Florida counterfeiters who sold copies of Windows 95 and Windows 98 without authorization. According to a study from International Planning & Research Corp., a market research company commissioned by Microsoft, software piracy cost Florida 7,186 jobs in 1997 and $490 million in lost wages, tax revenue and retail sales.

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

1999-04-30 **software piracy intellectual property theft misappropriation costs**

San Jose Mercury News

According to Bradford Smith of Microsoft, his company alone has lost more than $6B due to Chinese and other software piracy. Colleen Pouliot of Adobe estimated that 40% of all business applications are used without permission — a staggeringly damaging depression of the industry's production.

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

1999-10-04 **theft piracy counterfeit intellectual property contraband Internet Web upload download software music copyright violations**

Reuters

Jim Loney wrote a summary for Reuters news wire of the losses due to piracy of intellectual property and counterfeiting. Some key points:
* US Customs Commissioner Bonni Tischler predicted that copyright violations and counterfeiting was "going to dwarf every type of crime in the next millennium."
* U.S. companies have estimated they lose $200B a year to product piracy involving designer clothes, shoes, handbags, software, CDs and videos.
* World-wide, software piracy costs industry $11B a year.
* 38% of the 615M new software product installations were illegal copies.
* 97% of all the software in Vietnam was stolen.
* 90%+ of all software was stolen in Bulgaria, China, Indonesia, Lebanon, Oman, and Russia.
* 60% of the software being sold by auction on the Net is illegitimate.
* Criminals are setting up shop in jurisdictions with no cyberspace laws or lax law enforcement (such as Russia) and selling stolen property all over the world.
Loney concludes, "Customs officials say judicial systems lag behind exploding crime on the Internet. Cybercrime is difficult for juries to visualize, penalties are small and the risk of jail is minimal in comparison to crimes like armed robbery."

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

1999-11-30 **ATM automated teller machines fraud forgery confidentiality fake cards convictions**

DAILY TELEGRAPH

Two criminals in a British "hole-in-the-wall" gang were convicted of fraud and theft in Middlesex Crown Court at the end of November. The gang specialized in adding equipment to automatic banking machines to record card numbers and PINs. They would then manufacture forged cards and withdraw small amounts from each card, often thereby evading the notice of their victims; total thefts were estimated to be in the millions of pounds. According to British police, all the major banks had been victimized. The ringleaders of the scam remained at large.

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

1999-12-01 **ATM automated teller machines counterfeit cards fraud international**

MOSCOW TIMES

In October 1998, reports surfaced of organized data theft from banks in Moscow, where unsuspecting users of automated teller machines (ATMs) were the victims of a crime ring that used their stolen card information and PINs to create counterfeit cards that were then used for unauthorized withdrawals in several European cities. Both VISA and Europay accounts were charged; the companies have stated or implied that their Russian agency, Union Card of Moscow, was heavily involved in the fraud. The first arrests occurred in March 1999, when four Kazakh nationals were arrested in Munich with counterfeit cards at an ATM; they were convicted of organized credit card forgery and sentenced to up to 4 1/2 years in jail. Other arrests in the case were made throughout 1999 in Stockholm, Paris and London. The London arrest of Krister Elgsgem, a 32 year old Swedish man, occurred by chance in late November; an off-duty policeman was in line immediately behind the criminal as he fed about 50 obviously counterfeit (white, without logo) bank cards into an ATM. Russian police authorities have issued no statements about their investigation.

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

1999-12-08 **credit card theft cookies Web browser embarrassment**

Network News

Eric Schmidt, CEO of Novell, was embarrassed when a criminal stole his credit-card information and bought more than 100 copies of Netware's chief competition, Windows NT. Schmidt guessed that the thief may have used (Trojan?) software that used cookies stored on his PC to obtain personal information.

Category 19 *Counterfeits, forgery (including commercial software/music piracy)*

2006-02-13 **intellectual property rights group call Russia focus copyright anti-piracy USTR IIPA**

EDUPAGE; http://www.itworld.com/Man/2683/060213iipa/ 23

INTELLECTUAL PROPERTY GROUP CALLS FOR FOCUS ON RUSSIA

In comments submitted to the U.S. Trade Representative (USTR), the International Intellectual Property Alliance (IIPA) urges the agency to identify Russia as a Priority Foreign Country, a designation for countries considered most threatening to intellectual property. The IIPA estimates that piracy rates in Russia are as high as 85 percent for business software, 67 percent for music, 81 percent for movies, and 82 percent for entertainment software. In addition, the Priority Foreign Country list indicates countries whose antipiracy efforts are minimal. The IIPA has previously requested that Russia be put on the list, but only Ukraine is on the highest-priority list. According to the IIPA, Ukraine should be moved down a step, to the Priority Watch List, with 15 other countries, including China, Egypt, Thailand, and Venezuela. The IIPA said countries including Pakistan, Brazil, and Taiwan had improved efforts during 2005 to address intellectual property concerns.

19.1 Software piracy

Category 19.1 *Software piracy*

1997-01-02 **software theft**

Reuters

Jacqueline Wong of Reuters reports on the battle against software theft in Singapore. Microsoft has planted its own store in the shopping center that is most popular with computer users and is joining actively with police in raids on factories and stores where the pirated software is manufactured and sold. Local software developers applaud the move, saying that software theft harms their efforts to earn a living from writing software.

Category 19.1 *Software piracy*

2000-05-05 **intellectual property copyright violation theft counterfeit warez criminal hackers juveniles investigations arrests**

NewsScan, Wall Street Journal
http://interactive.wsj.com/articles/SB957492236169474418.htm

The FBI has arrested 17 people, five of them former or current employees of Intel, on charges of involvement with Internet sites devoted to pirated software. The five were described as having held low-level engineering jobs, and an Intel spokesman said four out of the five were no longer with the company. All 17 suspects were members of a loosely organized group called Pirates with Attitudes, which operated one of the Internet's oldest "warez" sites — a term describing a hacker variation of software sold in stores by merchants. Most warez sites are run as hobbies and their users are often teenage boys who view downloading a pirated software program to be a rite of passage. The indictments do not allege that the perpetrators were attempting to make money through their activities, but the potential penalties include a US$250,000 fine and five years in prison. "This is the most significant investigation of copyright infringement involving the use of the Internet conducted to date by the FBI," says a spokeswoman for the Bureau's Chicago office. "It demonstrates the FBI's ability to successfully investigate very sophisticated online criminal activity." (Wall Street Journal 5 May 2000)

Category 19.1 *Software piracy*

2000-08-17 **intellectual property IP wireless communications software sabotage copyright infringement violation**

NewsScan

[In August,] America Online . . . [said] that an unauthorized distribution of its new software for wireless devices . . . [posed] no danger to the privacy of AOL users, though about 10,000 people . . . download the software from the Web in . . . [a] few days. Carnegie Mellon University computer science professor Mahadev Satyanarayanan thinks the release of the software (code-named Gamara, for the flying turtle monster that battled with Godzilla) could give clues about how to hide out on AOL's systems. Gamara uses Mozilla, a browser made by Netscape, which was purchased by AOL in 1998. (Washington Post 17 Aug 2000)

Category 19.1 *Software piracy*

2001-11-15 **Windows XP counterfeit operating system decryption vulnerability copy protection copyright intellectual property software piracy**

RISKS 21 76

A few hours after its release, Windows XP was hacked and its copy protection mechanisms defeated. According to an article from a London paper, "Black market copies of the supposedly uncrackable Windows XP. . . are already on sale for 5 pounds."

Category 19.1 *Software piracy*

2001-11-16 **software piracy counterfeit seizure investigation law enforcement police intellectual property**

NewsScan

FEDS MAKE RECORD COUNTERFEIT SOFTWARE SEIZURE [16 Nov 2001]
California law enforcement officials made the largest seizure of counterfeit software in U.S. history, estimated to be worth about $100 million. The products, which originated in Taiwan, included about 31,000 high-quality copies of Microsoft's Windows Millennium Edition and 2000 Professional operating systems and tens of thousands of copies of Symantec security software. "They look so good that the purchaser would not know it was counterfeit," said Los Angeles County Sheriff Lee Baca. Some of the bogus discs even carried the "Do not make illegal copies of this disc" warning. Authorities have arrested three people on bribery conspiracy and smuggling charges, and another has been charged with state violations of counterfeiting a registered trademark. (AP 16 Nov 2001)
http://news.excite.com/news/ap/011116/20/counterfeit-software

---

Category 19.1 *Software piracy*

2001-12-19 **software piracy industrial espionage copyright intellectual property organized crime international universities academia executives investigation international cooperation law enforcement police**

NewsScan

CUSTOMS SERVICE EXPANDS SOFTWARE PIRACY INVESTIGATION [19 Dec 2001]
The U.S. Customs Service, which is conducting what is described as the largest criminal investigation into software piracy ever pursued by the federal government, is expanding "exponentially" its questioning of employees and students at some of the nation's top universities. Included in the Operation Buccaneer sweep are Duke University, the Massachusetts Institute of Technology, the University of California at Los Angeles, and the Rochester Institute of Technology. Executives at several software companies have also been questioned as law enforcement officials work to shut down a multibillion-dollar international piracy ring that has produced counterfeit versions of everything from the newly launched Windows XP operating system to such recent Hollywood fare as "Harry Potter and the Sorcerer's Stone." Customs officials say some of the software appears to have been stolen by executives and other insiders at the affected companies. No arrests have been made so far, and officials are trying to persuade more suspects to cooperate in exchange for leniency. "We have people here who have never contemplated spending any time in prison who all of a sudden are coming to the realization that, wait a minute, I'm in trouble here," says Special Agent Alan Doody, who's heading up the operation. (New York Times 19 Dec 2001)
http://www.nytimes.com/2001/12/19/technology/19PIRA.html

Category 19.1 *Software piracy*

2002-02-28 **music software piracy intellectual property theft shoplifing data storage connectivity**

NewsScan

HAVE IPOD, WILL SHOPLIFT?
It turns out that Apple's new iPod device is well-suited to electronic shoplifting, with its roomy 5GB hard drive capable of serving as portable storage for very large files, such as the latest Mac OS. A CompUSA shopper describes watching a young man equipped with an iPod walk over to a nearby display Macintosh, plug his iPod into the machine with a FireWire cable, and copy Microsoft's new Office for OS X suite, which retails for $500. The whole process took less than a minute. "Watching him, it dawned on me that this was something that was very easy to do," said witness Kevin Webb. "In the Mac world it's pretty easy to plug in and copy things. It's a lot easier than stealing the box." And while the iPod has a built-in anti-piracy mechanism that prevents music files from being copied, there are no such protections for software. "This is the first we have heard of this form of piracy," said a Microsoft product manager. "And while this is a possibility, people should be reminded that this is considered theft." (Wired.com 28 Feb 2002)
http://www.wired.com/news/mac/0,2125,50688,00.html

Category 19.1 *Software piracy*

2002-04-19 **software piracy intellectual property copyright violations counterfeit arrests police international**

NewsScan

RAIDS ON SOFTWARE PIRACY RING
More than 125 FBI and state and local enforcement officers in California arrested 27 people, mostly Taiwanese [nationals], in Freemont, San Jose, and Union City, charging them with participation in an international software piracy ring that has cost Microsoft $75 million in lost sales of its software products. The ring has been under police surveillance for more than two years. (San Jose Mercury News 18 Apr 2002)
http://www.siliconvalley.com/mld/siliconvalley/3093841.htm

Category 19.1 Software piracy

2002-05-21 **software piracy criminal gangs sentence prosecution intellectual property copyright**

FindLaw Download This 86

INTERNET SOFTWARE PIRACY GROUP HEAD SENT TO PRISON
The leader of "DrinkorDie," one of the oldest and largest international software piracy rings on the Internet, was sentenced on Friday to three years and eight months in prison for conspiring to commit copyright infringement, U.S. officials said. They said John Sankus, 28, of Philadelphia, whose screen name was HellFire spelled backward, received the sentence as part of plea agreement reached with prosecutors in February. Prosecutors have described DrinkorDie as a highly structured, security-conscious group that illegally reproduced and distributed hundreds of thousands of copies of copyrighted works around the world.
http://news.findlaw.com/news/s/20020517/crimetechdc.html

FindLaw's Computer Crime Publications
[Copy and paste link into browser]
http://www.findlaw.com/01topics/10cyberspace/computercrimes/publications.html

---

Category 19.1 Software piracy

2003-06-24 **Microsoft worker $17m racket office exchange SQL server XP Richard Gregg internal store program coordinator**

NIPC/DHS

June 24, The Register — MS worker 'ran' $17m software racket.

A Microsoft worker has been charged with stealing $17 million of software from Microsoft's internal store. Richard Gregg, a Windows program coordinator, has pleaded not guilty to 62 counts of mail and computer fraud. From January to October 2002, Gregg allegedly ordered 5,436 copies of software such as Windows XP, SQL Server, Exchange and Office which he subsequently resold.

Category 19.1 Software piracy

2003-12-01 **asian pirate longhorn microsoft operating system secure fewer annoying reboots**

NewsScan

ASIAN PIRATES HAWKING 'LONGHORN' OPERATING SYSTEM
Microsoft's next-generation operating system, code-named "Longhorn," won't be released before 2005, but an early version is already on sale in southern Malaysia for $1.58 (6 ringgit). The software was demonstrated and distributed at a conference for Microsoft programmers in October, but the company's corporate attorney says, "It's not a ready product. Even if it works for awhile, I think it's very risky" to install it on a home or office computer. Longhorn purportedly promises new methods of storing files, tighter links to the Internet, greater security and fewer annoying reboots. (Reuters 1 Dec 2003)

Category 19.1 Software piracy

2004-01-19 **peer-to-peer P2P software piracy Kazaa Morpheus economic loss**

NewsScan

PEER-TO-PEER SOFTWARE THEFT

Peer-to-peer (P2P) file-sharing programs like Kazaa are increasingly being used for software piracy; in fact, William Plante of the security company Symantec thinks that roughly half of the illegal copies of his company's software are made through P2P electronic downloads. The thieves are "truly ghosts on the Internet" who are "virtually untraceable." One approach to curbing software piracy is mandatory online activation, and even though Plante admits those methods can be broken, he says it's "extremely inconvenient to try and use the cracked version." Michael Weiss of StreamCast Networks, which makes the P2P program Morpheus, says the software industry should get an entirely new attitude, which would "embrace the technology, just like the movie studios ended up embracing VCR's. This is not going to go away. Technology always wins out. You would think the software companies would know that more than Hollywood." (New York Times 19 Jan 2004)

Category 19.1 *Software piracy*

2004-02-14 **Microsoft source code Windows XP NT online Internet intellectual property rights issues**

NewsScan

STOLEN CODE RAISES SECURITY CONCERNS

The distribution on the Internet of stolen source code for portions of Microsoft's Windows 2000 and Windows NT operating systems is raising new concerns among security experts. A former federal computer crime prosecutor says, "This raises real national security concerns. The fact that Microsoft's software is so widely available will have an impact across the computer security industry." Critics have often accused Microsoft of doing a poor job of protecting the security of its software from network vandals. A Microsoft executive's response to the latest theft was: "We take this seriously. It's illegal for third parties to post or make our source code available. From that standpoint we've taken appropriate legal action to protect our intellectual property." (New York Times 14 Feb 2004)

Category 19.1 *Software piracy*

2004-07-07 **Business Software Alliance BSA theft piracy copyright infringement statistics one third**

NewsScan

STOLEN: ONE THIRD OF THE WORLD'S SOFTWARE

The Business Software Alliance, a trade group, says that 36% of all the software in the world has been pirated, costing the industry $29 billion in lost revenue. The five countries with the highest incidence of pirated software are: China (92%), Vietnam (92%) and Indonesia (88%), Ukraine (91%),
and Russia (87%). (AP/San Jose Mercury News 7 Jul 2004)

Category 19.1 *Software piracy*

2004-08-24 **software piracy law enforcement police crackdown music video films copyright infringement plagiarism**

NYT http://www.nytimes.com/reuters/technology/tech-crime-poland-hackers.html?th

Polish police arrested members of a large software-piracy gang accused of stealing and selling music and videos.

The criminals stored their materials on large computer systems at universities around the world and may also have stolen theses from these computers for sale in plagiarism services.

Category 19.1 *Software piracy*

2004-09-16 **Federal Bureau of Investigation FBI illegal pirated software seize Digital Marauder**

DHS IAIP Daily; http://www.infoworld.com/article/04/09/16/HNfbi_1.html

September 16, InfoWorld — FBI seizes $87 million worth of illegal software.

A two-year investigation by U.S. law enforcement authorities has resulted in one of the largest seizures of fake software ever in the U.S. and charges against 11 individuals. The defendants from California, Washington, and Texas were indicted, Wednesday, September 15, with conspiring to distribute counterfeit computer software and documentation with a retail value of more than $30 million, the U.S. Attorney's Office for the Central District of California said in a statement. The value could rise to $87 million, U.S. Attorney's Office spokesperson Thom Mrozek said. When arresting the defendants and searching their homes, offices and storage facilities, Federal Bureau of Investigation agents uncovered an additional stockpile of more than $56 million worth of fake Microsoft Corp., Symantec Corp. and Adobe Systems Inc. products. Microsoft worked closely with the authorities in Los Angeles on the case, which was code-named "Digital Marauder."

Category 19.1 *Software piracy*

2004-11-03 **hackers software piracy source code club Cisco PIX firewall Enterasys IDS Usenet e-mail sales**

DHS IAIP Daily; http://www.pcworld.com/news/article/0,aid,118452,00.asp

November 03, IDG News Service — Hackers reopen online store.

An anonymous group of malicious hackers has reopened an online store that sells the stolen source code of prominent software products. The Source Code Club is offering the code for Cisco Systems' PIX firewall software to interested parties for $24,000, according to messages posted in online discussion groups. The group is using e-mail and messages posted in a Usenet group to communicate with customers and receive orders for the source code of several security products, including Cisco's PIX 6.3.1 firewall and intrusion detection system (IDS) software from Enterasys Networks, the group says. Cisco did not immediately respond to a request for comment.

Category 19.1 *Software piracy*

2004-11-12 **SQL theft Microsoft software piracy intellectual property**

NewsScan; http://australianit.news.com.au/articles/0

FOUR IN COURT OVER SQL THEFT

Four former Microsoft employees have been charged with stealing $32 million worth of software and selling it on the side. According to a complaint filed by Microsoft, the workers ordered software available to Microsoft employees for free to use for business purposes, then sold it to online software retailers. The complaint said the employees blocked managers from getting routine email notification that the workers were ordering the software. The software the four are accused of stealing included the SQL Server 2000, which normally sells for $15,000, and the SQL Enterprise Server 7.0, which sells for $29,000. (The Australian, 12 Nov 2004)

Category 19.1 *Software piracy*

2004-11-24 **Microsoft Windows XP piracy countermeasure Counterfeit Project**

DHS IAIP Daily; http://www.vnunet.com/news/1159640

November 24, VUNet — Microsoft gets tough with XP pirates.

Microsoft has moved to clamp down on software pirates in the UK after discovering what it describes as a large volume of high quality counterfeit versions of Windows XP. The software maker has invited "anyone unsure as to the legitimacy of their Windows XP software" to submit their products for analysis. Software that is found to be counterfeit will be replaced for free subject to the terms and conditions of its offer, Microsoft promised. The XP Counterfeit Project marks the latest in a series of moves by Microsoft to target software pirates.

Category 19.1 *Software piracy*

2005-01-07 **software pirate Internet Adobe Autodesk Macromedia Microsoft copyright infringement**

EDUPAGE; http://washingtontimes.com/upi-breaking/20050107-054741-2893r.htm

SOFTWARE PIRATE GETS 18 MONTHS

A federal court in Virginia has sentenced a Maryland man to 18 months in prison for selling pirated software on the Internet. The Justice Department alleged that Kishan Singh operated a Web site where users could pay for access to downloads of copyrighted applications from companies including Adobe, Autodesk, Macromedia, and Microsoft. Singh removed copy protections from the files he made available on his Web site. Singh pleaded guilty to one count of copyright infringement and was also ordered to forfeit the computer equipment he used to commit his crime. According to the Justice Department, during the time Singh's Web site was operating, users from around the world downloaded thousands of copies of various applications, worth a total value estimated to be between $70,000 and $120,000.

Category 19.1 *Software piracy*

2005-01-25 **Microsoft limit downloads software owners Windows Genuine Advantage patches updates pirated counterfeit version China Norway Czech Republic piracy**

EDUPAGE; http://news.com.com/2100-1016_3-5550205.html

MICROSOFT TO LIMIT DOWNLOADS TO LEGAL SOFTWARE OWNERS

Microsoft will soon begin requiring users to employ a program called Windows Genuine Advantage before downloading software patches or updates. The program verifies that the computer requesting the download is running a legitimate copy of Windows software rather than a pirated or counterfeit version. Initially, the requirement will apply to users in China, Norway, and the Czech Republic, but it will include all users by the middle of the year. Users will still be able to receive software updates and patches using the Automatic Updates feature. The program is part of Microsoft's three-pronged approach to limiting software piracy: educating users, designing products that discourage illegal copying, and legal enforcement. In addition to allowing downloads, the program will also offer users discounts on Microsoft products and services. Analysts noted that although the obvious benefit of the program is to Microsoft by way of decreasing the incidence of software piracy, users stand to benefit as well. Ensuring that a computer is running a legitimate version of an operating system shields that computer from bugs and glitches associated with pirated software, while guaranteeing that patches and upgrades will work properly.

Category 19.1 *Software piracy*

2005-08-01 **Microsoft anti-piracy system hacked Windows Genuine Advantage WGA copy**

DHS IAIP Daily;
http://www.techworld.com/security/news/index.cfm?NewsID=4134

HACKERS BREAK INTO MICROSOFT'S ANTI-PIRACY SYSTEM

Hackers found a way around Microsoft's Windows Genuine Advantage (WGA) anti-piracy system last week, only a day after the system went into effect. WGA requires Windows users to verify they are using a genuine copy of Windows before they are allowed to download certain software updates. Security patches aren't covered by the system, and remain available to any Windows user, legitimate or not. Using a simple JavaScript hack, all users had to do was paste a JavaScript URL into the Internet Explorer browser window at the beginning of the process; this turned off the key check, according to users. Microsoft said it was investigating the hack but didn't consider it a security flaw. The company said that it may not take immediate action to fix the problem. "As the validation system is updated from time to time, we will address this and other issues that may arise," a Microsoft spokesperson said. Microsoft put WGA into place to cut down on Windows piracy, and to persuade users who are running pirated copies of Windows to buy legitimate licences.

Category 19.1 *Software piracy*

2005-12-07 **Microsoft eBay partnership software piracy online auction**

DHS IAIP Daily; http://www.vnunet.com/vnunet/news/2147277/ebay−tackles−
micro soft−software

MICROSOFT AND EBAY HOOK UP TO CATCH PIRATED SOFTWARE

Microsoft and eBay are working together to stop the sale of pirated software on the online auction site. The companies said in a statement that over 21,000 suspect software sales were removed from the eBay United Kingdom site between August and October this year. Around half were sales of counterfeit copies of Windows, and 36 percent were fake copies of Microsoft Office. Microsoft claimed that the crackdown is working because eBay removed 11,535 suspected counterfeit sales from the site in August. This fell to 4,460 in September and 5,423 in October.

Category 19.1 *Software piracy*

2005-12-08 **software piracy intellectual property rights violation copyright infringement study BSA**

EDUPAGE; http://news.com.com/2100-1014_3-5987127.html

PUTTING THE NUMBERS TO SOFTWARE PIRACY

A study conducted by research firm IDC on behalf of the Business Software Alliance (BSA) indicates that as much as 35 percent of software is pirated, down only about 1 percent from last year. The study covered 70 countries, representing 99 percent of the global market for IT spending. Software piracy is significantly lower than it was in the early 1990s, when, for example, the piracy rate in Europe was nearly 80 percent. That number has fallen to 35 percent, but, according to Beth Scott, European vice president of the BSA, the current rate is still 20 times higher than losses to shoplifting. The IDC study estimates that a reduction in the piracy rate to 25 percent would lead to the generation of 2.4 million jobs and $400 billion of economic growth. Piracy remains rampant in some countries, including China (90 percent) and Russia (87 percent). The problem is so bad that China, which is one of the world's largest markets for PCs, is not on the list of top 20 global markets for software because so much software is obtained illegally. CNET, 8 December 2005

Category 19.1 *Software piracy*

2006-01-30 **Britain ISPs order disclose identities BSA FAST UK**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4663388.stm 23

ISPS IN BRITAIN ORDERED TO DISCLOSE IDENTITIES

In the United Kingdom, the High Court has ordered 10 ISPs to disclose the identities of 150 individuals suspected of trading copyrighted software. The Business Software Alliance estimates that one-quarter of all software used in the United Kingdom is illicit. The court ruling came after a group called the Federation Against Software Theft (FAST) petitioned the court to order the disclosures, noting that software pirates hide behind fake names and bogus e-mail addresses and are notoriously difficult to track down. FAST said that after it has obtained the identities of those suspected of illegally trading software, it will consult with law enforcement authorities. John Lovelock, an official at FAST, said the group intends to make an example of software pirates, and the group's legal counsel said the current court action is "only the first wave of an ongoing strategy."

19.2 Music piracy

Category 19.2 Music piracy

2000-05-05 **copyright infringement violation illegal copies counterfeit music files theft lawsuit ruling penalty**

NewsScan; Los Angeles Times
http://www.latimes.com/business/20000505/t000042406.html; San Jose Mercury
News http://www.sjmercury.com/svtech/news/breaking/merc/docs/010346.htm

U.S. District Judge Jed Rakoff . . . [said] MP3.com is using "indefensible" and "frivolous" arguments in its defense against charges of copyright violations brought by the Recording Industry Association of America. The judge, in ruling against MP3.com, determined that the company "is replaying for the subscribers converted versions of the recordings it copied, without authorization, from plaintiffs' copyrighted CDs. On its face, this makes out a presumptive case of infringement." Rakoff called MP3.com's fair-use defense "indefensible" and its claim that it was protecting record companies from music pirates "frivolous." (Bloomberg/Los Angeles Times 5 May 2000)

[In a related case,] Settling a copyright infringement lawsuit brought against it by Warner Music and BMG Entertainment, the Internet music distribution company MP3.com . . . signed licensing agreements with both those companies. Customers are able to access music in the MP3 database at any time and from any device with Internet access. Warner executive Paul Vidich . . . [said] that the settlement agreement "clearly affirms the right of copyright owners to be compensated for the use of their works on the Internet." (AP/San Jose Mercury News 9 Jun 2000)

[In September,] . . . federal judge [Jed Rakoff] . . . ruled that MP3.com willfully violated music copyrights and . . . ordered it to pay at least $117 million in damages to Seagram's Universal Music Group — believed to be the largest copyright infringement penalty in history. "This should send a message that there are consequences when a business recklessly disregards the copyright law," says a senior VP of the Recording Industry Association of America, which represents Universal and the four other major music companies. "We trust this will encourage those who want to build a business using other people's copyrighted works to seek permission to do so in advance." The industry's lawsuit claimed that MP3.com had violated copyright laws by creating a database of 80,000 unauthorized CDs, and the judge's ruling assessed a $25,000 penalty for every Universal CD illegally posted on its My.MP3.com service — somewhere between 4,700 and 10,000 recordings. MP3.com . . . [said] it will appeal the ruling, which it called "draconian." (Los Angeles Times 7 Sep 2000)

Category 19.2 Music piracy

2000-09-25 **intellectual property IP copyright violations infringements music band owners money profits**

NewsScan, San Jose Mercury News
http://www.sjmercury.com/svtech/news/breaking/merc/docs/025084.htm

Although The Grateful Dead is famous for allowing its fans to make and swap personal recordings of its live concerts, the group has never authorized bootlegged copies of its studio recordings and has never allowed anyone to sell a tape of a concert, not even for the price of the tape itself. Grateful Dead's attorney, Eric Doney, says: "They have always been vehement about this: If someone is going to make money, it should be them. The music belongs to the creators, not someone else." (AP/San Jose Mercury News 25 Sep 2000)

Category 19.2 Music piracy

2000-10-02 **intellectual property IP copyright violation infringement music distribution law bill proposal regulation decriminalization**

NewsScan, New York Times
http://partners.nytimes.com/2000/10/02/technology/02NECO.html

Democrat congressman Rick Boucher and three Republican colleagues . . . introduced legislation designed to change the focus of the debate over digital copyright issues from the courts to the legislature. Called the Music Owners' Listening Rights Act of 2000, the bill would legalize the controversial MP3.com music downloading service, which is now defending itself in multimillion dollar lawsuits. Boucher says, "What matters is whether new technologies are consistent with the theory of copyright laws, not just consistent with the details of the copyright law. The law should not stand in the way of an entirely legitimate technology that provides consumer convenience without costing the record companies anything." But Recording Industry Association of America president Hilary B. Rosen thinks that Congress should stay out of the fray and that "I have a hard time believing this is going to get resolved anywhere but in the marketplace." (New York Times 2 Oct 2000)

Category 19.2 Music piracy

2000-10-02 **intellectual property IP copyright violation infringement music distribution ethics popular opinion feeling survey study attitudes**

NewsScan, E-Commerce Times
http://www.ecommercetimes.com/news/articles2000/001002-1.shtml

Downloading music off the Internet is not stealing in the eyes of 53% [±7% for 95% confidence limits] of all U.S. Internet users, according to a new study by the Pew Internet & American Life Project [which interviewed 237 people who download music and 12,751 candidates of which 6,413 were Internet users; the interviews were carried out by phone from March through August, 2000]. And those who are active downloaders are even more adamant about their position — 78% do not believe that downloading and sharing files for free is wrong, and 61% don't care if the music they're downloading is copyrighted. Even among the general population, 40% of those surveyed said they didn't see anything wrong with downloading music off the Internet, while 35% said the downloaders are stealing, and 25% chose not to take a position. In a finding guaranteed to raise the ire of the Recording Industry Association of America, only 21% of music downloaders end up actually buying the music they get off the Internet. (E-Commercetimes 2 Oct 2000)

Category 19.2 Music piracy

2000-10-18 **music copyright infringement violations agreement lawsuit**

NewsScan, San Jose Mercury News
http://www.mercurycenter.com/svtech/news/breaking/internet/docs/527752l.htm

Under the terms of a tentative 3-year agreement between the National Music Publishers' Association and online music company MP3.com, MP3 will pay music publishers as much as $30 million to reimburse them for past uses of their music and to make advance royalty payments on future uses. MP3's 80,000 album collection was originally created without the permission of the publishers and recording companies that own the copyrights to the music. (Reuters/San Jose Mercury News 18 Oct 2000)

Category 19.2 Music piracy

2001-02-23 **music peer-to-peer networking copyright infringement bootleg intellectual property rights infringement lawsuit judgement lawsuits**

NewsScan

RECORD INDUSTRY TAKES AIM AT 'OPEN NAPSTER' CLONES
With legal victory over Napster on the horizon, the record industry has begun to take action against hundreds of Napster clones that also offer free music downloading via the Internet. Since [the 19th of February 2001], the Recording Industry Association of America has sent about 60 legal notices to the ISPs that provide Web connections for "Open Napster" servers -- computers that run Napster-like software, but aren't affiliated with Napster. One expert estimates that there are 350 such servers operating globally, although the number varies daily. Legal observers say the issues against Open Napster operators are clear-cut, but battling these guerilla operations is difficult. It's likely that smaller versions of Napster will continue to pop up on the Internet, because all it takes to run an Open Napster site is a PC and a fast Internet connection. (Wall Street Journal 23 Feb 2001)
http://interactive.wsj.com/articles/SB982898110704921 78.htm (sub req'd)

Category 19.2 Music piracy

2001-03-05 **music sharing copyright intellectual property service alternative**

NewsScan

PAID MUSIC SERVICES READY TO PICK UP WHERE NAPSTER LEFT OFF
A handful of file-sharing startups -- including U.K.-based Wippit, and U.S. firms CenterSpan Communications and Ipingpong -- are hoping to establish their paid music download services before Napster can follow through with plans to retool itself into a fee-based system by summer. An early version of Wippet is already in public trials, and later this month CenterSpan plans to start its own public tests of a new, secure file-sharing system based on technology it acquired from the now-defunct Scour. Meanwhile, Ipingpong plans to sweeten the pot by offering financial rewards to users based on the amount of music they ship to friends. "Napster has certainly opened up the [music] industry's minds," says Wippit's CEO, who says he approached an industry executive six months ago who "actually laughed in my face, saying, 'This can't happen.'" (Los Angeles Times 5 Mar 2001)
http://www.latimes.com/business/20010305/t00001951.html

Category 19.2 *Music piracy*

2001-04-10 **music peer-to-peer networking copyright infringement bootleg intellectual property rights infringement lawsuit judgement award error**

NewsScan

OOPS -- MP3.COM JURY DROPS A ZERO
Jurors who ordered MP3.com to pay Tee Vee Toons $300,000 for violating its copyrights have told the trial judge they goofed -- they meant to award something closer to $3 million. "The total was supposed to be between $2 and $3 million," said U.S. District Judge Jed Rakoff. "This matter is far from obvious in how it should be adjudicated." News that the jurors had essentially dropped a zero in arriving at the announced award of $296,873 stunned both sides. Tee Vee Toons, the largest U.S. independent music label, had sought damages of $8.5 million, but MP3.com said at this point there was no basis for upsetting the award, noting that one of the jurors was a math teacher. Rakoff said he would issue a ruling in several weeks. (Bloomberg/Los Angeles Times 10 Apr 2001)
http://www.latimes.com/business/20010410/t000030496.html

Category 19.2 *Music piracy*

2001-08-21 **music peer-to-peer networking copyright intellectual property rights infringement lawsuit**

NewsScan

MP3 SUED FOR "VIRAL" COPYRIGHT INFRINGEMENT [21 Aug 2001]
A new lawsuit brought by a group of independent songwriters and music publishers against the MP3.com service is demanding copyright infringement damages for "viral" uses of the material, including every bootleg track exchanged through any of the underground file-swapping services that were created after MP3 set the stage for massive piracy activities. An attorney for the plaintiffs says: "If a song has been downloaded hundreds of thousands of times on Napster, and at least a portion of that is attributable to MP3.com, the magnitude of damages that should be assessed would be many, many times what they would be liable for under direct infringement." (San Jose Mercury News 21 Aug 2001)
http://www.siliconvalley.com/docs/news/svfront/mp3082101.htm

Category 19.2 *Music piracy*

2001-09-06 **music piracy copyright intellectual property peer-to-peer**

NewsScan

MORE PEOPLE TRADING BOOTLEGGED MUSIC THAN EVER
An estimated 15 million people downloaded illicit music online this summer, surpassing the song-swapping binge that followed the federal appeals court ruling against Napster in February. In the wake of that ruling, a new generation of file-swapping sites has arisen to fill the void. "It's like playing whack-a-mole: You kill one of these guys and another one pops up to take its place," says a Gartner Dataquest researcher. The fastest growing of these new services -- MusicCity's Morpheus and KaAaA, have logged 3 million users since Napster installed song-filtering technology in June, according to Jupiter Media Metrix. And a host of other sites -- Aimster, AudioGalaxy, iMesh and BearShare -- are expanding at a slower pace. "Not only are these services less centralized -- and more difficult to police, but whereas Napster was only an MP3 application, consumers now have been introduced to the wonderful world of porn and movie pirating," says a Jupiter analyst. The sustained popularity of these underground services is eroding CD revenues, with sales of albums and singles down 5.4% for the second quarter this year. Gartner predicts CD sales will continue to decline dramatically, with revenue off 20% by 2005. "No amount of wishful thinking on the part of the music industry will stop this." (Silicon Valley 6 Sep 2001)
http://www.siliconvalley.com/docs/news/svtop/music090601.htm

Category 19.2 *Music piracy*

2001-10-09 **music copyright intellectual property distribution channel alternative agreement**

NewsScan

MUSIC PUBLISHERS, RECORDING INDUSTRY INK LICENSING DEAL
The National Music Publishers' Association, Harry Fox Agency and the Recording Industry Association of America (RIAA) have signed a licensing agreement that will pave the way for a new generation of online music subscription services backed by the Big Five record labels. Under the terms of the agreement, all RIAA member labels and their licensees -- including the new online services -- will have access to every musical work authorized to be licensed by the Harry Fox Agency. Harry Fox will issue licenses for subscription services offering on-demand streaming and limited downloads, or downloads that can be played only for a designated period of time or number of times. To get the ball rolling, the RIAA will pay Harry Fox $1 million toward royalties to be determined. Once rates are determined, royalties will be payable on a retroactive basis, but if the two sides don't settle on a rate within the next two years, the recording industry will pay $750,000 a year until a rate is set. (Wall Street Journal 9 Oct 2001)
http://interactive.wsj.com/articles/SB1002623694407861800.htm (sub req'd)

Category 19.2 *Music piracy*

2001-10-30 **music peer-to-peer networking copyright infringement bootleg intellectual property rights infringement lawsuit judgement**

NewsScan

NAPSTER RULING [11 Feb 2001]
A California federal appeals court [ruled on February 12, 2001] on whether to shut down Napster or allow it to keep operating while its legal case continues. Napster lost the first round in its battle with the recording industry last July when a lower court ruled that the file-swapping service was guilty of "wholesale" copyright violation and ordered it to cease trading copyrighted material pending a full trial. The appeals court prevented that order from taking effect until it had a chance to review the injunction. If Napster wins its case, the ruling could unleash any number of other ventures that have been awaiting a decision on whether a "personal use" exception to copyright law extends to downloadable music. But even if it loses, the peer-to-peer file-sharing technology on which it's based is here to stay. Meanwhile, Napster has teamed up with recording giant Bertelsmann, which has offered it much-needed capital if it switches to a subscription-based service that pays artists' royalties. (AP 11 Feb 2001) http://news.excite.com/news/ap/010211/22/napster-lawsuit

NAPSTER RIVALS SEE OPPORTUNITY IN RULING [13 Feb 2001]
[The] appeals court decision [on February 12, 2001] prohibiting Napster from facilitating the sharing of copyrighted music files was welcomed by Napster rivals, who believe that record labels will now become more receptive to licensing agreements with them. Analysts say the recording industry's legal battle with Napster has stymied the online music distribution industry, and with the conclusion of the protracted court case in sight, may be more willing to negotiate deals with sites that present an alternative to Napster, which has been labeled a haven for "electronic shoplifting." Shares in RealNetworks, MP3.com, Liquid Audio and EMusic.com all rose on yesterday's news. "Now it's the time for the industry to move forward to build great businesses that respect the legitimate interests of consumers, artists and rights holders," says RealNetworks chairman and CEO Rob Glaser. (Reuters/InfoWorld 13 Feb 2001) http://www.infoworld.com/articles/hn/xml/01/02/13/010213hnnapriv.xml?p=br&s=6

NAPSTER OFFERS $1 BILLION TO RECORD COMPANIES; "NOT ENOUGH" [21 Feb 2001]
Online music-swapping service Napster, which is still embroiled in lawsuits for infringing on copyrights, is proposing to pay record companies $1 billion over five years to end the dispute. The five major companies would divide up $150 million annually (according to what percentage of their works are exchanged by Napster users) and an additional $50 million would be directed to independent music companies and artists. Music industry executives and analysts dismissed the offer as insufficient. Napster also announced details of its plan to convert its operation into a subscription-based activity. Users probably will be charged a fee of $5.95 to $9.95 for computer downloads of an unlimited number of music files, plus an additional fee for downloads to their own compact disks. (New York Times 21 Feb 2001) http://partners.nytimes.com/2001/02/21/technology/21NAPS.html

NAPSTER RULING MAY COME [2 March 2001]
With a federal judge about to rule (maybe today) on whether online music-swapping service Napster must shut down for ignoring copyright laws, some analysts are worried that the downfall of Napster would have a serious negative impact on the Internet itself. Ford Cavallari of the research firm Adventis says: "We believe that if you take Napster out of the mix, you basically stunt the growth of DSL and cable modems." And computer manufacturing companies have been busy selling computers configured specifically for people who want to download free music and create custom CDs. Cavallari estimates that Napster's 64 million users account for 3% of all Internet traffic. Some of those users are now convinced that "it doesn't make sense to pay" the piper anymore: they can call the tune without paying. (Washington Post 2 Mar 2001)
http://washingtonpost.com/wp-dyn/articles/A10875-2001Mar1.html

NAPSTER HOPES TO SURVIVE ORDER TO CURB COPYRIGHT ABUSE [6 March 2001]
Online music-swapping service Napster is now under a court order from U.S. District Judge Marilyn Hall Patel in San Francisco to delete from its database any song protected by copyright. It will have three business days to accomplish the task of removing a huge inventory of songs identified by the five major record companies suing it for copyright infringement. Copyright law professor Peter Jaszi of American University predicted: "What is likely to happen is that the recording companies will blanket Napster with a very, very large number of file names." To stay alive, Napster is making efforts to evolve its free service into one that charges a subscription fee and pays royalties for copyrighted material. (Washington Post 7 Mar 2001)
http://washingtonpost.com/wp-dyn/articles/A32654-2001Mar6.html

NAPSTER ACCUSED OF EVADING JUDGE'S ORDER [28 March 2001]
The Recording Industry Association of America (RIAA) is complaining that online music-swapping service Napster has failed to remove from its database 675,000 copyrighted songs it is required by court order to shield from its users. RIAA president Hilary Rosen said: "Amazingly, every single one of the copyrighted works that was originally contained in our law suit is still readily available on Napster. Napster's filter fails to do even that which Napster claims it should do - let alone all of the things we believe Napster should do." The parties to the dispute will appear in court again in mid-April. (San Jose Mercury News 28 Mar 2001) http://www.siliconvalley.com/docs/news/svfront/nap032801.htm

MEDIATOR NAMED IN LAWSUIT AGAINST NAPSTER[10 Apr 2001]
U.S. District Court Judge Marilyn Hall Patel has picked A.J. "Nick" Nichols to serve as a mediator to evaluate the technical issues in the recording industry's lawsuit against online music-swapping service Napster. The industry says that Napster has

failed to observe a court order requiring it to keep copyrighted music off its site, whereas Napster claims it is doing everything that is technically possible. Nichols has a Ph.D. in engineering from Stanford University and has previously served as mediator in a lawsuit between Sun and Microsoft. (WSJ/AP/San Jose Mercury News 10 Apr 2001)
http://www.siliconvalley.com/docs/news/svfront/078061.htm

NAPSTER LICENSES RELATABLE SOFTWARE [20 Apr 2001]
Napster has harnessed a new tool in its efforts to remove copyrighted music from its service. Relatable's TRM software identifies songs by mapping their sound patterns -- a process that the company says will work regardless of the file format or quality. "TRM will help ensure that the millions of music files transferred through the new Napster system will be accurately monitored, and it will enable the appropriate allocation of royalties," says Relatable CEO Pat Breslin. (AP 20 Apr 2001)
http://news.excite.com/news/ap/010420/16/napster

SONGBIRD TARGETS NAPSTER LISTINGS [10 May 2001]
New software written by a 20-year-old Internet entrepreneur enables artists and record labels to quickly identify songs available on Napster even if the song's title or artist's name is garbled. Songbird, as the software's called, improves on Napster's own efforts to identify copyrighted material because it can simultaneously tap into some 90 different Napster servers rather than checking one server at a time, says creator Travis Hill. Songbird was recently demonstrated at the International Federation of Phonographic Industries headquarters in London, and was able to ferret out 40 Janet Jackson files listed under such names as anetJ acksonJ. The software is available on www.iapu.org. (Wall Street Journal 10 May 2001)
http://interactive.wsj.com/articles/SB989427592571440686.htm (sub req'd)

NAPSTER STRIKES DEAL WITH MAJOR RECORD LABELS [6 Jun 2001]
Napster has inked a deal to license music from three major record companies once it starts operating as a legal service later this summer. The agreement between Napster and MusicNet, the online music collaboration backed by AOL Time Warner, Berteslmann and EMI Group, marks Napster's latest step toward legitimacy. Under the deal, Napster users would pay one fee to access Napster's database of songs from independent record labels, and an additional fee to access MusicNet's content. The exclusive arrangement could give MusicNet a significant edge over rival service Duet, which is backed by Sony and Vivendi Universal. (Los Angeles Times 6 Jun 2001)
http://www.latimes.com/business/20010606/t000047089.html

NAPSTER, THE MOVIE [6 Jun 2001]
The film production arm of Liberty Media Group, cable TV organization, is working on a movie called "Napster" to tell the story of the music-swapping software that turned the recording industry upside down. Napster, which was created in 1999 by Shawn Fanning, a Northeastern University dropout with "nappy" hair, allows a community of users to share music files over the Internet, including songs protected by copyright. Outraged, the music industry lodged numerous lawsuits against Napster, though it now appears there will be an accommodation between Napster and the industry. The big record labels are planning use Napster to offer consumers a paid subscription service. (Reuters/USA Today 6 Jun 2001)
http://www.usatoday.com/life/cyber/tech/review/2001-06-06-napster-movie-reut.htm

NAPSTER STRIKES ROYALTIES DEAL WITH EUROPEAN RECORD LABELS [27 Jun 2001]
In another step toward legitimacy, Napster announced it has signed a commercial deal with groups representing 150 European independent record labels. The non-exclusive deal with the UK's Association of Independent Music (AIM) and Europe's Independent Music Companies Association marks a minor victory for Bertelsmann, which has backed Napster's efforts to move from renegade status to a legitimate fee-based service. Meanwhile, the independent labels hailed Tuesday's deal as a victory for collective licensing. "The majors are busy creating an (online) duopoly of their own. We don't know to what extent we will be closed out of their plans. It makes sense for us to have an alternative," said AIM vice-chairman Martin Mills. The European Commission has launched an antitrust investigation into PressPlay and MusicNet, the two online music services run by the big five record labels. (Financial Times 27 Jun 2001)
http://news.ft.com/news/industries/media

NAPSTER SUSPENDS ITS SERVICE [3 Jul 2001]
Napster, struggling to comply with a federal court order to stop its users from illegally swapping copyrighted music, suspended operations over the weekend because its technological solution needs more work. The company has been using filtering software that identifies a song by its unique acoustic properties, but some number of pirated songs have been slipping through the filter. Analyst P.J. McNealy says: "We knew they had technical challenges. this is the first time that they've outwardly said, 'They're huge,' and they shut it down." (San Jose Mercury New 3 Jul 2001)
http://www.siliconvalley.com/docs/news/svfront/nap070301.htm

NAPSTER ORDERED TO STAY CLOSED [12 Jul 2001]
Unconvinced by Napster's claim that its new filtering technology works "with 99% accuracy" to prevent customers from illegally swapping copyrighted music, Federal District Judge Marilyn Hall Patel has ordered Napster to shut down. An attorney representing the music publishers who'd filed the suit says: "Instead of being able to distribute infringing works while they figure out some way to stop doing it, Napster just has to stop distributing until they can do it legally. Which is sort of what we've been after for a year and a half." (San Jose Mercury News 12 Jul 2001)
http://www.siliconvalley.com/docs/news/svfront/nap071201.htm

NAPSTER GETS REPRIEVE [19 Jul 2001]
Napster got a breather on Wednesday when a U.S. federal appeals court temporarily suspended a lower court decision ordering it to shut down while it implemented filters to block the trading of copyrighted material. The court decision offers Napster the chance to demonstrate the effectiveness of its new fingerprinting filters, which it says are capable of blocking over 99% of copyrighted songs from its service. U.S. District Court Judge Marilyn Hall Patel had said that anything less than 100% effectiveness failed to comply with her ruling ordering Napster to remove all copyrighted material from its site. Meanwhile, the Recording Industry Association of America says it's confident that Napster will be blocked once again after the Court of Appeals reviews the case. (Financial Times 19 Jul 2001)
http://news.ft.com/news/industries/infotechnology

NAPSTER TO OFFER SUBSCRIPTION SERVICES BEFORE YEAR'S END [22 Aug 2001]
Napster's new chief executive, Konrad Hilbers, is promising that, as soon as his company fully complies with a court order to remove all copyrighted material from its site, he will start offering music-subscription services, to begin by the end of this year. "I'm very much a believer in what Napster stands for, which is the sharing of music among friends and private consumers when it comes to making available things like my children's Christmas carol singing or a garage band... It is quite obvious that we are challenging some of the music industry's business. (AP/USA Today 22 Aug 2001)
http://www.usatoday.com/life/cyber/tech/2001-08-22-new-napster-services.htm

NAPSTER INKS PRELIMINARY DEAL WITH MUSIC PUBLISHERS [24 Sep 2001]
Napster has reached a preliminary settlement with U.S. songwriters and music publishers in a further step toward legitimizing its online music service. Napster has agreed to pay songwriters and publishers $26 million in damages for past infringement, plus $10 million in advance for future royalty payments. The company, though, is still facing court action by the record labels, and talks in those lawsuits are continuing. The agreement marks the first of what is likely to be several announcements from companies hoping to launch online music services before the end of the year. Such agreements are a prerequisite for two industry-backed services -- Pressplay and MusicNet -- to launch their member-supported sites this fall. Napster CEO Konrad Hilbers says his revamped service will be up and running before the end of the year, also. (Financial Times 24 Sep 2001)
http://news.ft.com/news/industries/media

NAPSTER RELAUNCH HIT WITH DELAYS [30 Oct 2001]
Napster says it will postpone the launch of its new secure subscription-based service until next year, citing difficulties in obtaining record label licenses. The delay is a setback for Napster, which had hoped to beat the upcoming competition by several months. Industry-backed Pressplay and MusicNet both hope to launch their services before the end of the year, although they'll face several hurdles -- most notably, antitrust investigations in the U.S. and Europe. (Financial Times 30 Oct 2001)
http://news.ft.com/news/industries/media

Category 19.2 *Music piracy*

2001-11-14 **music copyright intellectual property distribution channel alternative agreement**

NewsScan

EMI TO OFFER NEW SUBSCRIPTION SERVICE EMI
Recorded Music has cut a deal with Liquid Audio that will provide EMI a way to launch a subscription service for consumers who want to permanently download song tracks off the Internet, burning copies to CDs, and transferring music compilations to portable players. Gerry Kearby of Liquid Audio says: "People can go out, for a pre-prescribed amount of money a month and download a bunch of songs, own those songs and burn them to CD -- not just rent them like the other services. For the first time, it brings the consumer much closer to the experience that they learned to love with Napster -- in a legitimate way." The new service will begin by focusing on EMI's Christian music catalog, offering subscribers access to an online jukebox of thousands of Christian songs for $14 a month; jazz, classical and other genres are expected to be added to the service at a later date. (San Jose Mercury News 14 Nov 2001)
http://www.siliconvalley.com/docs/news/svfront/audio111401.htm

---

Category 19.2 Music piracy

2001-12-03 **music copyright intellectual property marketing prediction**

NewsScan

BERTELSMANN THINKS THE DAY OF FREE MUSIC IS OVER [13 Feb 2001]
"I don't think in the long term there will be any free services left out there," says the e-commerce chief executive of Bertelsmann, the German media conglomerate that forged a deal last year with Napster and laid out plans to develop a fee-based music swapping service on the Internet. "When we closed the alliance with Napster, we never focused on the lawsuit. We focused on the new membership-based service. Whatever is happening on the legal front has no impact on our position." (Reuters/San Jose Mercury News 13 Feb 2001)
http://www.mercurycenter.com/svtech/news/breaking/internet/docs/843771l.htm

[The company certainly put its money where its mouth is, as shown in the next item:]

BERTELSMANN BUYS MYPLAY.COM [30 May 2001]
German media giant Bertelsmann is acquiring Myplay.com for $30 million in an strategy aimed at building up its Web-based music business. Myplay operates an online music storage locker, which enables users to manage and store their song collections online. It also owns technology used to create digital subscription services. The purchase continues the trend of large media companies acquiring Internet music startups. Bertelsmann also backs Napster, the file-swapping service, and is part of MusicNet, a venture formed by RealNetworks, AOL Time Warner and EMI. (Financial Times 30 May 2001)
http://news.ft.com/news/industries/media

BMG TO TEST PROTECTIVE CDs [31 Jul 2001]
Bertelsmann's BMG Entertainment is testing a new type of compact disc that enables consumers to make a limited number of digital copies, but prevents unlimited "ripping" of songs. Listeners can e-mail songs to others, but the recipients will have to pay a fee to listen to them. The CDs use technology from SunnComm, based in Phoenix, Ariz. BMG's test is the latest sign that the era of free music is drawing to a close. (Wall Street Journal 31 Jul 2001)
http://interactive.wsj.com/archive/retrieve.cgi?id=SB996530381990482524.djm

BERTELSMANN LICENSES NAPSTER TECHNOLOGY [23 Oct 2001]
Bertelsmann, which has backed Napster with funding, says it will use Napster's new secure technology for the German group's BeMusic operations as part of a licensing arrangement between the two companies. BeMusic's holdings consist of Web retailer CDNow, record club BMG Direct, and myplay Inc, a digital music locker business. The technology's underlying architecture, which does not include Napster's peer-to-peer functionality, will serve as the platform for BeMusic's offerings. (Reuters 23 Oct 2001) http://dailynews.yahoo.com/h/nm/20011023/tc/tech_bertelsmann_napster_dc_1.html

LISTEN UP: NEW ONLINE MUSIC SERVICES READY FOR LAUNCH [3 Dec 2001]
Several online music sites are ready for launch, offering musical selections for a monthly subscription fee. Rhapsody, created by the independent music firm Listen.com, will be presented as a streaming service available for $5.95 to $7.95 a month (visit www.listen.com if you want to see how it works). Tomorrow, MusicNet (backed by EMI, RealNetworks, AOL Time Warner, and Bertelsmann's BMG) will begin a similar service priced at about $9.95 a month. Later this month, Pressplay (jointly owned by Vivendi Universal's Universal Music and Sony Music) will join the competition for your mind and heart and ears. (Reuters/San Jose Mercury News 3 Dec 2001)
http://www.siliconvalley.com/docs/news/svfront/013946.htm

Category 19.2 Music piracy

2001-12-12 **music sharing copyright intellectual property service alternative**

NewsScan

REALNETWORKS IN TALKS WITH 3 MAJOR RECORD LABELS
RealNetworks is negotiating license rights with three major record companies -- Warner Music Group, BMG Entertainment and EMI Group -- to use their music in its planned subscription service, tentatively called MusicNet. As part of the deal, RealNetworks is offering the companies the option of an ownership interest in MusicNet. Other possibilities include making MusicNet available to other online services, and giving Napster an opportunity to license the service. If RealNetworks can sign a deal with Warner, BMG and EMI, the resulting service would present a strong challenge to the Duet subscription music service now being developed by Sony and Universal Music Group. (Wall Street Journal 30 Mar 2001)
http://interactive.wsj.com/articles/SB985905203900372337.htm (sub req'd)

MICROSOFT LAUNCHES MUSIC SERVICE [4 Apr 2001]
Microsoft is jumping on the music bandwagon with the first public test of MSN Music, its free Web-based service designed to help listeners discover new songs and artists. Users can specify styles and characteristics of music that they'd like to listen to, and a string of songs is then streamed to their PCs. The result is comparable to a custom-tailored radio channel -- users do not have the capability to listen to a particular song on demand. The distinction is important -- by not allowing users to download songs, Microsoft is relieved of the burden of negotiating individually with record labels for copyright licenses. Microsoft's announcement comes on the heels of the launch of MusicNet, a joint venture of AOL Time Warner, EMI Group, Bertelsmann and RealNetworks. (Wall Street Journal 4 Apr 2001)
http://interactive.wsj.com/articles/SB986337880412283670.htm (sub req'd)

AOL TIME WARNER UNVEILS ONLINE MUSIC SERVICE [12 Dec 2001]
AOL Time Warner has launched its long-awaited MusicNet online music subscription service, which it will offer for $9.95 a month. AOL's move into the online music space is being closely watched by experts who see it as a natural leader in the nascent market. "AOL beginning to sell digital music subscriptions is critically important and potentially cataclysmic for a lot of retailers out there in the long run," says a Jupiter Media Metrix analyst. Meanwhile, RealNetworks just launched its service, dubbed RealOne, last week and AOL rival Microsoft's MSN service is poised to launch its competing Pressplay service in the next few weeks. MusicNet is jointly owned by AOL's Warner Music, RealNetworks, EMI and Bertelsmann. Pressplay is owned by Vivendi Universal and Sony. (Wall Street Journal 12 Dec 2001)
http://interactive.wsj.com/archive/retrieve.cgi?id=SB1008087024649633040.djm (sub req'd)

Category 19.2 *Music piracy*

2001-12-19 **music peer-to-peer networking copyright intellectual property rights infringement lawsuit judgement service alternative**

NewsScan

VIVENDI, SONY PLAN A DUET [23 Feb 2001]
Vivendi Universal and Sony are teaming up to launch an online "virtual jukebox" music service this summer. Duet, as it's called, will challenge the recently announced deal worked out between Napster and Bertelsmann to offer a subscription-based Napster service. "It is an alternative to Napster which will allow us to monitor exactly which titles have been listened to and downloaded," says the head of Vivendi's Universal Music France. "It is over a secure network that prevents the item from getting distributed all over the Internet and provides better sound quality." Sony and Vivendi will have equal ownership of Duet and will offer a subscription service and a pay-per-listen option. (Reuters/Los Angeles Times 23 Feb 2001)
http://www.latimes.com/business/20010223/t000016279.html

YAHOO JOINS DUET WITH VIVENDI AND SONY [6 Apr 2001]
Yahoo has inked a deal with Vivendi Universal and Sony to deliver music over the Net. The new alliance, which calls for Yahoo to provide worldwide distribution for Duet, the online music platform being developed by Universal and Sony Music, will add a much-needed channel to Vivendi's U.S. distribution network. The alliance comes only days after the three other big music companies -- AOL Time Warner, Bertelsmann and EMI -- launched their MusicNet initiative with RealNetworks. "We're really jazzed about this," says Jeff Mallett, Yahoo's president and COO. "It provides our 100 million registered users with access to the premier entertainment destination." (Financial Times 6 Apr 2001)
http://news.ft.com/news/industries/internet&e-commerce

VIVENDI MAKES A PLAY FOR MP3.COM [21 May 2001]
Vivendi Universal, the world's second largest media group, is buying online music distributor MP3.com for $372 million in cash and shares. The amount is considerably less than MP3's peak valuation, but values the company at 3.1 times its estimated 2001 earnings. The purchase is Vivendi's third and most substantial move this year in terms of opening up new U.S. distribution channels. In March, Vivendi and Sony announced their Duet collaboration, an online music distribution service, and last month Vivendi announced a separate music deal with Yahoo. (Financial Times 21 May 2001)
http://news.ft.com/news/industries/internet&e-commerce

VIVENDI AND AOL CHARGED WITH CD PRICE-FIXING [1 Aug 2001]
The Federal Trade Commission has accused Warner Music (a unit of AOL Time Warner) and PolyGram (now a part of Vivendi) of colluding in 1998 to fix prices on CDs, cassettes and videos of opera singers Placido Domingo, Luciano Pavarotti, and Jose Carreras, knowns as "The Three Tenors." Neither company has admitted wrong-doing, but AOL has settled the case and Warner "has made the business decision to resolve this matter amicably rather than engage in protracted adversarial proceedings." (Washington Post 1 Aug 2001)
http://www.washingtonpost.com/wp-dyn/articles/A12775-2001Jul31.html

VIVENDI PUTS A LOCK ON ITS MUSIC CDs [26 Sep 2001]
Vivendi Universal's Universal Music Group, the world's biggest music company, says it is preparing to roll out "a number of releases" on CDs that contain technology preventing consumers from making digital copies. The move is the most aggressive to date among U.S. record labels to block copying onto computers and other devices. A company spokesman declined to say exactly what technology would be used, but said it "will not impede the consumer experience." Meanwhile, Sony Music Entertainment reported it has used copy protection on some promotional releases of its new Michael Jackson single that were sent to radio stations last month, but doesn't plan to use on commercial releases of the singer's new album. However, the company affirmed that its "goal is to implement copy protection on a broader basis to deter digital piracy." BMG Entertainment said it's conducting trials of copy-protection on promotional CDs in the U.S. and Warner Music is "looking closely at the technology" and doing market research on the concept. No comment was available from EMI. (Wall Street Journal 26 Sep 2001)
http://interactive.wsj.com/archive/retrieve.cgi?id=SB1001427903167857240.djm (sub req'd)

PRESSPLAY SET TO LAUNCH TOMORROW [19 Dec 2001]
The long-awaited online music service backed by Sony and Vivendi Universal will launch tomorrow, offering a tiered service priced between $9.95 and $24.95 a month for users who want to access music through their computers. Pressplay, which will offer 14-day free trials, has differentiated itself from rival MusicNet by allowing some users to "burn" a limited number of songs based on which tier of service is selected. The $24.95 Platinum Plan allows users to "stream" 1,000 songs, download 100 songs, and "burn" 20 songs a month. Subscribers are limited to no more than two songs from a particular artist each month. The pressplay service will be available through MSN Music, Roxio and Yahoo. (Wall Street Journal 19 Dec 2001)
http://interactive.wsj.com/articles/SB1008716795123839160.htm (sub req'd)

Category 19.2 *Music piracy*

2002-01-10 **music copyright intellectual property marketing distribution subscription**

NewsScan

NAPSTER GETS READY FOR REBIRTH AS SUBSCRIPTION SERVICE [10 Jan 2002]
Napster, the Internet file-swapping service that was plagued by lawsuits accusing it of violating the intellectual property rights of music producers and artists, has launched a new six-week trial in which 20,000 volunteers will swap music files legally. The company will offer 50 downloads per month for about $5-10, and will be using improved file identification technology. A Napster spokesman says the company is "close to getting all major label content." (AP/New York Times 10 Jan 2002)
http://www.nytimes.com/aponline/technology/AP-Napster.html

Category 19.2 *Music piracy*

2002-01-24 **music peer-to-peer networking copyright infringement bootleg intellectual property rights infringement lawsuit judgement**

NewsScan

NAPSTER LAWSUIT ON HOLD WHILE PARTIES RECONSIDER SETTLEMENT [24 Jan 2002]
U.S. Federal District Judge Marilyn Patel has granted a request by Napster and four record companies to suspend for 30 days the lawsuit brought by the record industry charging Napster, the Internet music-swapping service, with illegal distribution of copyrighted material. The four record companies joining Napster in the request were AOL Time Warner, BMG, Vivendi Universal and Sony; a fifth company, EMI, declined to participate in the request. Napster is gradually transitioning itself from a free to a paid-subscription service, and Hilary Rosen of the Recording Industry Association of America says of Napster: "We understand they have limited their repertory to licensed music. Resolving the lawsuit may now be feasible." (New York Times 24 Jan 2002)
http://partners.nytimes.com/2002/01/24/technology/ebusiness/24NAPS.html

---

Category 19.2 *Music piracy*

2002-02-26 **intellectual property music piracy e-commerce**

NewsScan

RIAA: PUT ANOTHER NICKEL IN THAT NICKELODEON FOR MUSIC, MUSIC, MUSIC
The music industry is desperate to find a way of downloading a solution to the problem of illegal downloading of copyrighted songs. The Recording Industry Association of America (RIAA) says that shipments by record companies to consumers have dropped by more than 10% in the past year, and RIAA president Hilary Rosen complains: "When 23% of surveyed music consumers say they are not buying more music because they are downloading or copying their music for free, we cannot ignore the impact on the marketplace. " (Reuters/New York Times 25 Feb 2002)
http://partners.nytimes.com/reuters/technology/tech-leisure-music.html

---

Category 19.2 *Music piracy*

2002-02-28 **music peer-to-peer networking copyright intellectual property rights infringement lawsuit judgement service alternative**

NewsScan

SONY LICENSES MUSIC TO SONG-SWAPPING SERVICE [28 Feb 2002]
Peer-to-peer music-swapping service CenterSpan Communications says it's clinched a deal to distribute Sony Music Entertainment songs, marking the first time a major record label has licensed its content to a file-sharing outfit. CenterSpan bought the file-swapping Web site Scour.com after it declared bankruptcy in 2000. The pact calls for CenterSpan to pay Sony about $2 million in cash plus 283,556 shares and a warrant to buy 189,037 additional shares at $8.11 per share. A CenterSpan spokesman said the company is also talking to other record labels and movie studios, as well as online music subscription services such as Pressplay. "The deal continues the experimental phase the music industry is going through as it tries to figure which digital distribution model is going to work," says a GartnerG2 analyst. (Reuters 28 Feb 2002)
http://story.news.yahoo.com/news?tmpl=story&cid=581&u=/nm/20020228/tc_nm/media_centerspan_sony_dc_1

Category 19.2 *Music piracy*

2002-05-06 **intellectual property P2P peer-to-peer file sharing music download piracy sales surveys**

NewsScan

DOES FREE ONLINE MUSIC MAKE FANS WANT TO BUY?
The market and consumer research firm Jupiter Research has issued a report reports that, contrary to what the music industry thinks, music file-sharing networks such as Kazaa and Music City are actually good for business: "File-sharing is a net positive technology", says the report, because "it gets people enthusiastic about new and catalog music." But not so fast there. Hart Research Associates, in a study prepared in November for the Recording Industry Association of America, came to just the opposite conclusion: "People who love music and buy it and who also use file-sharing services would be buying more of it were it not for the availability of free music online." The correct answer? Pay your money and take your choice. (New York Times 6 May 2002)
http://partners.nytimes.com/2002/05/06/technology/06MUSI.html

---

Category 19.2 *Music piracy*

2002-05-15 **music swapping copyright intellectual property music piracy bankruptcy purchase ownership**

NewsScan

NAPSTER PONDERS BANKRUPTCY
Napster is considering filing for Chapter 7 bankruptcy protection following the breakdown of talks with Bertelsmann, which wanted to take a majority stake in the online music swapping business. Bertelsmann was offering between $15-20 million for the stake, but the board was split between John Fanning, uncle of Napster founder Shawn Fanning, and former Napster CEO Hank Barry and John Hummer of Hummer Winblad Venture Partners. At the same time, Napster CEO Konrad Hilbers, Shawn Fanning, who serves as chief technology officer, and four other vice presidents announced their resignations. Bertelsmann may still be able to lay claim to Napster's technology, which was used as collateral for the $85 million in loans it has already made to the company. The failure of Napster would signal a major victory for the entertainment industry in the battle for control over digital music and film, but some Silicon Valley groups warn such a view may be short-sighted: "Hollywood needs to offer a legal and suitable legitimate opportunity for downloading movies," said Intel chairman Andy Grove. "It is self-protection. But technology always wins in the end." (Financial Times 15 May 2002)
http://news.ft.com/news/industries/internet&e-commerce

BERTELSMANN BUYS NAPSTER'S ASSETS FOR A SONG
Bertelsmann is acquiring Napster's brand and products for $8 million and will forgive $85 million in loans it has already made to the online music swapping service, which is in the process of filing for Chapter 11 bankruptcy protection. The announcement came as a surprise, because negotiations over a possible sale had broken down last week -- at that point, Bertelsmann was offering $15-20 million for the company. Under the new deal, Konrad Hilbers and Shawn Fanning, who had resigned last week, will rejoin, with Hilbers assuming the position of chairman in addition to his earlier role as CEO, and Fanning re-assuming his title of chief technology officer. Bertelsmann hopes to relaunch Napster as a paid service. It is already a backer of MusicNet, which it operates in combination with AOL Time Warner and EMI Group, and sources close to the company say it has not yet decided how it will position the two separate online music ventures. (Financial Times 17 May 2002)
http://news.ft.com/news/industries/media

Category 19.2 *Music piracy*

2002-05-28 **intellectual property copyright music piracy lawsuit**

FindLaw Download This 87

MUSIC INDUSTRY TAKES SONG-SWAPPING SITE TO COURT
In its latest attempt to halt music piracy, a contingency of music industry groups, including the labels, songwriters and music publishers, filed a lawsuit against American file-sharing Internet service Audiogalaxy.com. The Recording Industry Association of America (RIAA), a powerful trade association for the music labels, and the National Music Publishers Association (NMPA), filed the suit on Friday in a New York federal court.
http://news.findlaw.com/entertainment/s/20020528/medialawsuitdc.html

View the Complaint (ZOMBA RECORDING, CORP. v. AUDIOGALAXY, INC.)
http://news.findlaw.com/hdocs/docs/recordcos/zmbaudglxy52402cmp.pdf

---

Category 19.2 *Music piracy*

2002-06-19 **P2P peer-to-peer networks search engines bots investigation intellectual property movies films piracy**

Edupage

SOFTWARE SEARCHES FOR ILLEGAL MOVIES
A software program called Ranger searches Web sites, chat rooms, newsgroups, and peer-to-peer file-sharing sites for illegal movies on behalf of film studios represented by the Motion Picture Association of America. Ranger covers 60 countries, searching in English, Chinese, and Korean for pirate movie sites. Some of its targets object to the software's findings, however. Internetmovies.com has filed suit against the MPAA because Ranger identified its Web site as a movie pirate in 2001, prompting the company's Internet service provider to stop access.
Washington Post, 18 June 2002
http://www.washingtonpost.com/wp-dyn/articles/A5144-2002Jun18.html

---

Category 19.2 *Music piracy*

2002-06-19 **P2P peer-to-peer network file sharing permission settlement copyrght intellectual property music piracy**

EDUPAGE

AUDIOGALAXY TO SEEK PERMISSION FOR SWAPS
Audiogalaxy agreed to obtain permission from a songwriter, music publisher, or recording company to use and share copyrighted music before allowing people to swap copyrighted songs using its file-trading service. The concession was part of an out-of-court settlement with the Recording Industry Association of America, National Music Publisher's Association, and Harry Fox Agency, which sued the company a year after Audiogalaxy began filtering copyrighted music from its system. The plaintiffs claimed that the filters failed to perform adequately. Audiogalaxy also agreed to pay an undisclosed sum to settle the suit. It remains to be seen whether the company can survive without the free music services it offered previously. Napster, which shut down after its filters failed to perform adequately, has not resumed service. CNET, 18 June 2002
http://news.com.com/2100-1023-936932.html

Category 19.2 *Music piracy*

2002-06-21 **music piracy file-swapping network copyright intellectual property patent law court bankruptcy assets licenses**

EDUPAGE

NAPSTER TECHNOLOGY OWNERSHIP CHALLENGED
PlayMedia Systems claims that it provided key parts of the Napster technology, which cannot, therefore, automatically be transferred to Bertelsmann in its purchase of Napster's assets. PlayMedia created the MP3-playing functions of Napster's original file-swapping software and security features of the planned subscription service. PlayMedia representatives said that the company does not plan to interfere with the bankruptcy proceedings and sale of assets to Bertelsmann, but wants to protect its technology licenses during those proceedings.
CNET, 19 June 2002
http://news.com.com/2100-1023-937459.html

Category 19.2 *Music piracy*

2002-06-28 **P2P peer-to-peer music piracy countermeasures intellectual property copyright violations information warfare theft spoofing denial-of-service attack swamping corruption**

NewsScan

MUSIC INDUSTRY WAGES GUERRILLA WARFARE AGAINST P2P SERVICES
In a practice called "spoofing," the music industry has been swamping online music-swapping services like Morpheus, Kazaa, and Grokster with thousands of phony or mangled music files rather than the sought-after songs. One music executive, speaking anonymously, says: "We're not using any of this with any kind of promotion or marketing in mind. We're doing this simply because we believe people are stealing our stuff and we want to stymie the stealing." And Cary Sherman, president of the Recording Industry Association of America, says: " From the outset, it's been very clear that one of the only ways -- as a practical matter -- to deal with the peer-to-peer problem is by means of technological measures. There are certainly mechanisms that are available -- that are completely lawful, such as spoofing." (San Jose Mercury-News 27 Jun 2002)
http://www.siliconvalley.com/mld/siliconvalley/3560365

Category 19.2 *Music piracy*

2002-07-03 **intellectual property lawsuit prosecution peer-to-peer swapping P2P**

NewsScan

MUSIC LABELS PLAN ACTION AGAINST INDIVIDUAL SONG-SWAPPERS
The major music labels, working through the Recording Industry Association of America, are preparing to file copyright lawsuits targeting high-volume song providers on peer-to-peer music services. The suits will be part of a broader effort, including a PR campaign that may feature prominent artists urging fans to respect copyright laws. The industry's new legal tack is a marked shift from earlier efforts, which had focused on putting peer-to-peer music services such as Napster, Morpheus and Kazaa out of business. People close to the situation say the RIAA is still in the early stages of planning its efforts and hasn't decided yet exactly what actions should trigger such a lawsuit, although it's agreed that legal retaliation would focus on individuals who supply the largest amounts of music, as well as so-called "supernodes," or people who provide the centralized directories that enable online music-sharing. Suits against individual Internet users could cause a backlash from some fans, but record companies say they have no choice as they face diminishing music sales while home CD-burning has soared. (Wall Street Journal 3 Jul 2002)
http://online.wsj.com/article/0,,SB1025639431553502280.... (sub req'd)

Category 19.2 *Music piracy*

2002-08-22 **intellectual property ISP Internet service provider international jurisdiction music piracy lawsuit**

NewsScan

RECORD LABELS SUE ISPs OVER CHINA-BASED SITE
The world's major record labels have sued the major U.S. Internet service and network providers, alleging that their routing systems enable users to access the China-based Listen4ever.com Web site, which provides access to downloadable music from a central location containing thousands of files. The suit alleges that Listen4ever uses offshore servers located in China to host the site where the illegal copying occurs, but that the site uses a U.S. domain name, is written entirely in English, and appears to target an American audience by focusing on U.S. works by artists such as Bruce Springsteen, Red Hot Chili Peppers, Eric Clapton and Whitney Houston. Plaintiffs include units of Vivendi Universal, Sony, Bertelsmann and AOL Time Warner. Defendants in the suit are AT&T Broadband, Cable & Wireless USA, Sprint, Advanced Network Services and UUNet Technologies. (Reuters 17 Aug 2002)

MUSIC PIRACY SITE IN CHINA SHUTS DOWN
The Recording Industry Association of America and 13 record companies have dropped a lawsuit against four Internet service and network providers they'd sued for providing services to Listen4ever.com, a Chinese Web site accused of distributing pirated music. Apparently Listen4ever.com has ceased operation, making the suit unnecessary unless its owners resume activity under a new name or location. The defendants in the lawsuit were AT&T Broadband, Cable & Wireless, Sprint, and WorldCom's UUNet. (AP/USA Today 22 Aug 2002)

Category 19.2 *Music piracy*

2002-09-26 **intellectual property music download e-commerce**

NewsScan

ALBUM LAUNCHES IN STORES AND ON THE WEB SIMULTANEOUSLY
Music artist Peter Gabriel is exploring ways to incorporate legitimate music downloading into the distribution strategy for his latest album, "Up." On Tuesday, at the same time CDs were arriving at music stores to be sold, the album was also available online as a hi-fidelity download embellished with several security features to prevent unauthorized sharing. The online album is priced at $9.99 while the CD version carries a list price of $18.98. The downloaded version can be transferred to digital audio players supporting Microsoft's Windows Media Audio format and can also be burned up to two times on blank CDs. While some popular singles have been offered for sale online in the recent past, Gabriel's is the first full-length release from a major artist. (AP 26 Sep 2002)
http://apnews.excite.com/article/20020926/D7M9GBP82.htm

Category 19.2 *Music piracy*

2002-10-11 **intellectual property copyright piracy education ethics universities P2P peer-to-peer privacy**

NewsScan

COLLEGES TOLD STUDENT PIRACY "OUT OF CONTROL"
A letter sent to more than 2,000 university presidents by the Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA) says: "We are concerned that an increasing and significant number of students are using university networks to engage in online piracy of copyrighted creative works. We believe there must be a substantial effort, both disciplined and continuous, to bring this piracy under control... Students must know that if they pirate copyrighted works they are subject to legal liability. It is no different from walking into the campus bookstore and in a clandestine manner walking out with a textbook without paying for it." (Cnet 11 Oct 2002)
http://news.com.com/2100-1023-961637.html

Category 19.2 *Music piracy*

2002-11-27 **university students policies copyright infringement intellectual property education ethics violations**

NewsScan

STUDENTS EVADE UNIVERSITY TACTICS TO PROTECT MEDIA FILES
As colleges and universities across the country take steps to rein in rampant unauthorized file downloading, students are ignoring policy changes that discourage such activities and are becoming more adept at circumventing technology blockades. "If you don't know how to do it, other people will just tell you," says one student. "There's not much they can do to stop you." And while university administrators are moving to placate entertainment companies complaining of student abuses, there's a pragmatic motivation at work as well — a large portion of most universities' bandwidth is being devoured by students' insatiable demand for online entertainment. Schools have closed off file-trading portals such as Kazaa, but the newest version of the Kazaa software includes a "port-hopping" feature that automatically seeks out open ports for its downloading activities. "It's an ongoing battle," says one network administrator. "It's an administrative nightmare trying to keep up." Meanwhile, schools appear conflicted in their quest for more ethical behavior among their students. "The biggest problems that universities are having is they have not openly decided whether their primary responsibility in this regard is law enforcement or education," says Virginia Rezmierski, who teaches in the University of Michigan's School of Information and recently surveyed universities on their monitoring practices. "Right now they're doing more monitoring than education." (New York Times 27 Nov 2002)

Category 19.2 *Music piracy*

2002-12-04 **music piracy peer-to-peer networking downloads copyright intellectual property alternative distribution lawsuits trademark infringement**

NewsScan

PRESSPLAY DEBUTS, AIMSTER RESURFACES AS MADSTER [23 Jan 2002]
Pressplay, the online music distribution service backed by Sony and Vivendi Universal, announced its launch this week following about a month of public testing. U.S.-based subscribers will be able to receive up to 300 streamed tunes on demand, as well as up to 30 downloads each month for $9.95. Heavy users can opt for a $24.95 deal that provides 1,000 songs and 100 downloads. Unlike rival MusicNet, pressplay subscribers will be able to burn a limited number of songs onto their own CDs. Meanwhile, renegade music-downloading Web site Aimster has resurfaced under a new moniker — Madster, named after company founder John Deep's daughter Madeleine. Aimster had been under siege by AOL Time Warner, which that the "Aimster" name and Internet domain infringed on its trademarked AIM instant messaging software. (Newsbytes 23 Jan 2002)
http://www.newsbytes.com/news/02/173858.html

INJUNCTION AGAINST MADSTER
A U.S. district court in Chicago has ruled in favor of the record companies and the Recording Industry Association of America, which had sued the file-sharing company Madster over the use of its file-swapping services by individuals who misappropriated copyrighted music. The said Madster?s very reason for being seemed to be "the facilitation of and contribution to copyright infringement on a massive scale." Madster founder Johnny Deep says his company has no way of knowing how people are using the service, since the files are all encrypted. More to come. (AP/San Jose MercuryNews4 Sep 2002)
http://www.siliconvalley.com/mld/siliconvalley/4003605

JUDGE ORDERS MADSTER TO SHUT DOWN
A federal judge in Chicago has issued a temporary restraining order against Madster, telling it to immediately disable its file-servers. U.S. District Judge Marvin Aspen said that record labels "will continue to suffer irreparable harm" otherwise. The Madster Web site continued to advertise $4.95 a month memberships last night, although downloads of the company's file-sharing software were not available. Lawsuits against Madster (formerly Aimster) had been on hold following its March bankruptcy filing, but a bankruptcy judge recently lifted the stay for the purpose of allowing plaintiffs to seek a preliminary injunction motion. That motion was issued October 30, but the service disregarded the order, which set the stage for yesterday's restraining order. The order is in effect through December 22, barring further notice from the court. (AP 4 Dec 2002)
http://apnews.excite.com/article/20021204/D7NMPD1G0.html

Category 19.2 *Music piracy*

2002-12-04 **intellectual property piracy legal action international lawsuits threats privacy ISP Internet service providers**

NewsScan

DANISH ANTI-PIRACY GROUPS SENDS BILLS TO VIOLATORS
The Copenhagen-based AntiPiratGruppen, an organization whose efforts to stop theft of digital media are supported by the Danish entertainment industry, has found a new strategy. Instead of attacking Internet service providers for allowing copyright violations to happen, the organization goes directly against the violators themselves, sending them bills ranging from $130 to $13,300. (The $13,300 bill went to a disc jockey). If the recipients of bills do not pay up they will be sued. Various Danish newspapers and consumer groups are upset that Internet service providers have cooperated with AntiPiratGruppen by helping it identify copyright violators. (AP/USA Today 4 Dec2002)
http://www.usatoday.com/tech/news/techpolicy/2002-12-03-music-swap_x.htm

---

Category 19.2 *Music piracy*

2003-01-31 **copyright intellectual property music piracy prosecution investigation legal proceeding injunction subpoena identity ISP Internet service provider**

NewsScan

MUSIC INDUSTRY PRESSURES VERIZON ON FILE-SWAPPER'S IDENTITY
The Recording Industry Association of America is pressuring a federal judge to force Verizon to reveal the identity of an Internet service subscriber accused of illegally trading copyrighted songs. Verizon general counsel Sarah Deutsch says if the judge capitulates, it would set a precedent that would harm the privacy rights of Verizon's ISP customers and could force other ISPs to give up the names of subscribers without judicial review. Verizon has already agreed to hand over the information if the RIAA files a separate "John Doe" suit against the alleged file-swapper, but the RIAA refused, saying that anti-piracy laws don't require a separate lawsuit. The Verizon subscriber who's the focus of the controversy is accused of sharing thousands of songs on the Kazaa network, and is located in the Pittsburgh area. Deutsch pointed out that the person in question may be totally unaware of the dispute. "Our general policy is to inform a user when we receive a subpoena. Since in our view this isn't valid, we haven't gotten the customer involved in the debate." (AP 4 Oct 2002)
http://apnews.excite.com/article/20021004/D7MENVS00.htm

COURT ORDERS INTERNET PROVIDER TO IDENTIFY A SUBSCRIBER
To facilitate the enforcement of the 1998 Digital Millennium Copyright Act, a federal district court judge in Washington has ordered Verizon Communications to identify a subscriber whom the Recording Industry Association of America (RIAA) suspects of using to Internet to make available unauthorized copies of several hundred copyrighted songs. The ruling is significant for at least two reasons. First, it shows that the recording industry is now targeting not only big companies accused of large-scale copyright violations but also individual violators. Second, it indicates that a willingness by the court to compel Internet service providers to yield subscriber information without requiring a copyright holder to file a lawsuit. (New York Times 22 Jan 2003)

VERIZON GOES TO COURT TO DEFEND CUSTOMER PRIVACY
Verizon Communications is asking a federal appeals court to declare unconstitutional a lower-court decision that ordered it to reveal the identity of a customer suspected of downloading copyrighted music files over the Internet. Verizon deputy general counsel John Thorne says, "I see a great jeopardy of privacy for people who are not doing anything wrong," and notes the lower court's ruling would make it possible for "strangers, stalkers, telemarketers, pollsters, creditor and anybody else" to obtain the identity of almost any Internet user. "No matter where you go, your identity can be compelled to be revealed under this process." (Reuters/USA Today 30 Jan 2003)

Category 19.2 *Music piracy*

2003-04-03 **agreement recording industry Internet webcasters**

NewsScan

RECORDING INDUSTRY, WEBCASTERS REACH ROYALTY PACT
In a move to head off a potentially difficult arbitration process, the recording industry and Internet radio operators have agreed on terms for paying royalties to labels and artists for songs played on the Web. The rate set for 2003-2004 is nearly identical to that set by the Librarian of Congress for 2002 — webcasters can either pay a rate of 0.0762 cents per song per listener, or 0.0117 cents per listener hour. Webcasters that sell subscriptions to listeners can also choose to pay 10.9% of their subscription revenue. Both groups appeared to be satisfied with the agreement, which will save them millions of dollars in legal fees by avoiding arbitration. (Wall Street Journal 3 Apr 2003)

Category 19.2 *Music piracy*

2003-04-04 **music piracy lawsuit RIAA**

NewsScan

MUSIC PIRACY VIOLATIONS: $150K A SONG
The Recording Industry Association of America (RIAA) has filed lawsuits against four students it says it misappropriated academic computing resources to "illegally distribute millions of copyrighted works over the Internet." Two of the accused students are enrolled at Rensselaer Polytechnic Institute, one student is enrolled at Princeton, and the fourth is at Michigan Technological University. If they are convicted, they could be fined as much as $150,000 for each song they illegally traded. Digital media analyst Phil Leigh says of the RIAA's action: "This is just another step in the direction of demonstrating to the public that there will be penalties for what they consider to be copyright violations. I think they're attempting to take a carrot-and-stick approach here. They're whacking a few people with a stick now. And the carrot is the more liberal rules relating to label-backed subscription online services." (San Jose Mercury News 4 Apr 2003)

Category 19.2 *Music piracy*

2003-04-14 **Apple legal music download iTunes server**

NewsScan

APPLE TO LAUNCH ITS OWN MUSIC SERVICE
Apple Computer is launching its own music service in the next few weeks, offering users songs from all five major record labels. The new music service will be integrated with Apple's iTunes music software, which is used to organize and play MP3 files on Macs. Rather than following the subscription-based model adopted by the record-label-backed pressplay and MusicNet services and others, Apple plans to sell its songs individually for about 99 cents a track. And while the service is rumored to be more consumer-friendly than many of the other legitimate online music services, it's available only to Mac users — a group that comprises about 5% of the global market. (Wall Street Journal 14 Apr 2003)

Category 19.2 *Music piracy*

2003-04-25 **music industry lawsuit RIAA DMCA Verizon intellectual property rights**

NewsScan

JUSTICE DEPT. SUPPORTS MUSIC INDUSTRY IN VERIZON CASE
The U.S. Justice Department filed a brief Friday supporting the effort by the Recording Industry Association of America to force Verizon Internet Services to identify a subscriber suspected of violating copyrights by offering more than 600 songs online. Verizon had asked a federal judge to block the subpoena, arguing that it violated the First Amendment's "protection of the expressive and associational interests of Internet users." However, the Justice Dept. filing said the subpoena, which was sought under the Digital Millennium Copyright Act, was legal. The judge will now have to decide the constitutional issue, which is viewed as an important test of the DMCA's applicability in Internet copyright cases. The filing comes as the recording industry is becoming increasingly aggressive in its quest to identify and punish music "pirates." (AP 19 Apr 2003)

JUDGE SAYS IT AGAIN: VERIZON MUST REVEAL CUSTOMERS' IDENTITIES
U.S. District Court Judge John Bates has reaffirmed his previous ruling requiring Verizon to reveal to the Recording Industry Association of America (RIAA) the names of two Verizon customers accused by RIAA of illegally downloading hundreds of copyrighted songs from the Internet. The ruling will probably be appealed to the U.S. Supreme Court, with Verizon asserting that the subpoena is invalid, since it relies on the Digital Millennium Copyright Act (DMCA), yet falls outside the scope of DMCA, which does not cover material that is merely transmitted over a network, and not stored on it. Verizon is asserting that the protection of its customers' privacy takes precedence over the subpoena that was issued. (Internet.com 25 Apr 2003)

Category 19.2 *Music piracy*

2003-04-26 **music services not responsible piracy intellectual property rights copyright peer-to-peer P2P**

NewsScan

GROKSTER AND STREAMCAST: WE DIDN'T DO IT
A federal judge has ruled that two Internet music services that offer peer-to-peer software used by millions of people to share copyrighted music illegally are not themselves guilty of copyright infringement. The judge's reasoning was that, since the technology is also used for many perfectly legal purposes, the two services should not be held responsible in those cases when it happens to be used for illegal purposes. The ruling will be appealed. The music industry insists that the two services, Grokster and StreamCast, are overwhelmingly used by people to exchange copyrighted material, and that legal uses are insignificant. Many industry analysts predict that the industry will soon have to change fundamentally and begin providing inexpensive, easy-to-access music over the Internet. (New York Times 26 Apr 2003)

RULING FORCES ENTERTAINMENT INDUSTRY TO RETHINK STRATEGY
Friday's ruling exonerating Grokster and StreamCast of charges of violating copyright laws will force the entertainment industry to broaden its battle against Internet piracy on three fronts: the courts, in Congress and in the marketplace. In addition to appealing the most recent ruling, the movie studios and record labels may start suing individuals who trade copyrighted files. One music label president, who spoke on condition of anonymity, says the ruling leaves industry no choice: "It makes them [consumers] angrier, but we have no other path right now. It's ridiculous what we're doing, but we have so few options." The industry is also lobbying Congress for stricter anti-piracy laws, and at the same time must find a way to give consumers a compelling alternative to piracy: "The most effective way to combat unlicensed sites is to offer licensed services with reasonable consumer rules at attractive prices," says a digital media analyst at Raymond James. "This attempt to enforce prohibition is a failure." The fact that many of the illegitimate sites are polluted with viruses, pop-up ads and low-quality files creates an opportunity for industry to offer a high-quality, hassle-free online service, he adds. (Los Angeles Times 26 Apr 2003)

Category 19.2 *Music piracy*

2003-04-28 **music piracy countermeasure fails artist Madonna profanity**

NewsScan

MADONNA FIGHTS PIRACY WITH PROFANITY
Madonna and Warner Music Group decided to play a trick on music pirates and hackers responded by defacing her Web site and offering yet-unreleased songs for downloading. It all started when Madonna lent her voice to a popular antipiracy technique. "Decoy" files purportedly carrying her new songs were uploaded onto peer-to-peer file-sharing services, but when unsuspecting fans downloaded them, they heard Madonna saying "What the f*** do you think you're doing??" While some music fans got angry, others saw a creative opportunity and the now-infamous phrase is turning up in dozens of remixes and the computer-aided musical collages called mashups. "Madonna was trying to put one over on the kids… and they in turn wanted to let her know that she's not in as much control as she thinks she is," says TechTV's Morgan Webb. (CNN.com/Reuters/Hollywood Reporter 28 Apr 2003)

Category 19.2 *Music piracy*

2003-04-29 **music downloading legal iTunes Apple Steve Jobs**

NewsScan

JOBS: 'WE BELIEVE IN THE FUTURE OF MUSIC'
Apple Computer launched its iTunes Music Store on Monday in a move that CEO Steve Jobs called "a major milestone in the evolution of the real digital music age. We believe in the future of music." iTunes offers 200,000 downloadable songs for 99 cents apiece and is the first industry-endorsed online music service to forgo subscription fees in favor of a "pay-per-download" business model. Jobs said the real draw for music fans will be the easy-to-use interface and high-quality files available at the iTunes Music Store. "Using current piracy services is very frustrating. It takes you 15 minutes to find and download a song of reasonable quality that doesn't have the last four seconds cut off or a break in the middle. We offer super-fast, high-quality downloads with pristine encoding. You certainly can't get that on any other service — pirate or legal." (Los Angeles Times 29 Apr 2003)

Category 19.2 *Music piracy*

2003-05-03 **music wars piracy freeze lock computers halt downloads intenret connections attack Stanford Law School**

NewsScan

CYCLES OF VIOLENCE IN THE MUSIC WARS
The record industry's options for fighting illegal music downloads from the Internet include some that may be illegal, such as attacking personal Internet connections to slow or halt the downloads, or the use of software called "freeze" that locks up a computer system for a certain minutes or hours and risks the loss of data, as well as software called "silence" that would scan a computer's hard drive for pirated music files and attempt to delete them, at the risk of deleting legitimate music files as well. Stanford Law School professor Lawrence Lessig, who specializes in Internet copyright issues, says: "Some of this stuff is going to be illegal. It depends on if they are doing a sufficient amount of damage. The law has ways to deal with copyright infringement. Freezing people's computers is not within the scope of the copyright laws." (New York Times 3 May 2003)

Category 19.2 *Music piracy*

2003-06-05 **Verizon identity personal information music RIAA illegal download pirated**

NewsScan

VERIZON AGREES TO REVEAL IDENTITIES OF SUBPOENAED CUSTOMERS
Following a federal appellate court's rejection of its efforts to resist a subpoena, Verizon has relented and is releasing the names of four individuals alleged to have illegally downloaded copyrighted music. The music-downloading lawsuit was filed by the Recording Industry Association of America (RIAA), whose president, Cary Sherman, says: "The Court of Appeals decision confirms our long-held position that music pirates must be held accountable for their actions and not be allowed to hide behind the company that provides their Internet service." Privacy advocates and Internet service providers are unhappy with the decision, and some are urging new legislation to prevent the release of the identities of previously anonymous Internet subscribers; however, entrepreneur Jorge A. Gonzales of Zeropaid.com thinks that new laws will be unnecessary: "The technology will move faster than the court systems. The new programs being developed are going to mask users. By the time Verizon has to start turning over a lot of names, the identities of users will be unknown." (New York Times 5 Jun 2003)

Category 19.2 *Music piracy*

2003-06-26 **recording industry RIAA KaZaA Grokster file sharing peer-to-peer**

NewsScan

RECORDING INDUSTRY TO MUSIC SWAPPERS: WE'RE GONNA GET YOU
Cary Sherman, president of the Recording Industry Association of America (RIAA), says his organization plans to file at least several hundred lawsuits within the next 10 weeks against individual computer users who share substantial amounts of copyrighted music online. The RIAA, which represents the five major music labels, will start gathering evidence against file-swappers by using software to scan the public directories of peer-to-peer networks such as KaZaA and Grokster. Sherman says, "A lot of people think they can get away with what they are doing because peer-to-peer file sharing allows them to hide behind made-up screen names. They are not anonymous. The law is very clear. What they are doing is stealing." (New York Times 26 Jun 2003)

Category 19.2 *Music piracy*

2003-07-14 **intellectual property copyright P2P peer-to-peer file-sharing RIAA lawsuits**

NewsScan

DECLINE IN FILE-SWAPPING ATTRIBUTED TO RIAA THREATS
The recording industry's threats to sue individuals who involved in illegal music file-swapping are generating results, according to Nielsen/NetRatings, which reports use of popular file-trading sites such as Kazaa and Morpheus have dropped by 15% since the end of June. "I would definitely say it's not a coincidence that the numbers fell that far," says a Nielsen/NetRatings senior analyst. "A drop this significant probably has some kind of external cause." The Recording Industry Association of America issued its threat on June 25 and says it plans to start filing copyright infringement lawsuits next month. Officials at StreamCast Networks, which distributes Morpheus software, disputed the Nielsen/NetRatings findings, maintaining that there had been no perceptible decline in the number of visitors to its site, and the company plans to release a new version of Morpheus that will enable users to upload and download files through proxy servers in an effort to shield their identities online. (CNet News.com 14 Jul 2003)

Category 19.2 *Music piracy*

2003-07-16 **music download service Buy.com legal**

NewsScan

BUY.COM'S NEW MUSIC DOWNLOAD SERVICE
Buy.com, a mainstream Internet shopping site, will soon be offering a new music download service that (like the Apple iTunes Music Store) will sell individual music tracks without collecting an up-front monthly subscription fee. Since Apple has not yet developed a Windows version of its service, the PC music market offers a broad target for a company such as Buy.com, which will try to surpass its much larger rival, Amazon.com, which has 34.5 million monthly visitors compared to Buy.com's 3.1 million, according to Nielsen/NetRatings. (San Jose Mercury News 16 Jul 2003)

Category 19.2 *Music piracy*

2003-07-16 **P2P peer-to-peer file-sharing corporations traffic slowdown**

NewsScan

P2P PERVADES THE CORPORATE SUITE
Peer-to-peer file-swapping software is deeply entrenched in corporate networks, according to a study of 560 companies by Canadian firm AssetMetrix, which found that 77% of the companies reported P2P applications such as Kazaa and Morpheus installed. Among companies with more than 500 employees, 100% had at least one P2P program installed. "Corporations are frantic about how to rein in some control over this," says AssetMetrix president Paul Bodnoff. "Like with software licenses, most companies want to be on the right side of the law. The challenge is how they do that." In addition to worries over legal liability for employee's file-swapping activities, corporate IT managers say they're also concerned about the drain of resources caused by such activities. Transfers of large media files can bog down legitimate data traffic, and P2P software can also allow viruses to worm their way onto the systems, compromising network security. (CNet News.com 16 Jul 2003)

Category 19.2 *Music piracy*

2003-07-18 **intellectual property peer-to-peer P2P copyright RIAA lawsuits ISP caching**

NewsScan

P2P CACHING PUTS ISPs AT RISK FOR COPYRIGHT VIOLATION
Swedish firm Joltid is marketing its PeerCache technology, which is designed to ease network traffic gridlock by caching frequently traded digital files within file-swapping systems. The software, which has been licensed by three major European ISPs, is built to work with FastTrack, one of the most popular P2P protocols which forms the basis for applications such as Kazaa and iMesh. PeerCache plugs into the ISP network and temporarily caches FastTrack P2P traffic, easing the bandwidth crunch. However, the technology is raising the hackles of the recording industry, which warns that even temporarily storing copyright files could make ISPs accomplices in illegal file trading. "Just using the word 'caching' doesn't mean that the service is automatically exempt from copyright liability," says the IFPI, the international counterpart to the U.S.'s RIAA. Meanwhile, Joltid founder Niklas Zennstrom, who co-founded Kazaa, maintains that European Union laws allow ISPs to temporarily cache traffic on their servers regardless of the file's legal status. "One should bear in mind that [whether] an ISP is caching a file or not does not make the file more or less available for end users. It only impacts the load on the ISP's network. Thus, by caching P2P traffic, ISPs are not encouraging or [discouraging] users to download files. It is just a way for the ISP to organize their network." Zennstrom says PeerCache is being tested by a number of European ISPs. (CNet News.com 18 Jul 2003)

Category 19.2 *Music piracy*

2003-07-21 **intellectual property RIAA lawsuits peer-to-peer file-sharing**

NewsScan

OPPOSING ARMIES LINE UP IN INTELLECTUAL PROPERTY WAR
In an effort to battle Internet theft of copyrighted music, the Recording Industry Association of America (RIAA) has subpoenaed 871 individuals, and demanded that the Internet service providers used by those individuals reveal personal data about them. Verizon's Sarah Deutsch complains, "We've received 150 subpoenas in two weeks. This type of activity is unprecedented." Fred von Lohmann of the Electronic Frontier Foundation says, "The privacy questions are huge. They treat everyone as a copyright infringer, and you're assumed guilty until proven innocent." (USA Today 21 Jul 2003)

Category 19.2 *Music piracy*

2003-07-23 **intellectual propery copyright RIAA file-sharing peer-to-peer P2P universities subpoenas**

NewsScan

SCHOOLS RELUCTANT TO ENFORCE RIAA FILE-SWAP SUBPOENAS
Citing procedural concerns, MIT and Boston College have asked a court to quash subpoenas requesting that they provide the Recording Industry Association of American the identification of certain students accused of illegally downloading copyrighted music. The two institutions merely said that the subpoenas didn't allow for adequate time to notify the students, and a Boston College official explained: "We're not trying to protect our students from the consequences of cspyright infringement. Once the subpoenas are properly filed, we will comply with the subpoenas." The RIAA is trying to discourage illegal file-sharing by pursuing not only large-scale downloaders but small-time ones as well. Some schools (for example, Northeastern University) are complying with the subpoenas without protest. (AP/San Jose Mercury News 23 Jul 2003)

Category 19.2 *Music piracy*

2003-07-24 **copyright intellectual property RIAA lawsuits MP3 P2P peer-to-peer**

NewsScan

RIAA UNLEASHES LAWYERS ON PARENTS, GRANDPARENTS
The Recording Industry Association of America is targeting parents and, in some cases, grandparents of youthful music file-swappers, threatening them with legal action over their offspring's music-sharing activities. The subpoenas have come as a shock to both parents and their children, who assumed that using cryptic nicknames such as "hottdude0587" guaranteed them anonymity. The RIAA says it has cited the numeric Internet addresses of high-volume music downloaders on its subpoenas and can track users only by comparing those addresses against subscriber records held by ISPs, but the Associated Press had no trouble using those addresses and some details culled from the subpoenas to identify and locate some of the targets. Outside legal experts warned that the music industry should move carefully in selecting targets for prosecution. "If they end up picking on individuals who are perceived to be grandmothers or junior high students who have only downloaded in isolated incidents, they run the risk of a backlash," says one Hollywood attorney. (AP 24 Jul 2003)

Category 19.2 *Music piracy*

2003-07-28 **file-sharing P2P intellectual property peer-to-peer tips avoid lawsuit RIAA music piracy**

NewsScan

EXPERTS SHARE TIPS ON AVOIDING FILE-SHARING LAWSUITS
In the wake of the recording industry's unprecedented moves against individual consumers to enforce copyright laws, legal experts are warning people who engage in music file-swapping to immediately stop sharing potentially infringing files or to disable file-sharing software. "…(I)he first thing you should do if you want to be off (the RIAA's) radar is to stop uploading," says Electronic Frontier Foundation senior intellectual property attorney Fre von Lohmann. But whether that strategy will prove successful is uncertain, because the RIAA has been collecting snapshots of individuals' shared file folders since June 26 to use as evidence lawsuits. Even if a file-swapper has since deleted those files, "that snapshot establishes enough evidence to establish infringement," says copyright expert Evan Cox. An RIAA spokeswoman says her group might be "willing to talk settlement" if a file-sharer has erased the evidence, but that will be considered on a case-by-case basis. The RIAA is using a provision included in the 1998 Digital Millennium Copyright Act to issue subpoenas requiring ISPs to disclose the names of suspected infringers, raising the stakes in its battle against unauthorized use of its copyrighted music. "What I think they're going to do is start suing moms and dads and families across America," says California attorney Ira Rothken. "They could lose their house or lose their ability to send their kids to college. That is not the intent of copyright statutes, to bankrupt a middle-class family." (San Francisco Chronicle 28 Jul 2003

Category 19.2 *Music piracy*

2003-07-28 **EFF RIAA subpoena database copyright intellectual property P2P peer-to-peer lawsuits**

NewsScan

EFF SETS UP DATABASE OF RIAA SUBPOENA TARGETS
The Electronic Frontier Foundation has stepped right into the middle of the file-swapping fray, offering potential targets of the subpoenas recently issued by the Recording Industry Association of America (RIAA) a way to check and see if they're on the list.
We hope that the EFF's subpoena database will give people some peace of mind and the information they need to challenge these subpoenas and protect their privacy," says EFF senior counsel Fred Von Lohmann. The database allows people to check their file-sharing "handle" (e.g., hottdude123) against a list of subpoenas issued. If they see their name, they can access an electronic copy of the subpoena, which includes the name of their ISP, a list of songs pirated and the Internet address of the user. By the end of last week, nearly 900 subpoenas had been issued, with 75 additional being added every day. The subpoenas are intended to force the ISPs to divulge the identity of the alleged file-swappers and the RIAA is threatening lawsuits, claiming damages ranging from $750 to $150,000. "The recording industry continues its futile crusade to sue thousands of the more than 60 million people who use file-sharing software in the U.S.," says Von Lohmann. The EFF has teamed with the U.S. Internet Industry Association to set up a Web site called subpoenadefense.org, which provides information on lawyers and other resources for those facing legal action. (BBC News 28 Jul 2003)

Category 19.2 *Music piracy*

2003-08-21 **music download RIAA subpoena lawsuit**

NewsScan

LISTENING IN THE DARK: 'JANE DOE' WANTS TO REMAIN ANONYMOUS
Lawyers for an anonymous Verizon Communications customer known as "Jane Doe," who's accused of illegal music downloading from the Internet, have filed a motion in federal court in Washington, D.C., to assert her privacy and other constitutional rights. So far, the Recording Industry Association of America (RIAA) has issued more than 1,000 subpoenas to Internet service providers demanding the names and addresses of people it intends to sue for illegal use of copyrighted music found online. An RIAA official said the woman's arguments "have already been addressed by a federal judge — and they have been rejected. Courts have already ruled that you are not anonymous when you publicly distribute music online." (Reuters/USA Today 21 Aug 2003)

Category 19.2 *Music piracy*

2003-08-21 **file-sharing peer-to-peer P2P copyright infringement RIAA lawsuit**

NewsScan

ONLINE MUSIC SWAPPERS IN FEAR OF LAWSUITS
A new report from NPD Group, a market research firm, suggests that threats of copyright infringement suits by the Recording Industry Association of America (RIAA) seem to be having a chilling effect on individuals who swap online music. The report indicates that the number of households acquiring music files dropped from 14.5 million in April 2003 to 12.7 million households in May and to only 10.4 million households in June. NPD VP Russ Crupnick says, "Today, file sharing is the most popular method of digital music acquisition. While we can't say categorically that the RIAA's legal efforts are the sole cause for the reduction in file acquisition, it appears to be more than just a natural seasonal decline." (AtNewYork.com 21 Aug 2003)

Category 19.2 *Music piracy*

2003-08-27 **music RIAA lawsuit file-sharing MP3 copyright infringement**

NewsScan

THE RIAA HASHES IT OUT
How is the RIAA tracking down music file-swappers? (RIAA is the Recording Industry Association of America, a music-industry trade association.) It uses a library of digital fingerprints (or "hashes") that uniquely identify MP3 music files traded as far back as May 2000, and compares the hashes of music files on a person's computer against those in the library. Finding MP3 music files that precisely match copies that have been traded online provides evidence that a person may have participated in file-sharing services. One lawyer for a person already charged with illegal file-swapping protests: "You cannot bypass people's constitutional rights to privacy, due process and anonymous association to identify an alleged infringer." (AP/San Jose Mercury News 27 Aug 2003)

Category 19.2 *Music piracy*

2003-09-16 **indentity personal information SBC music downloaders piracy ISP RIAA**

NewsScan

SBC RESISTS SUBPOENAS TO IDENTIFY MUSIC DOWNLOADERS
In another challenge to the recording industry, No. 2 regional phone company and Internet service provider SBC is refusing to comply with subpoenas requiring it and other ISPs to turn over to the Recording Industry Association of America (RIAA) the identities of subscribers suspected of music copyright infringers. SBC's general counsel James D. Ellis sees it as a privacy issue: "Clearly, there are serious legal issues here, but there are also these public policy privacy issues. We have unlisted numbers in this industry, and we've got a long heritage in which we have always taken a harsh and hard rule on protecting the privacy of our customers' information." Matthew J. Oppenheim, a top RIAA executive, says: "SBC believes that free music drives its business. That's the only explanation for why they would relitigate issues that have been resolved." (New York Times 16 Sep 2003)

Category 19.2 *Music piracy*

2003-09-24 **RIAA mistaken indentity DHCP internet EFF attorney Kazaa ISPs**

NewsScan

RIAA WITHDRAWS IN A CASE OF MISTAKEN IDENTITY
The Recording Industry Association of America (RIAA) has withdrawn a lawsuit that accused a 66-year-old woman of illegally downloading and sharing more than 2,000 songs online. An attorney for the Electronic Frontier Foundation says the woman and her husband simply use the Internet to send e-mail to their children and grandchildren. Also, they use a Macintosh, which cannot run the software needed for the Kazaa file-sharing service they are accused of using illegally. The RIAA accusation seems to have been a case of mistaken identity, and the EFF attorney says more mistaken-identity cases are expected because many Internet service providers do not assign IP addresses to any one user but shuffle them around. (San Francisco Chronicle 24 Sep 2003)

Category 19.2 *Music piracy*

2003-10-01 **RIAA peer-to-peer P2P networking crackdown Kazaa**

NewsScan

RIAA CALLS ON P2P TO POLICE NETWORKS
Recording Industry Association of America (RIAA) chairman and CEO Mitch Bainwol suggested at a Senate hearing on Tuesday that Kazaa and other peer-to-peer file-sharing software vendors could institute three reforms that would discourage users from illegal activities: change the default settings so users aren't unwittingly sharing private documents; incorporate "meaningful" warnings about trading copyrighted content; and filter unauthorized copyrighted works off the P2P networks. "The file-sharing business must become responsible corporate citizens… moving beyond excuses. If the Kazaas of the world can institute three common-sense reforms, lawsuits can be avoided, the record industry will be healthier, there will be more jobs, consumers will get the music they want." Kazaa responded that it's already instituted the first two recommendations but that the third would be technically impossible. "If you're going to block the titles of every song, every word in every copyright song, every copyright movie, and every copyright book, you might as well input the whole dictionary," said Philip Corwin, attorney for Kazaa parent Sharman Networks. Meanwhile, rapper LL Cool J said though royalties generated through legitimate online music downloads were small, they were better than nothing. "Some of the artists may only get a nickel out of the 99 cents [charged per song]. Can we at least get that? Is it alright for us to make a living as Americans?" (IDG News Service/InfoWorld 1 Oct 2003)

Category 19.2 *Music piracy*

2003-10-03 **Napster file-sharing peer-to-peer legitimate Roxio**

NewsScan

NAPSTER TO MAKE A COMEBACK
Napster, the digital file-swapping service that had 60 million active users at the time court rulings caused it to go out of business, is planning to relaunch next week as a legitimate music subscription service. The relaunch will be made in a "star-studded gala in New York City" by Roxio, the company that acquired Napster's software last year for $19 million. (Beta News 3 Oct 2003)

Category 19.2 *Music piracy*

2003-10-06 **music download encrypted RIAA crackdown Kazaa**

NewsScan

MUSIC INDUSTRY CRACKDOWN SPAWNS 'CYBER-SPEAKEASIES'
Music download enthusiasts are flocking to 21st century versions of "speakeasies" —high-tech clubs that offer encrypted software designed to shield users from identification and prosecution by a zealous recording industry. Coincidentally, the software now being served up may have broader appeal in the business world as well. "The software that users are moving toward, it has characteristics that businesses need — which is a high degree of privacy, a high degree of security and the ability to handle large files," says New York University telecommunications professor Clay Shirky. "Thanks to the RIAA, ease of use surrounding encryption technologies, which was never a big deal before, is a big deal now." In addition to old favorites such as Kazaa and Morpheus, file-swappers are now turning to newer iterations, such as Blubster, which features both stronger privacy protection as well as easy-to-use encryption and decryption. Another program, called Waste, can be used to set up an encrypted instant-messaging and content-sharing network of 50 users, without the potential liability of a central server. And an offshoot of Freenet, dubbed Locutus, is targeting corporate users with its ability to search corporate networks for information distributed across a wide range of computers. "It's kind of like Google for people's hard disks, but with added security. You can define who has permission to find what kind of files," says Ian Clarke, who heads up Freenet and Locutus parent Cematics. (AP/CNN.com 6 Oct 2003)

Category 19.2 *Music piracy*

2003-10-10 **Napster peer-to-peer RIAA return Roxio file-sharing file-swapping legitiamate legal**

NewsScan

NAPSTER BACK, WITH BLESSING OF RECORDING INDUSTRY
The rapper Ludacris is hailing the return of Napster, which had been forced out of business by lawsuits brought against the once-free music file-swapping service by the recording industry: "To see them come back and do it right, it means the world to the music business. It's a legitimate, cool, fair service that can and will bring artists and fans back together." The new service is being formally released Oct. 29th by Roxio, whose chief executive, Chris Gorog, says: "We have been deeply focused on the liberation of online music from the PC." Napster 2.0 allows subscribers to tune in to the songs that other users are listening to, look at what others have downloaded, and send songs and playlists to other subscribers. (Los Angeles Times 10 Oct 2003)

Category 19.2 *Music piracy*

2003-10-16 **Apple iTunes Windows download music legal**

NewsScan

APPLE iTUNES DOES WINDOWS
Apple is expanding its popular iTunes music download service into Windows territory, promising a wider selection of songs and some new features to maintain its lead in an increasingly competitive market. The launch was accompanied by the usual Apple glitz — CEO Steve Jobs chatted via remote link-up with U2 lead man Bono and the Rolling Stones' Mick Jagger in a prelude to a live performance by singer-songwriter Sarah McLachlan. "It's like the pope of software meeting up with the Dali Lama of integration," gushed Bono — referring to the iTunes software and Apple's integrated online music store. Analysts say that iTunes faces stiff competition in the Windows space, but that its flexibility to download tunes onto multiple devices gives it an edge. "There's going to be a lot of jockeying for position in the next 12 months," says a Forrester Research analyst. "But I think iTunes is a real winner because it has the portable player, the jukebox and the store all together." (Reuters 16 Oct 2003)

Category 19.2 *Music piracy*

2003-10-27 **Napster music download pre-paid card Roxio**

NewsScan

PRE-PAID MUSIC CARDS FROM NAPSTER
The reincarnation of Napster is allowing customers to use prepaid cards to pay for music from the Napster online store. The cards will soon will be on sale at 14,000 electronics retailers and other stores around the U.S. Mike Bebel, head of Roxio's Napster division, says: "We're positive that the effect here is to substantially increase the opportunity for people to engage in online music legitimately. To reach all of the consumers that have in some cases not been reachable through typical channels, we felt that this made sense." Will it be necessary to educate customers in how to use the cards? No, says Bebel: "I'd say the average consumer has a pretty good understanding of what these cards are and what they represent. They wouldn't mistake it for an air freshener." (Los Angeles Times 27 Oct 2003)

Category 19.2 *Music piracy*

2003-11-06 **RIAA delete key households U.S. digital music deleted NDP hardball tactics**

NewsScan

U.S. HOUSEHOLDS HIT THE DELETE KEY
The aggressive campaign waged by the Recording Industry Association of America against illegal music downloads is showing results: 1.4 million U.S. households deleted all the digital music files residing on their computers in August, according to a report by the NPD Group. NPD said recent publicity over the RIAA's hardball tactics prompted the massive cleanup, but added that consumers' overall opinion of the recording industry is suffering because of it. (Reuters/CNN.com 6 Nov 2003)

Category 19.2 *Music piracy*

2003-11-26 **iTunes protection apple software digital rights management Jon Johansen QTFairUse DRM**

NewsScan

NEW SOFTWARE DERAILS APPLE ITUNES PROTECTION
Norwegian computer whiz Jon Johansen is at it again — the teenager best known for writing the DeCSS code that bypasses the copyright protection on DVDs has come up with a new program that does the same thing on Apple's iTunes songs. Johansen's QTFairUse software does not unlock the actual digital rights management (DRM) encryption, but rather intercepts the file while it is streaming, before the DRM gets locked on. The program, categorized as a "memory dumper," works only on Windows-based PCs and requires significant technical expertise to use. For the curious, it can be found on Johansen's Web page at www.nanocrew.net. (Hollywood Reporter/Reuters 26 Nov 2003)

Category 19.2 *Music piracy*

2003-12-23 **internet service providers music intellectual property EFF downloaders**

NewsScan

SUING DOWNLOADERS JUST GOT MORE EXPENSIVE
Friday's court ruling absolving Internet service providers of the duty to reveal subscribers' names when music companies serve them with a subpoena means that the costs for going after people who download music illegally just got a lot higher. Legal experts say the music industry can still bring civil lawsuits against individuals without knowing their names — so-called "John Doe" suits — and then ask a judge for permission to issue subpoenas, but "That's a time-consuming and fairly expensive process," says one intellectual property attorney. Previously, recording industry lawyers had been issuing subpoenas before filing any lawsuits. The new procedure will also allow targeted individuals to contest the subpoenas in court. "It's not going to stop (the recording industry) from filing legitimate claims. It's going to give the targets of those claims procedural protection if they're incorrectly named," says a lawyer for the Electronic Frontier Foundation. "This is certainly a setback for the industry if they're looking to threaten without suing. It raises the stakes all around," says Jonathan Zittrain, co-director of the Berkman Center for Internet and Society at Harvard Law School. (AP/Washington Post 23 Dec 2003)

Category 19.2 *Music piracy*

2004-01-04 **RIAA lawsuits piracy deterrent**

NewsScan

ONLINE PIRACY BEGAN TO DISSIPATE AFTER RIAA THREATENED LAW SUITS

A new study by the Pew Internet & American Life Project shows that the number of music downloaders fell in the past six months from 29% to 14% — and suggests that the drop-off was a consequence of the Recording Industry Association of America's plans to sue Internet users suspected of trading pirated music over file-sharing networks. RIAA Chairman Mitch Bainwol says: "This is another data point that tells us in fact that the lawsuits have had an enormous impact on public awareness about the legality of downloading. For some the prospect of getting sued is a pretty effective deterrent. For most folks, just understanding that it was illegal is enough." (Washington Post 4 Jan 2004)

Category 19.2 *Music piracy*

2004-01-05 **copyright piracy MP3 internet music downloading**

NewsBits; http://www.nytimes.com/2004/01/05/business/media/05song.html

Songwriters Say Piracy Eats Into Their Pay

David Bernstein wrote about the effects of music piracy on songwriters in a January 5, 2004 article in the New York Times. Songwriters' income depends largely on royalties from album sales; with the drop in such sales as a result of widespread theft of music tracks, writers have seen their income decline. For example, veteran songwriter Charles Strouse, 75, saw his income drop by 50% between 2002 and 2003 due to piracy. Typically, writers receive a few pennies for every copy of their music sold; with 2B illegal downloads per month displacing sales, their revenues are seriously affected. Many writers have lost steady jobs at music-publishing companies and are looking for other work.

Category 19.2 *Music piracy*

2004-01-22 **RIAA lawsuits illegal file sharing copyright infringemnet intellectual property rights**

NewsScan

PROVING IT'S SERIOUS, RIAA FILES NEW LAWSUITS

The Recording Industry Association of America (RIAA), the music industry trade group, has filed lawsuits against 532 people it's accusing of illegally sharing music downloaded from the Internet. The lawsuits are intended to show that the recording industry's drive against downloaders will continue. RIAA says: "Our campaign against illegal file-sharing is not missing a beat. We can and will continue to bring lawsuits against those who illegally distribute copyrighted music on peer-to-peer networks." (San Jose Mercury News 22 Jan 2004

Category 19.2 *Music piracy*

2004-01-27 **record labels bypassed MUDDA legal download**

NewsScan

MUSICIANS BYPASS RECORD LABELS WITH NEW ONLINE VENTURE

Rock veterans and Internet enthusiasts Peter Gabriel and Brian Eno are launching a musician's alliance next month that aims to cut the middlemen out of the music sales process by promoting online sales by musicians directly to their fans. The alliance, dubbed the "Magnificent Union of Digitally Downloading Artists" or MUDDA, would allow musicians to set their own prices and agendas, free from the artificial confines of the CD format. Gabriel says he's not trying to shut down the record labels, but wants to give artists more options, building on the success of legitimate download sites such as Apple's iTunes music store. "I'm an artist who works incredibly slowly. If some of those [songs] could be made available, you don't have to be so trapped into this old way of being confined only by the album cycle," says Gabriel. (AP/Los Angeles Times 27 Jan 2004)

Category 19.2 *Music piracy*

2004-02-11 **file music sharing digital piracy anonymous AnonX Kazaa copyright intellectual property rights peer-to-peer Vanavatu**

NewsScan

ANONYMOUS SERVICE MASKS FILE-SWAPPERS

Wyatt Wasicek, a programmer whose day job is working for an Internet service provider, is offering music downloaders who use file-sharing programs such as Kazaa a way to do so anonymously. His service, AnonX, is available for $5.95 a month and provides protection by setting up a virtual private network between the user's computer and the company's servers. The AnonX computers act as proxies, so that the actual users' identities are masked. Wasicek has promised not to divulge the e-mail addresses of his 7,000 subscribers and says he doesn't think he can be forced to do so because AnonX's official owner lives in Vanuatu, the Pacific island nation that also hosts Kazaa's parent company, Sharman Networks. AnonX's servers are located overseas as well. Wasicek says he decided to create AnonX to shield the occasional file-sharer who's unaware of copyright infringement ramifications. "I'm doing this to protect the family with the 13-year-old, not the 25-year-old with 25 movies he's sharing with his buddies. I wanted to go back to the good old days when people could surf anonymously," says Wasicek. (AP 11 Feb 2004)

Category 19.2 *Music piracy*

2004-02-17 **RIAA lawsuits file music sharing intellectual property rights copyrights**

NewsScan

RIAA FILES 531 MORE LAWSUITS AGAINST FILE-SHARERS

The Recording Industry Association of America has filed five separate lawsuits against 531 Internet users that it accuses of illegal file-sharing. The action comes on the heels of four similar suits filed by the RIAA against 532 users last month. All the suits are using the "John Doe" method, which identifies the alleged song-swappers through their numerical Internet addresses. The RIAA is seeking to discover the swappers' names and addresses through court-issued subpoenas. An appeals court in December ruled in favor of Verizon that the RIAA could not force ISPs to divulge the identities of subpoena targets before the lawsuits were filed. Sarah Deutsch, VP and associate general counsel for Verizon, says it has not yet received any subpoenas during this go-round, but is interested to see whether briefs filed by the Electronic Frontier Foundation and American Civil Liberties Union protesting RIAA's tactics will affect the case. "We're waiting for the resolution of the due process issues that have been raised by the public interest groups," says Deutsch. Meanwhile, Nielsen SoundScan, which tracks U.S. music sales, says U.S. album sales are up 10.4% this year compared to the same period in 2003. (Reuters/New York Times 17 Feb 2004)

Category 19.2 *Music piracy*

2004-02-18 **RIAA countersued New Jersey woman scare gang tactics**

NewsScan

TABLES TURNED ON RIAA — ACCUSED FILE-SWAPPER FIGHTS BACK

A New Jersey woman has countersued the Recording Industry Association of America, accusing it of extortion and racketeering tactics in its strategy to sue individual file-sharers. Michele Scimeca's lawsuit is one of "a handful" of countersuits, according to the RIAA. "If someone prefers not to settle, they of course have the opportunity to raise their objections in court," says an RIAA spokesperson. "We stand by our claims." Scimeca contends that by suing file-swappers and then settling the cases before they're brought to trial while threatening potential liabilities that could reach into the hundreds of thousands of dollars, the RIAA is engaging in activities more often associated with gangsters and organized crime. "This scare tactic has caused a vast amount of settlements from individuals who feared fighting such a large institution and feel victim to these actions and felt forced to provide funds to settle these actions instead of fighting," says Scimeca's attorney. "These types of scare tactics are not permissible and amount to extortion." The RIAA has sued a total of about 1,500 people and has settled with 381 of those. (CNet News.com 18 Feb 2004)

Category 19.2 *Music piracy*

2004-03-04 **intellectual property rights copyright music piracy file sharing peer-to-peer P2P Kazaa office raids Australia**

NewsScan

KAZAA RAIDS GET GREEN LIGHT

Australia's federal court has dealt a blow to locally based file-sharing network Kazaa, allowing music industry lawyers and investigators access to material seized in raids on the company's headquarters. The court dismissed an application by Kazaa owner Sharman Networks to have the civil search orders that permitted the February 6 raids stayed, ruling that major record companies should be allowed to examine documents and computer files taken in raids on Sharman's offices and the homes of several executives of the company. (The Australian 4 Mar 2004, rec'd from John Lamp, Deakin University

---

Category 19.2 *Music piracy*

2004-03-10 **peer-to-peer P2P legal music download Napster IBM Superpeer college student**

NewsScan

NAPSTER, IBM TARGET COLLEGES WITH NEW DIGITAL MUSIC SYSTEM

Napster took the wraps off a new "Super Peer" application, which uses IBM's eServer BladeCenter systems to store the most popular music tracks in on-site servers rather than on the Internet. The "Super Peer" application is being marketed to colleges and universities as a way to reduce their computing infrastructure's vulnerability to overuse. Citing usage statistics at Penn State, for instance, of 100,000 downloads and 100,000 streams per day, Napster CTO Bill Pence says storing the most popular songs on-site could save the university an estimated $50,000 in bandwidth fees the first year: "When we embarked on our industry-leading university program, we set out to alleviate the technical and business strains that illegal file-sharing puts on universities and ISPs." (Reuters/Washington Post 10 Mar 2004)

Category 19.2 *Music piracy*

2004-03-23 **lawsuit raid Kazaa offices intellectual property rights peer-to-peer P2P file music sharing**

NewsScan

SEARCH 'MESS' DELAYS KAZAA CASE

The music industry will have to wait until at least May before being granted access to material seized in raids on the headquarters of peer-to-peer network Kazaa. An Australian federal court judge has described the execution of civil search orders as "a bit of a mess," and ordered the seized material held until May. These materials include documents and computer files taken in raids on the office of Kazaa owner Sharman Networks and the homes of several key executives. (The Australian 23 Mar 2004)

Category 19.2 Music piracy

2004-03-30 **music industry internation lawsuit illegal file music sharing peer-to-peer P2P**

NewsScan

MUSIC INDUSTRY TARGETS EUROPEAN FILE-SHARERS

The International Federation of the Phonographic Industry has filed lawsuits against 247 people in Denmark, Germany, Italy and Canada, and warns of "further waves of lawsuits against major offenders" in coming months. The actions in Germany and Italy alleged criminal copyright infringement activity, because a criminal designation is required in order to obtain names from Internet service providers. The lawsuits are aimed primarily at large-scale file-sharers, with one case in Denmark allegedly involving more than 50,000 songs, according to IFPI chairman and CEO Jay Berman. The music industry has blamed piracy, both online and physical, for contributing to a decline in music sales over the past few years, from $38 billion in 1998 to $30 billion in 2003. In Denmark, CD sales have slipped by about 50% in the past four years. "The stealing has got to stop," says Johan Schluter, secretary general of the Danish Recording Industry Association. "Record stores are closing down, and artists find it increasingly difficult to get their music released." (Wall Street Journal 30 Mar 2004)

Category 19.2 Music piracy

2004-04-01 **file-sharing peer-to-peer P2P Kazaa effect music sales**

NewsScan

KAZAA OWNER WELCOMES SURVEY FINDINGS

Sharman Networks, owner of the Kazaa peer-to-peer software, has been quick to seize on the findings of a survey released in the U.S. on Monday which concluded that downloading music had no effect on album sales. In a media release issued last evening, Sharman chief executive Nicola Hemming said "We welcome sound research into the developing peer-to-peer industry and this study appears to have covered some interesting ground. The findings certainly support the vision we've always held for Kazaa and crystallizes our vision for the future of content distribution." The 2002 study was conducted jointly by researchers from Harvard Business School and the University of North Carolina, Chapel Hill, and used data from file-sharing services with 1.75 million downloads being studied over 17 weeks in autumn 2002. "Consider the possibilities if the record industry actually cooperated with companies like us instead of fighting," Ms. Hemming said. "We've offered content providers the opportunity to work with peer-to-peer customers for nearly two years, yet the record industry continues its narrow-minded strategy of litigation and legislation. (The Age, 31 March 2004, rec'd from John Lamp, Deakin University)

Category 19.2 Music piracy

2004-04-08 **copyright music intellectual property rights copy-protected CD**

NewsScan

SOFTWARE BYPASSES CD ANTI-COPYING PROTECTION

A new software program developed by German computer magazine c't (Computertechnik) and RapidSolution Software takes a decidedly low-tech approach to bypassing the copy-protection technologies that some music companies are including in their CDs. UnCDcopy works by recording the analog output from a regular CD player and automatically reconfiguring the analog file into digital format, splitting the file into separate tracks just like the original. The quality of the UnCDcopy version is significantly less than that of a digital copy, but will still work. "This is like CD to tape copying, only brought into the 21st century," says Jim Peters, a representative of the UK's Campaign for Digital Rights. "It will let you defeat any copy prevention system, but in an obvious low-tech way." (New Scientist 8 Apr 2004)

Category 19.2 Music piracy

2004-04-19 **music sharing copyright infringement RIAA amnesty program downloaders disbanded**

NewsScan

RECORDING INDUSTRY DISBANDS AMNESTY PROGRAM

The Recording Industry Association of America (RIAA) has terminated a program that offered to shield individuals from being sued by recording companies if they admitted to illegally sharing music online. Only 1,108 people signed up for amnesty program since it was launched last September, and the RIAA has now filed court papers indicating that the program is no longer necessary or appropriate, and is withdrawing it. Fred von Lohmann of the Electronic Frontier Foundation says the program "was sort of a sham from the beginning," because the RIAA has no way of keeping an individual copyright holder from suing any of the individuals who signed up for it. "The headlines for the amnesty program have dissipated and now it's pretty clear that their main goal is to use the stick of litigation." (AP/San Jose Mercury News 19 Apr 2004)

Category 19.2 *Music piracy*

2004-04-21 **flie-swapping blocker Palisade Systems peer-to-peer P2P copyrighted content**

NewsScan

PALISADE LAUNCHES FILE-SWAPPING BLOCKER

Palisade Systems is launching software that can identify and block copyrighted songs from being traded online. The software, created by Audible Magic, has received support from the recording industry as well as the interest of some higher education institutions who are seeking to gain control over the file-swapping activities of their students. "They want to take the position of not filtering out all peer-to-peer (traffic), stopping copyrighted works but not the other content," says Palisade founder Doug Jacobson. The Audible Magic technology will be included as an option in the newest version of Palisade's PacketHound network-management services. The technology sits inside a network and checks e-mails and other peer-to-peer transfers for audio "fingerprints" that match its database of copyrighted music files. If found, the technology blocks the file transfer midstream. (CNet News.com 21 Apr 2004)

Category 19.2 *Music piracy*

2004-04-23 **Napster backing venture copyright infringement intellectual property rights**

NewsScan

NAPSTER-BACKING VENTURE FIRMS HIT WITH LAWSUIT

Universal Music and EMI Group have filed a copyright infringement lawsuit against Hummer Winblad Venture Partners and two partners — John Hummer and Hank Barry — alleging that the venture capital group contributed to unauthorized copying of music through its $13 million investment in Napster and through Barry's role as Napster's CEO for more than a year. Both men also served on Napster's board. The suit seeks $150,000 per copyright violation plus punitive damages. "Businesses, as well as those individuals or entities who control them, premised on massive copyright infringement of works created by artists should face the legal consequences for their actions," said the two record labels in a joint statement. Hummer Winblad's investment was made in May 2000 — after the recording industry sued Napster for enabling copyright infringement, but the case never made it to trial. Napster filed for bankruptcy protection in June 2003. The National Venture Capital Association is watching the case closely and cautioned that the outcome could have a chilling effect on investment in unproven technologies, thus hampering economic growth. "The concern is that investors are being sued for investing in high-risk companies," says NVCA VP Jeanne Metzger. (Reuters 23 Apr 2003)

Category 19.2 *Music piracy*

2004-04-27 **music piracy bootlegging encouraged David Bowie artist mash-ups prizes**

NewsScan

BOWIE CALLS ON BOOTLEGGERS

David Bowie has invited fans to bootleg his music -- and he's offering prizes for the most creative theft. The musician's Web site invites fans to mix classic Bowie songs with material from his latest album, "Reality" to create a "mash-up" -- a track superimposing the vocal line from one song with the backing tracks from another. The technique has long been employed by record producers, but music software has made it accessible to thousands of "bedroom DJs" - to the alarm of record companies battling to control the distribution of music through the Internet. Bowie, 57, was quoted in The Times, saying mash-ups were "a great appropriation idea waiting to happen." "Being a hybrid maker off and on over the years, I'm very comfortable with the idea and have been the subject of quite a few pretty good mash-ups myself," he said. (The Australian, 27 Apr 2004, rec'd from John Lamp, Deakin University)

Category 19.2 *Music piracy*

2004-05-07 **anonymouse file-sharing music MP2P peer-to-peer RIAA**

NewsScan

TRULY ANONYMOUS FILE-SHARING

Pablo Soto, co-founder of Madrid-based Optisoft, which runs the music-only file-sharing networks Blubster and Piolet on proprietary MP2P peer-to-peer platform, says: "Our users are requesting more and more privacy. They are more than disgusted with the threat of lawsuits." Soto says a new system upgrade should protect Optisoft's users from legal action brought taken by the music trade group the Recording Industry Association of America (RIAA), which has sued a number of Internet users for putting their music collection online for others to download. Soto says, "I do not think it will stop the RIAA from suing our users. But if any of our users has the balls to go to court, I don't see any way on the planet for the RIAA to win." (Reuters/USA Today 7 May 2004)

Category 19.2 *Music piracy*

2004-07-27 **music sharing allowed permitted legal service MusicMatch Napster copyright infringement peer-to-peer**

NewsScan

LIMITED SHARING ALLOWED BY MUSIC SERVICES

MusicMatch is the latest online music service to provide a feature that lets subscribers send e-mail messages with Internet links for songs they want to share. Although Napster 2.0 and other licensed digital music services offer similar options, Napster allows nonsubscribers to listen only
to 30-second song snippets, whereas MusicMatch allows songs to be played by recipients three times before the songs lock. MusicMatch executive Bob Ohlweiler says, "Record companies like the fact that people can tell their friends and acquaintances about music. What the labels don't like about
peer-to-peer is that it's free." Media analyst Phil Leigh says of the limited file-sharing feature: "It will be an incremental feature that could lead them to be more competitive. You'll probably see other people follow MusicMatch's lead, particularly if it proves successful, and my guess is that it will be." (AP/San Jose Mercury News 27 Jul 2004)

Category 19.2 *Music piracy*

2004-07-30 **disc jockey DJ record store music piracy copyright infringement intellectual property rights violation case lawsuit payment Australia**

NewsScan

DJs ORDERED TO PAY IN MUSIC PIRACY CASE

The Federal Court of Australia has ordered five disc jockeys, a record store and its director to pay a total of $140,000 to the owners of copyright, whose music they had copied and sold. The award was in favor of Universal Music, Sony Music Entertainment (Australia) and Warner Music Australia. The DJs who were asked to pay go by the names Moto, Chocolate Boy Wonder, Peter Gunz, Demo, and Tikelz. Record store Anthem Records and its director Joe Sitoa were also asked to pay. The respondents had produced and distributed compilation CDs containing music from some of the biggest names in rhythm and blues, including Ja Rule, Jennifer Lopez and Missy Elliot. (The Age, 30 Jul 2004) rec'd from John Lamp, Deakin U.

Category 19.2 *Music piracy*

2004-08-05 **file sharing peer-to-peer software music piracy copyright infringement encryption law evasion US state attorney general**

NewsScan

STATES TO FILE-SHARING COMPANIES: WATCH OUT

Most of the country's state attorneys general have sent a warning letter to seven companies that promote online file-sharing software such as Kazaa and Morpheus, warning them that there could be legal consequences if they don't adequately inform computer users about the potential risks of using their software. The letter also urged the companies not to add encryption features to their software to hide users' identity: "Encryption only reinforces the perception that P2P technology is being used primarily for illegal ends. Accordingly, we would ask you to refrain from making design changes to your software that prevent law enforcement in our states from investigating and enforcing the law." Adam Eisgrau of P2P United, a trade group that represents several of the firms, says: "Asking us not to use encryption is incredibly shortsighted when there are clear legitimate corporate and public uses for a private network." Fred von Lohmann of the Electronic Frontier Foundation in San Francisco says of the letter: "I'm not aware of any state law that file-sharing violates. This letter is clearly an exercise of political clout on the part of the entertainment industry." (AP/San Jose Mercury News 5 Aug 2004)

Category 19.2 *Music piracy*

2004-08-20 **file sharing music peer-to-peer software copyright law infringement intellectual property rights Sony Betamax**

NewsScan

COURT ON FILE-SWAPPING: GET USED TO IT

A three-judge panel of the 9th Circuit Court of Appeals has ruled that the movie and recording industries can't stretch copyright law to block online piracy of songs and movies. If the decision is appealed, the U.S. Supreme Court could revisit its landmark Sony Betamax ruling that protected
from copyright lawsuits products that have substantial legitimate uses. Whereas the same appeals court ruled against file-sharing service Napster in 2001 because it stored illegally copied files on its central computers, today's peer-to-peer file-sharing networks have no central computers -- and
cannot even monitor users, let alone control them. The court urged the entertainment industry to adapt to file sharing the way movie studios did after losing the Betamax case: "The introduction of new technology is always disruptive to old markets, and particularly to those copyright owners whose
works are sold through well-established distribution mechanisms. History has shown that time and market forces often provide equilibrium in balancing interests, whether the new technology be a player piano, a copier, a tape recorder, a video recorder, a personal computer, a karaoke machine or an MP3 player."(Los Angeles Times 20 Aug 2004)

Category 19.2 *Music piracy*

2004-08-23 **anti-download file sharing peer to peer copyright infringement intellectual property rights student college university**

NewsScan

UNIVERSITIES BEEF UP ANTI-DOWNLOADING TACTICS

Many U.S. universities are greeting returning students with tighter restrictions on using campus networks for illegal music downloading and file-swapping. Until recently, universities had relied on a soft approach -- lecturing students on copyright issues and making them sign pledges to abstain from illegal downloading -- but many are now taking a more hardline stance. Virginia State University recently installed network firewalls that block download sites such as Kazaa and eDonkey -- a move that officials say instantly reduced bandwidth usage from 95% to 51%. The University of Nevada at Las Vegas has installed technology that automatically deletes files saved to communal computers whenever the machines are turned off. "We're not content police. We're bandwidth police," says UNLV associate provost Lori Temple. "We make it so downloading music is a horrible idea." And the University of Florida has developed its own software, Icarus, to detect
illegal downloading by scanning network traffic for peer-to-peer files. A first violation cuts off the student's for 15 minutes -- the second time, the penalty goes up to five days. Meanwhile, other schools are taking the carrot approach, striking deals with legitimate music services, such as the
reincarnated Napster, to offer free or very inexpensive access to streamed music. All these measures are necessary, say college administrators, in order keep their schools off the RIAA's growing lawsuit list. (Wall Street Journal 23 Aug 2004)

Category 19.2 *Music piracy*

2004-08-24 **anti-piracy copyright infringement music file sharing university efforts RIAA praise intellectual property rights**

NewsScan

UNIVERSITIES PRAISED FOR ANTI-PIRACY EFFORTS

Cary Sherman, president of the Recording Industry Association of America (RIAA), says he's pleased with recent efforts by academic institutions to curb illegal copying of copyrighted material: "It's quite clear that every university has gotten the message that this is a serious issue and they're all doing something." At least 20 universities (including Penn State, the University of Miami, and Northern Illinois University) have signed deals with such licensed download services such as Napster 2.0, Ruckus, and RealNetworks to provide students with discounted downloading of free music streaming. (AP/San Jose Mercury News 24 Aug 2004)

Category 19.2 *Music piracy*

2004-08-26 **P2P peer-to-peer police raid seizure evidence intellectual property piracy movies software games network**

http://www.nytimes.com/2004/08/26/technology/26share.html

FBI officers raided six peer-to-peer network operators participating in an illegal file-sharing operation called the "Underground Network."

Investigators infiltrated the network and, according to Saul Hansell, writing in the New York Times, "downloaded 84 movies, 40 software programs, 13 games and 178 songs from the network."

Category 19.2 *Music piracy*

2004-09-20 **Wire magazaine CD experiment artist copyright free copyleft rip burn share distribute peer-to-peer intellectual property rights**

NewsScan

STEAL THIS MUSIC

The editors of Wired magazine have compiled a CD whose contents are meant to be shared, copied, remixed and sampled in an experiment aimed at supporting the Creative Commons concept of intellectual property licensing. About 750,000 copies of "The Wired CD: Rip. Sample. Mash. Share" will be mailed along with Wired's November issue and the disc will also be distributed to audience members at a benefit concert headlined by David Byrne, whose "My Fair Lady" appears on the CD. Other artists include the Beastie Boys, Zap Mama and Gilberto Gil. "The artists were relatively easy to get on board," says Wired editor-in-chief Chris Anderson. "The labels have different priorities. Some of them, once briefed, got it, and some of them never really saw the advantages." Anderson says he approached 50-60 artists in order to come up with the 16 featured on the CD. (Wall Street Journal 20 Sep 2004)

Category 19.2 *Music piracy*

2004-09-27 **music industry Recording Industry Association of America RIAA legal tactics lawsuits overpriced micropayments MP3**

NewsScan <http://www.msnbc.msn.com/id/6037780/site/newsweek/>

MUSIC INDUSTRY SHOULD CHARGE LESS, SELL MORE

The music industry is fighting a losing battle, says Newsweek columnist Steven Levy, who says the RIAA's legal tactics make about as much sense as trying to sue a hurricane: "Technology generates its own form of nature, a set of conditions that enforce an artificial, yet equally unstoppable, reality… For the longest time, the labels viewed digital music as something that could hurt them with hurricane force but made no efforts to adjust to this new reality, let alone exploit it." Levy notes that Real Networks' experiment with sharply cutting prices for digital music -- to 49
cents per song -- was a losing proposition because they still owed 70 cents in royalties for each song sold. But what's impressive is that Real sold six times as much music and took in three times as much money as when they had prices pegged at the industry's 99-cent standard. Levy says that if
labels and artists would agree to smaller royalties, everyone could get richer quicker: "Behind Door One is the money you can make by selling a million copies of a tune. Behind the other door is the money to be reaped by selling 6 million copies at half the price. Do the math, guys!" Not only
that, but lowering prices significantly might just stamp out the scourge of pirated music -- and that's what the labels say they want, right? (Newsweek 27 Sep 2004)

Category 19.2 *Music piracy*

2004-10-04 **copy protection Sony music piracy**

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/9832592.htm

DECLARING VICTORY, SONY ABANDONS COPYRIGHT PROTECTED CDs

Sony's music unit will no longer be selling CDs that use built-in technology to prevent their being copied, because the company has come to the conclusion that its message against illegally copying of CDs has become widely accepted. Sony's persistent dilemma has been how to protect the copyrights on its movies, music and other entertainment assets while at the same time making its electronics devices attractive to consumers.

Category 19.2 *Music piracy*

2004-10-12 **file swapping piracy music RIAA supreme court loss SCOTUS Supreme Court ISP Internet Service Provider DMCA Digital Millennium Copyright Act extension**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A26513-2004Oct12.html

SUPREME COURT TURNS DOWN INTERNET PIRACY CASE

The Recording Industry Association of America has lost a round in its ongoing efforts to use the courts in its battle against online music piracy. The U.S. Supreme Court on Tuesday turned down a request to settle a dispute over whether Internet service providers can be forced to identify subscribers accused of illegally swapping music and video files. Lawyers for Verizon, which had sought to keep subscribers' information private, argued that the recording industry has been quite successful in going after people who trade copyrighted works, having sued more than 3,000 alleged infringers in the past 10 months. The issue turns on the provisions of the 1998 Digital Millennium Copyright Act, which was written before the problem of file-swapping was common. An appeals court earlier ruled that it's up to Congress, not the courts, to expand the law to cover popular file-sharing networks. This latest decision is separate from a petition filed last week by the recording industry asking the Supreme Court to hold Grokster and Streamcast Networks responsible for their customers' file-swapping activities.

Category 19.2 *Music piracy*

2004-10-27 **mp3 RIAA iTunes Napster Musicmatch RealNetworks**

NewsScan; http://news.com.com/From+gold+records+to+gold+MP3s/2100-1027_3-5429377.html

SIGN OF THE TIMES: GOLD MP3s

In a nod to the digital age, the Recording Industry Association of America has issued its first gold, platinum and multiplatinum certifications for digital downloads. RIAA chief executive Mitch Bainwol calls the awards "a reflection of both the commitment of the entire music community to consumer-friendly legitimate digital services and fan appetite for high-quality music." The RIAA based its certifications on sales from legitimate digital download services, including Apple iTunes, Musicmatch, Napster and RealNetworks. And the winner is: Outkast's "Hey Ya!" with more than 400,000 downloads (earning it the only multiplatinum designation). In addition, six songs qualified for platinum (200,000 downloads) and 45 for gold (100,000 downloads). (CNet News.com 27 Oct 2004)

Category 19.2 *Music piracy*

2004-12-06 **music piracy Kazaa Grokster artist**

NewsScan; http://www.nytimes.com/2004/12/06/arts/06down.html

ARTISTS LOVE THE WEB, HATE MUSIC PIRACY

In the first large-scale survey of artists (i.e., filmmakers, writers and digital artists), musicians and the general public, the Pew Internet and American Life Project has found that only about half of the artists polled thought that sharing unauthorized copies of music and movies online should be illegal. Nearly two-thirds of those said filesharing services such as Kazaa and Grokster should be held responsible for illegal fileswapping, while only 15% thought it was a good idea to go after individual users. Among musicians, 37% said the file-sharing services and users should share the blame for illegal file-swapping, while 17% singled out the services as the guilty parties. The survey results indicate that while file-swapping is an ongoing irritant to artists and musicians who see their work distributed for free on the Net, they also value the widescale exposure that the Internet makes possible. "The overall picture is that the musician-artistic community has a much wider range of views and experiences than folks who watch the Washington debate about copyright might imagine," says Lee Rainie, director of the Pew Internet Project. (New York Times 6 Dec 2004)

Category 19.2 *Music piracy*

2005-01-20 **music legal piracy digital downloads**

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/10684757.htm

DO PEOPLE DO ANYTHING BESIDES LISTEN TO MUSIC?

A report from the International Federation of the Phonographic Industry (IFPI) says that music fans in the U.S. and Europe legally downloaded more than 200 million song tracks in 2004 -- compared to just 20 million the previous year. IFPI top executive John Kennedy says, "Digital music is now in the mainstream" -- yet he worries that the digital music market continues to be threatened by piracy. He would like to see the piracy issue placed higher on government agendas and more responsibility shown by Internet service providers for misuse of their networks. (AP/San Jose Mercury News 20 Jan 2005)

Category 19.2 Music piracy

2005-01-25 **music piracy Russia copyright infringement intellectual property international**

NewsScan; http://online.wsj.com/article/0

RUSSIAN MUSIC SITES SPECIALIZE IN CHEAP DOWNLOADS

Russian music sites with names like MP3search.ru and 3MP3.ru provide music fans with a way to bypass the copyright restrictions on most U.S. and European online music services and pay less while they're at it. The sites offer a large selection of highquality downloads with no restrictions for about 10 cents or less per song, but U.S. lawyers warn that downloading music from these sites is just as illegal as downloading from free P2P sites like Kazaa: "It doesn't matter if somebody downloads in the U.S. and believes that it's legal because the site tells them so," says one intellectual property attorney. However, several of the Russian sites say they pay licensing fees to a group called the Russian Organization for Multimedia & Digital Systems (ROMS), which purports to represent Russian copyright holders and acts "in conformity with the requirements of the Russian laws," according to ROMS legal expert Konstantin Leontiev. Meanwhile, the International Federation of the Phonographic Industry says that Russia is second only to China in CD piracy and is threatening legal action against some Russian music sites. (Wall Street Journal 25 Jan 2005)

Category 19.2 Music piracy

2005-02-18 **music piracy Napster copy protection bypass copyright infringement**

NewsScan; http://theage.com.au/articles/2005/02/18/1108609381923.html

USERS BYPASS NAPSTER COPY PROTECTION

Users have found a way to skirt copy protection on Napster's portable music subscription service just days after its high-profile launch, potentially enabling them to make CDs with hundreds of thousands of songs free. Such users are already providing instructions to other would-be song burners through technology websites like BoingBoing. Napster is offering a free trial of its new Napster To Go service, which will enable users for a monthly $15 fee to download as much music as they want and transfer it to a portable device. They can also pay 99 cents for each track they want to burn to a CD. That "rental" model for digital entertainment, backed by giant software concern Microsoft and others, is getting its most serious mass-market tryout yet with Napster To Go. But, according to various Web sites, thwarting the intellectual property protections of the service is as easy as a free software patch. (The Age 18 Feb 2005)

Category 19.2 Music piracy

2005-04-22 **RIAA legal defeat North Carolina student identity disclosure ISP DMCA John Doe lawsuits illegal downloading music piracy intellectual property rights violation copyright infringement**

EDUPAGE; http://chronicle.com/prm/daily/2005/04/2005042201t.htm

JUDGE REJECTS RIAA'S EXPEDITED SUBPOENAS

A federal judge in North Carolina handed the Recording Industry Association of America (RIAA) a legal defeat in its effort to learn the identities of two students accused of illegal file sharing. The RIAA had sought the identities from the students' universities, the University of North Carolina at Chapel Hill and North Carolina State University, under an expedited subpoena process the group has since abandoned. In a December 2003 decision, another federal judge had rejected the expedited subpoenas, which did not require a judge's signature, ruling that Verizon could not be forced to disclose identities of its customers. In their capacity as Internet service providers (ISPs) for students, universities were given similar protection from the expedited subpoenas. In this case, Judge Russell A. Eliason ruled that an ISP that does not store information but merely transmits it cannot be compelled under the Digital Millennium Copyright Act to reveal identities of its users. After the 2003 decision, the RIAA began filing individual "John Doe" lawsuits for illegal file sharing. Under that process, which costs the RIAA more time and money than the other, ISPs can be forced to turn over identities of users. Chronicle of Higher Education, 22 April 2005 (sub. req'd)

Category 19.2 *Music piracy*

2005-06-07 **peer-to-peer P2P legal music downloading services report**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=8721861

MORE CONSUMERS TURNING TO LEGAL MUSIC SERVICES

Growing numbers of U.S. consumers are using legal online music services, making them viable competitors to peer-to-peer (P2P) services, which are typically rampant with illegal file sharing, according to research firm NPD Group. NPD data indicate that Apple's iTunes music store ties for second on a list of the most-used online music services, even with LimeWire and just behind WinMX. Other legal services Napster and RealNetworks's Rhapsody placed seventh and ninth on the list, which also includes such P2P services as Kazaa and BearShare. Isaac Josephson of NPD pointed out that, aside from avoiding the risk of prosecution, legal online music services offer several advantages over P2P networks, including convenience of finding what you're looking for and knowing that files you download do not contain spyware. These factors, coupled with the threat of legal action for copyright violations on P2P networks, make paying for music online an attractive proposition, according to Josephson. Reuters, 7 June 2005

Category 19.2 *Music piracy*

2005-07-27 **study report illegal downloading music piracy purchase intellectual property rights violation copyright infringement**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4718249.stm

STUDY SHOWS DOWNLOADERS BUY SONGS TOO

According to British research firm The Leading Question, illegal file sharers are more likely to purchase legal music downloads than others. Authors of the organization's report characterized as a "myth" the notion that illegal file sharers are simply "mercenaries hell-bent on breaking the law in pursuit of free music." Those who illegally share music are four and a half times more likely to buy music online, according to The Leading Question, indicating that these are users who are enthusiastic about music and are willing to patronize legal online music services if they are sufficiently compelling. A spokesperson from the British Phonographic Industry said the group was pleased with the new report but added that the practice of illegal file trading still is a significant drain on revenues to record labels. The report also found that most users are not likely to start using cell phones as their preferred music devices any time soon. BBC, 27 July 2005

Category 19.2 *Music piracy*

2005-08-19 **college campuses higher education student download habits peer-to-peer P2P intellectual property rights violation copyright infringement**

EDUPAGE; http://www.siliconvalley.com/mld/siliconvalley/12426744.htm

CAMPUSES STILL WORKING TO CHANGE STUDENT DOWNLOAD HABITS

Despite the availability of legal online music services on a growing number of college and university campuses, many students continue to get their music from illegal P2P downloads. At American University in Washington, D.C., only about half of the 3,800 students use the Ruckus music service. A similar percentage was reported for the 10,000 students of the University of Rochester, who have access to Napster. Pennsylvania State University estimates that about 40 percent of its 70,000 students use the Napster service provided to them. For students willing to risk being sued by the entertainment industry and downloading computer viruses, incentives for illegally downloading songs include the ability to copy the songs to CDs and to portable devices and to keep the music after they have left college. Officials from legal online music services acknowledged the hurdles in persuading all college students to abandon illegal file sharing, but they said that offering the services to college students will prove to be beneficial in the long term. San Jose Mercury News, 19 August 2005

Category 19.2 Music piracy

2005-08-22 **intellectual property rights violation copyright infringement music piracy legal download services college campuses RIAA pressure**

EDUPAGE; http://chronicle.com/free/2005/08/2005082201t.htm

COLLEGES CONTINUE TO OFFER LEGAL MUSIC SERVICES

Despite mixed or negative ratings from students, universities offering legal music and movie download services plan to continue doing so for two reasons: students have come to expect it, and legal file swapping remains part of higher education's plan to reduce Internet piracy. Colleges signing up for the services for the first time point to the same reasons. The arrangements are also a visible response to lawsuits filed by the Recording Industry Association of America against students swapping files on campus and the recent U.S. Supreme Court decision holding network administrators liable for individual acts of piracy if they "induced" the infractions. Offering the legal download services provides evidence of a good-faith effort to reduce illegal downloading activity on campus. Chronicle of Higher Education, 22 August 2005

Category 19.2 Music piracy

2005-08-29 **peer-to-peer P2P intellectual property rights violation copyright infringement music piracy file sharing eDonkey benefit BitTorrent crackdown**

EDUPAGE;
http://money.cnn.com/2005/08/29/technology/piracy_crackdown.reut/

EDONKEY BENEFITS FROM BITTORRENT CRACKDOWN

A new study by research firm CacheLogic suggests that the recent crackdown on BitTorrent P2P sites has merely shifted illegal file trading to eDonkey, which now has as many users as BitTorrent in the United States, China, Japan, and Britain. It is the leading P2P service in South Korea, Italy, Spain, and Germany. CacheLogic estimates that as much as 60 percent of global Internet traffic is attributable to P2P file sharing, and before the crackdown, BitTorrent represented up to one third of total Internet traffic. Andrew Parker, chief technology officer of CacheLogic, said the recent upswing of activity on eDonkey "is almost assuredly a result of the increased legal action toward the once-ignored BitTorrent." Parker also noted that the recent U.S. Supreme Court decision against Grokster has not resulted in a decline of file sharing. Parker said, "This cat and mouse game [between P2P services and entertainment industries] will continue." CNN, 29 August 2005

Category 19.2 Music piracy

2005-09-12 **RIAA MPAA Internet2 research laboratory lab anti-piracy efforts**

EDUPAGE; http://chronicle.com/daily/2005/09/2005091202t.htm

RIAA AND MPAA JOIN INTERNET2

The Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA) have become corporate members of Internet2, joining companies including the Ford Motor Company and C-Span. "Internet2 is a stepping stone between the research lab and the commercial sector," said Lauren Kallens, a spokesperson for the organization. Earlier this year, the entertainment groups sued hundreds of Abilene users for using the network to illegally trade files, but, according to Gayle Osterberg, a spokesperson for the MPAA, the groups' membership in Internet2 is unrelated to their antipiracy efforts. "This particular partnership," she said, "is more of an opportunity for us to have a technology testing ground." The groups plan to collaborate with the Internet2 community to study distribution and digital rights management technologies for networks faster than today's commercial Internet. Chronicle of Higher Education, 12 September 2005 (sub. Req'd)

Category 19.2 Music piracy

2005-09-22 **file sharing report peer-to-peer P2P campus higher education efforts**

EDUPAGE; http://www.insidehighered.com/news/2005/09/22/filesharing

REPORT ADDRESSES CAMPUS EFFORTS TO CONTROL FILE SHARING

A report submitted to Congress this week provides a snapshot of campus programs to provide legal alternatives to illegal file trading. Prepared by the Joint Committee of the Higher Education and Entertainment Communities, the report noted that the number of institutions offering legal download services has tripled during the past year, to 70, covering more than 670,000 students nationwide. Campuses offering such services include a number of large and high-profile institutions, and many other colleges and universities are expected to introduce such programs. The report acknowledged that measuring the effect of legal options on student behavior can be difficult, and it noted that large numbers of students at some schools continue to engage in illegal file trading despite the option of a legal service. The most successful approach, according to the report, is for a campus to enforce copyright policies and work to limit illegal file trading while offering students a legal alternative.
Inside Higher Ed, 22 September 2005

Category 19.2 *Music piracy*

2005-09-23 **anti-piracy tool file sharing peer-to-peer P2P MPAA IFPI**

EDUPAGE; http://news.zdnet.com/2100-9588_22-5876687.html

NEW TOOL DEFEATS FILE-SHARING APPLICATIONS

A new tool from the recording and film industries uninstalls or disables P2P applications, and it scans computers for illegal copies of songs or movies and deletes them. Digital File Check was developed by the International Federation of the Phonographic Industry (IFPI) in conjunction with the Motion Picture Association of America (MPAA) and is available free from the IFPI Web site. A statement from the IFPI noted that the tool does not report evidence of file sharing to any antipiracy organization. Rather, it is designed as an aid to parents and employers who want to discourage children and employees from using computers to violate copyrights. The IFPI will also publish a guide called "Copyright and Security Guide for Companies and Governments" that offers advice to employers about the risks they face by failing to prevent copyright violations on their networks. ZDNet, 23 September 2005

Category 19.2 *Music piracy*

2005-09-23 **Congress anti-piracy file sharing report peer-to-peer P2P campus higher education efforts**

EDUPAGE; http://chronicle.com/daily/2005/09/2005092301t.htm

CONGRESSMEN TO ASK FOR REVIEW OF HIGHER ED ANTIPIRACY EFFORTS

At a U.S. House of Representatives subcommittee meeting this week, lawmakers, campus officials, and representatives of the movie industry and of a provider of legal download services discussed efforts by U.S. Colleges and universities to curtail copyright violations on their networks. Reps. Lamar Smith (R-Tex.) and Howard Berman (D-Calif.) said they will ask the Government Accountability Office to issue a formal report on what effects those efforts have had on student file-trading habits. According to Smith, "We will ask for the report so we can increase the scrutiny and increase the public attention to piracy." Also at the hearing, Norbert Dunkel, director of housing at the University of Florida, described his institution's use of an application called Icarus, which automatically restricts usage of the network for students who connect to P2P services. Dunkel said the tool, which the university developed, has led to a 95 percent reduction in outgoing traffic from the university's network and virtually eliminated notices of copyright infringement. Smith applauded the application, but Daniel Updegrove, vice president for information technology at the University of Texas at Austin, expressed concerns that such a blanket approach to the problem could limit the academic freedom and privacy of students. Chronicle of Higher Education, 23 September 2005 (sub. req'd)

Category 19.2 *Music piracy*

2005-11-14 **I2Hub peer-to-peer P2P networking Internet2 shut down copyright infringement intellectual property rights violation**

EDUPAGE; http://news.com.com/2100-1027_3-5952060.html

I2HUB SHUTS DOWN

I2Hub, the P2P service that ran on Internet2's very high-speed network, has ceased operation amid growing concerns over the liability of such services for copyright infringements by their users. I2Hub was launched in early 2004 on the academic and research network that connects more than 200 locations. Although the service made forays into legal activities, it was largely used by students at connected campuses to trade music and movies at speeds substantially higher than possible with commercial Internet services. A number of i2Hub users had been targeted by the entertainment industry for copyright infringement, however, and the service itself was cited by the Recording Industry Association of America in September as a possible target of legal action. The closure of i2Hub follows that of Grokster last week and an announcement by eDonkey, the most popular P2P service, that it would change its business model to a paid download service. CNET, 14 November 2005

Category 19.2 *Music piracy*

2005-11-15 **music piracy intellectual property rights violation copyright infringement international lawsuits IFPI**

EDUPAGE; http://news.bbc.co.uk/2/hi/entertainment/4438324.stm

IFPI RATCHETS UP LAWSUITS

The International Federation of the Phonographic Industry (IFPI) has filed lawsuits against 2,100 individuals in a number of countries for allegedly sharing copyrighted material over the Internet. The new round of lawsuits, which targets users in the United Kingdom, France, Germany, Italy, Switzerland, Sweden, Argentina, Singapore, and Hong Kong, brings the IFPI's total to more than 3,800. In the United States, nearly 16,000 individuals have been sued for illegal file trading, resulting in more than 3,500 settlements so far. The sharp upswing in the number of lawsuits from the IFPI comes after strong victories for copyright holders in the United States, Australia, and South Korea against operators of P2P services, which in those countries can be held liable for copyright infringement by their users. IFPI Chief John Kennedy said the new suits represent "a significant escalation of our enforcement actions" and noted that through such lawsuits, thousands of individuals "have learnt to their cost the legal and financial risks involved in file-sharing copyrighted music." BBC, 15 November 2005

Category 19.2 *Music piracy*

2005-11-28 **intellectual property rights violation copyright infringement peer-to-peer P2P file music sharing piracy Kazaa Australian Court order keyword filter**

EDUPAGE;
http://www.infoworld.com/article/05/11/28/HNjudgeorderskazaa_1.html

AUSTRALIAN COURT ORDERS KAZAA TO INSTALL KEYWORD FILTER

The Federal Court of Australia in Sydney has ordered the operators of the Kazaa file-sharing service to install a keyword filter to screen out copyrighted material by December 5. The filter will keep users from trading files containing keywords from a list of 3,000 chosen by record companies. The order follows a September ruling that found Kazaa had been used extensively to infringe copyrights. Sharman Networks, the owner of Kazaa, won an extension until February 2006 to comply fully with the court's injunction to block file trading of copyrighted materials. The filtering system is seen as an interim measure, with Sharman expected to appeal I n early 2006. InfoWorld, 28 November 2005

Category 19.2 *Music piracy*

2005-12-09 **peer-to-peer P2P illegal file trading limit bogus junk files shut down sale Loudeye Overpeer**

EDUPAGE; http://news.zdnet.com/2100-9595_22-5989758.html

P2P CLOGGER TO CLOSE

A company that tried to limit illegal file trading by flooding P2P networks with junk files is being shut down and put up for sale. Overpeer, which is owned by Loudeye, contracted with record companies and movie studios to place thousands of bogus versions of songs and movies on P2P services. When users searched for and downloaded those files, they would get garbage or advertisements rather than the desired files. Since late 2002, when Overpeer was at its height, a number of strategies have been developed to allow file traders and the services they use to make reasonably good guesses about files and to filter out the bogus ones. Officials from Loudeye said revenues had fallen significantly and that the division would cease operations immediately. Loudeye will attempt to sell Overpeer's assets. ZDNet, 9 December 2005

Category 19.2 *Music piracy*

2006-01-08 **legal music download increase after Christmas 2005 piracy anti-piracy intellectual property right theft**

EDUPAGE; http://news.com.com/2100-1027_3-6023769.html 23

LEGAL DOWNLOADS SURGE AFTER CHRISTMAS

Sales of music tracks online surged over the holidays, indicating what might be new baseline levels for the market. During the Christmas week, 9.5 million tracks were downloaded from legal online music services, a new record for single-week sales. The following week, that number jumped to nearly 20 million tracks, triple the number sold during the same week a year earlier. Analysts attribute much of the gain to the ballooning number of portable MP3 players in the hands of consumers and to strong sales of gift cards. For the year, legal downloads rose 147 percent to 142.6 million. Although a drop always follows the holiday spike, analysts said the holiday numbers could indicate a market that will grow to perhaps 750 million or 1 billion tracks in 2006. Such numbers still pale compared to downloads on P2P services, which are estimated at 250 million per week, but experts say the upswing in legal downloads signals a changing tide for online music.

Category 19.2 Music piracy

2006-01-19 **students blame software tool peer-to-peer I2HUB RIAA lawsuit settlement EFF**

EDUPAGE; http://chronicle.com/daily/2006/01/2006011901t.htm 23

STUDENTS BLAME I2HUB FOR THEIR DOWNLOADING HABITS

A group of students at the University of Massachusetts at Amherst are demanding that the operators of the now-shuttered i2hub pay for their settlements with the Recording Industry Association of America (RIAA). According to Lisa Kent, an attorney at the university's Student Legal Services Office, which is representing the 42 students, i2hub deceived students into believing the service was endorsed by the university. This deception led to their believing that downloading materials over the network was legal. Unless i2hub pays the $157,500 that the RIAA is seeking from the students, the student legal office will file a lawsuit, said Kent. Charles S. Baker, the attorney for Wayne Chang, who created i2hub when he was a sophomore at UMass Amherst, rejected Kent's argument, saying that the software that Chang wrote was technically legal. "i2hub," he said, "is not responsible if your clients used the software for an improper purpose." Fred von Lohmann, a lawyer for the Electronic Frontier Foundation, compared the students' legal argument to "a shooter deciding to sue a gun company, saying, 'The gun made me do it.'"

19.3 Movies / TV piracy

Category 19.3 *Movies / TV piracy*

2000-01-26 **DVD encryption cracking cryptanalysis copyright prosecution teenager**

NewsScan, New York Times
http://www.nytimes.com/library/tech/00/01/biztech/articles/26disc.html, AP

Jon Johanson, a 16-year-old Norwegian boy, and his father Per Johanson were charged with violating copyright after they created and distributed a cracking program to decode DVDs (digital versatile disks) so they could be copied illegally and played on computers. The family computers were seized by police pending trial.

Category 19.3 *Movies / TV piracy*

2000-07-21 **cryptanalysis cracking DVD scrambling hackers free speech litigation lawsuit**

http://www.nytimes.com/library/tech/00/07/cyber/cyberlaw/21law.html

The ongoing legal battle between the owners of movies on DVDs and criminal hackers who distributed the DeCSS program that allows unauthorized computer access to the copy-protected materials had a visitor from Norway in late July: Jon Johansen, the 16-year-old who wrote DeCSS with two other hackers in 1999. Mr Johansen's testimony was dismissed as irrelevant by the attorneys for the plaintiffs, but the judge wearily allowed the youngster to speak. "The man is here from Norway. I may as well hear it," he said. Mr Johansen's father Per said that his son was carrying on a proud tradition as a freedom fighter. [Helping people make illegal copies of movies is equivalent to fighting the Nazis??]

Category 19.3 *Movies / TV piracy*

2000-10-03 **unexpected consequences movie copyright violation theft volume downloads astronomical invoices**

RISKS, The Register.com http://www.theregister.co.uk/content/1/13668.html 21 08

An enthusiastic computer-game fan placed illegal copies of a fancy advertisement on his Web site — one version at 45 Mb and the other at 32Mb. In July, at least 1400 people downloaded one or other of the files for a total of 62Gb of traffic; in August, downloads totaled even more (the exact number is in doubt). Since "Cannibal Harry" had a contractual limit of 500 Mb per month of data transfers included in his Web page service, his ISP slapped him with an invoice for $6,000 for the month of July and a $24,000 invoice for August.

Category 19.3 *Movies / TV piracy*

2001-04-16 **music video DVD movies film copyright intellectual property new technology volume distribution**

NewsScan

DIGITAL FOUNTAIN GUSHES CONTENT
Digital Fountain has developed new technology that packages streaming video and audio in a different way for Internet transmission, making its server hardware as much as 30 times more efficient than existing hardware in broadcasting movie and music files. When coupled with multicasting software, a single machine can deliver files on demand to an almost unlimited audience. The technology uses "meta-content" packets that provide mathematical snapshots that represent random chunks of files. Unlike the conventional process, which requires that all of a file's packets be received in the correct order, Digital Fountain's technology enables a server to receive the packets in any order -- missing packets don't slow the process. One Digital Fountain server can pump DVD-quality video simultaneously to 4,000 users, a load that could require up to 30 conventional servers. (Wall Street Journal 16 Apr 2001)
http://interactive.wsj.com/articles/SB987369482760951166.htm (sub req'd)

Category 19.3 *Movies / TV piracy*

2001-11-01 **copyright intellectual property television video lawsuit**

NewsScan

NETWORKS SUE PERSONAL DIGITAL RECORDER MAKER [1 Nov 2001]
Three major television networks -- NBC, ABC and CBS -- are suing SONICblue Inc., maker of ReplayTV personal digital video recorders, saying that new ReplayTV 4000 would violate their copyrights by allowing users to distribute programs over the Internet. In a joint statement, the broadcasters said the device "violates the rights of copyright owners in unprecedented ways" and "deprives the copyright owners of the means by which they are paid for their creative content and thus reduces the incentive to create programming and make it available to the public." The company, which has not yet released the ReplayTV 4000, said the device limits to 15 the number of times a user can send any particular show to another ReplayTV 4000 owner, or so-called "TV buddy." The product also supports a digital rights copy protection technology that broadcasters could use to restrict consumers from sending shows over the Internet. Analysts say the lawsuit marks the networks' preemptive strike against a technology that is expected to flourish over the next few years and that could spark the same controversial issues as Napster's music-sharing technology. (AP 1 Nov 2001)
http://news.excite.com/news/ap/011101/00/tech-networks-replaytv

---

Category 19.3 *Movies / TV piracy*

2002-02-06 **video online distribution copyright alternative**

NewsScan

VIVENDI PLANS ONLINE VIDEO SERVICE
Vivendi Universal is launching MP4.com -- a Web site that features a collection of short videos, including animated flicks, feature film-related content, movie trailers and games -- in a few weeks. MP4.com piggybacks on the concept of MP3.com, a music-aggregation site that Vivendi acquired last May. The move into online video follows Sony's debut last September of Screenblast, a site that offers would-be film and animation makers the publishing tools to create video, animation and music. The target user group is 18- to 24-year-olds, an age cohort most likely to have access to broadband connections in dorms or on college campuses. "The concept of MP4 is good if Vivendi can afford the bandwidth and the streaming costs that could attract a big audience," says a digital media researcher at Raymond James Financial. In recent years, a number of similar endeavors have failed to find a viable business model, with Pop.com, AOL Time Warner's Entertaindom, Digital Entertainment Network, Pseudo Programs, CMGI's iCast, and Icebox all falling victim to the dot-com debacle. (CNet News.com 6 Feb 2002)
http://news.com.com/2100-1023-831091.html

Category 19.3 *Movies / TV piracy*

2002-02-20 **video online distribution copyright alternative**

NewsScan

MGM AND CINEMANOW PLAN VIDEO-ON-DEMAND OVER THE NET
MGM is teaming up with CinemaNow of Marina del Rey, Calif., to become the first major Hollywood studio to offer video-on-demand via the Internet. The companies will offer both downloadable and "streamed" versions of "What's the Worst That Could Happen?" and "The Man in the Iron Mask" to any consumer with a high-speed Internet connection and a Windows-based computer. "Our intention in the next two years is to find out as much as we can about how consumers want VOD delivered, what they think about it, [and] how much they want to pay," says MGM Home Entertainment marketing VP Blake Thomas. MGM had previously joined with four other Hollywood studios in the "Movielink" joint venture, but that effort and its rival, Movies.com, have become bogged down in an antitrust probe by the Justice Department. The MGM movies will be available at two streaming speeds: 300 kbps, which is described as a near-VHS-quality picture, and 700 kbps, which is between VHS and DVD quality. Prices will range from $2.99 to $5.99, depending on location and Internet connection. (Los Angeles Times 20 Feb 2002)
http://www.latimes.com/technology/la-000012921feb20.story?coll=la%2Dheadlines%2Dtechnology

---

Category 19.3 *Movies / TV piracy*

2002-05-18 **DVD copyright intellectual property backup copies piracy movies**

NewsScan

'WE FEEL IT'S LEGAL': NEW DVD BACKUP SYSTEM
The software developer 321 Studios, based in St. Louis, Mo., plans to start using its Web site to sell downloadable copies of its software for making backup copies of DVD movies. The Motion Picture Association of America (whose chairman Jack Valenti has called DVD recorders "the newest incarnation of movie piracy") will probably file a lawsuit against 321, but the company's president says: "Our position is that our product is for the purpose of making backup copies of the movies you already own. We feel it's legal." (USA Today 29 Oct 2002)

DVD-COPYING SOFTWARE MAY BE JUDGED TO BE ILLEGAL
Federal District Judge Susan Ilston has hinted that she may ban certain software products made by 321 Studios that allow consumers to copy movies onto DVDs. The 321 software makes it possible to evade the electronic locks designed to deter consumers from copying a movie onto another DVD or a CD, thereby violating the anti-piracy protections included in the Digital Millennium Copyright Act (the constitutionality of which has been under attack). In her ruling, the judge referred to two recent rulings against the distribution of other programs that circumvent electronic locks: the DeCSS software for copying DVDs and ElcomSoft Co.'s program to decrypt certain electronic books. However, 321 Studios is arguing that those products are different from its own because its has the legitimate purpose of helping consumers make backups of the discs they own. However, an attorney for the movie studios says manufacturers of DVD players are authorized to unlock discs, but 321 Studios is not. (Holland Sentinel 18 May 2003)

Category 19.3 *Movies / TV piracy*

2002-09-09 **online video movies distribution e-commerce intellectual property piracy**

NewsScan

VIDEO-ON-DEMAND GETS A BOOST
Two major deals announced today signal the first steps toward building a marketplace for online films: Movielink, the digital-film venture backed by five major Hollywood studios, has struck an agreement with IBM to provide the servers that will host its movies, and CinemaNow, a rival VOD majority owned by Lions Gate Entertainment, signed its first major-studio licensing deal with Warner Bros., allowing it to offer "dozens" of its titles, including the blockbuster "Harry Potter and the Sorcerer's Stone." CinemaNow, which is already operational, says it's negotiating with other studios to secure film licenses, and Movielink CEO Jim Ramo says his venture is "moving forward with all the necessary ingredients for launch in a timely manner." (Wall Street Journal 9 Sep 2002)

Category 19.3 *Movies / TV piracy*

2002-12-11 **DVD movie counterfeits piracy copyright infringement intellectual property lawsuits**

NewsScan

HOLLYWOOD AND THE PIRATES
The Motion Picture Association of America (MPAA) has filed copyright-infringement lawsuits against individuals in eight states it accuses of using the Internet to sell bootlegged DVD copies of movies. The MPAA detected the piracy by purchasing some of the DVDs and then examining the contents. (AP/USA Today 11 Dec 2002)

Category 19.3 *Movies / TV piracy*

2003-10-09 **digital piracy Disney scare entertainment privacy**

NewsScan

DISNEY WANTS TO 'SCARE THE HECK OUT OF' DIGITAL PIRATES
Disney executives think that Hollywood need to find digital locks on entertainment content to bar people who don't pay. Chief Operating Officer Bob Iger says: "I realize that there are a lot of concerns regarding privacy in this regard, invading people's homes and their home PCs, but at some point we've got to somehow ... scare the heck out of these people that they could get caught." (USA Today 9 Oct 2003)

Category 19.3 *Movies / TV piracy*

2003-10-24 **movie piracy prevent Oscars screeners VHS coded**

NewsScan

SCREENERS CODED TO PREVENT MOVIE PIRACY
A compromise has been reached that will make possible a carefully controlled distribution of free cassettes to Oscar voters for private screening during the upcoming awards season. The movies will be numbered VHS cassettes rather than easily copied DVDs, and they will be coded for tracing if they are sold or pirated. Academy members will sign contracts taking responsibility for any "screeners" they accept, and making them subject to possible banishment from the Academy if the screeners are later found on the black market. (Washington Post 24 Oct 2003)

Category 19.3 *Movies / TV piracy*

2003-10-29 **MPAA digital piracy Dick Valenti copyright infringement**

NewsScan

VALENTI ON DIGITAL PIRACY
Dick Valenti, president of the Motion Picture Association of America, sees the fight against digital piracy as vital to America's economic future: "Piracy is a fact plain and real, with the unwanted prospect of its rapid spread in the future. Antipiracy must take precedence over everything. Current conservative estimates indicate that the film industry loses $3.5 billion each year to hard-goods piracy (counterfeit DVDs, VHS tapes and optical discs). That figure does not take into account the damage done by online piracy. The digital world with its zeroes and ones and perfect copies of originals has changed the movie landscape forever, which is why the movie world's priorities have been permanently altered. The industry wants to use the Internet to dispatch films to consumers. But as we do, we must also challenge piracy and defeat it with every weapon we can summon — and we will succeed, I am convinced — or one day we will sit upon the ground and tell sad stories of the decline and fall of America's greatest artistic triumph and an awesome engine of job and economic growth." (Wall Street Journal 29 Oct 2003)

Category 19.3 *Movies / TV piracy*

2003-12-23 **DVD copying anti-copying Jon Johansen MPAA Motion Picture Association of America film television industry**

NewsScan

OSLO COURT EXONERATES 'DVD JON'
An Oslo appeals court has upheld a lower court ruling clearing 20-year-old Jon Johansen (dubbed "DVD Jon" by fans) of piracy charges, saying he had broken no Norwegian law by developing and distributing software that disables digital locks that prevent unauthorized copying of DVDs. The court noted that such software prevents DVD owners from making personal copies that could be used as backup if the original sustains damage. The ruling applies only in Norway, but the case has been closely watched by advocates on both sides who see it as a test for cyberspace copyright rules around the globe. The U.S. Motion Picture Association of America expressed its disappointment in the verdict in a statement: "The actions of serial hackers such as Mr. Johansen are damaging to honest consumers everywhere. While the ruling does not affect the laws outside of Norway, we believe this decision encourages circumvention of copyright that threatens consumer choice and employment in the film and television industries." (Reuters/Los Angeles Times 23 Dec 2003)

Category 19.3 *Movies / TV piracy*

2004-02-19 **intellectual property rights copyrights FBI warning CDs DVDs**

NewsScan

FBI WARNING LABELS TO APPEAR ON CDs, DVDs

The Federal Bureau of Investigation is giving Hollywood film studios, music companies and software makers permission to use the FBI's name and logo on various digital media to deter consumers from making illegal copies. FBI official Jana Monroe says, "This anti-piracy seal should serve as a warning to those who contemplate the theft of intellectual property, that the FBI will actively investigate cyber crimes and will bring the perpetrators of these criminal acts to justice." Unauthorized copying and distribution of digital content is punishable by up to five years in prison and a fine of $250,000. (Los Angeles Times 19 Feb 2004)

Category 19.3 *Movies / TV piracy*

2004-07-12 **Internet usage South Korea movie piracy illegal download films high-speed access**

NewsScan

S.KOREA: 3 OF 5 INTERNET USERS ILLEGALLY DOWNLOAD FILMS

About one-fourth of Internet users in an eight-country survey admit to illegally downloading movies but the percentage is more that twice as high in South Korea. According to a survey by the Motion Picture Association of America (MPAA), an average of 24% of Web users in the eight countries have downloaded at least one movie, and in South Korea (a country with the highest percentage of Internet users on high-speed connections) the number was 58%. Since downloading a movie over high-speed connections takes just a few minutes, the MPAA fears that piracy will grow as more Internet users boost their speed. (The Age 12 Jul 2004) Rec'd from John Lamp.

Category 19.3 *Movies / TV piracy*

2004-08-04 **DVD piracy copying copyright infringement intellectual property rights lawsuit company shutdown**

NewsScan

DVD-COPYING COMPANY SIGNS OFF

321 Studios, which has been embroiled in lawsuits brought by deep-pocketed movie studios and video game producers, has quietly given up the ghost. In a posting on the 321 Web site it announced "it has ceased business operations including, but not limited to, the sale, support and promotion of our products." Tuesday's announcement came on the heels of another legal setback when a New York federal judge imposed a worldwide ban on the production and distribution of 321's Games X Copy software in response to a lawsuit by three leading makers of video games. 321 has steadfastly maintained that its copy software was merely intended for consumers who prefer to make backups of expensive DVDs and video games in case of damage to the originals. (AP/Washington Post 4 Aug 2004)

Category 19.3 *Movies / TV piracy*

2004-08-10 **DVD software company MPAA copyright infringement intellectual property rights financial settlement lawsuit**

NewsScan

DVD SOFTWARE COMPANY YIELDS TO MPAA

Software company 321 Studios in St. Louis will stop selling DVD copying software worldwide and has agreed to a financial settlement with the Motion Picture Association of America (MPAA). MPAA chief executive Jack Valenti says: "321 Studios built its business on the flawed premise that it could
profit from violating the motion picture studios' copyrights; the courts have been amply clear -- there is no leniency for violating federal copyright laws. Now that the company's illegal copying software is off of store shelves worldwide, we have moved to settle the case." In addition, Valenti warned: "This is not the end of the story in our massive fight against piracy." (AP/San Jose Mercury News 10 Aug 2004)

Category 19.3 *Movies / TV piracy*

2004-10-05 **fraud piracy music movies anti-counterfeiting initiative Homeland Security US government**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/articles/A7331−
2004Oct4 .html

October 05, Washington Post — Anti-counterfeiting initiative launched.

On Monday, October 4, four U.S. agencies announced a coordinated attack to stem the global trade in counterfeit merchandise and pirated music and movies, an underground industry that law-enforcement officials estimate to be worth $500 billion each year. The effort, known as the Strategy Targeting Organized Piracy (STOP), includes stepping-up border enforcement to intercept fake goods as they are entering the United States, targeting the earnings of traders of counterfeit goods and publicizing the names of overseas companies that traffic in counterfeit products. Joining the campaign are U.S. Trade Representative Robert B. Zoellick, the Justice Department, the Commerce Department and the Department of Homeland Security, which includes the customs and border-protection bureau.

Category 19.3 Movies / TV piracy

2004-10-12 **US federal task force piracy crackdown intellectual property rights protection**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/articles/A27583−2004Oct 12.html

October 12, Associated Press — U.S. authorities call for piracy crackdown.

A federal task force has recommended expanded investigative and prosecutorial powers to combat intellectual property theft ranging from counterfeit drugs to swapping songs over the Internet. Wiretaps should be allowed to investigate intellectual property theft that threatens health and safety and more investigators should be added in key U.S. cities and in piracy hot spots in Asia and Eastern Europe, the report released Tuesday, October 12 said. The report also endorsed the rights of companies to compel Internet service providers to turn over the names of people who have traded songs, movies, software or other copyright-protected items over the Internet. Piracy costs American companies $250 billion per year, the report estimated. Report: http://www.usdoj.gov/criminal/cybercrime/IPTaskForceReport.p df

---

Category 19.3 Movies / TV piracy

2004-11-04 **movie piracy Hollywood MPAA video lawsuits litigation education criminal prosecution copyright infringement**

NewsScan; http://www.latimes.com/technology/la-fi-mpaa4nov04

HOLLYWOOD LAUNCHES ANTI-PIRACY CAMPAIGN

Taking its lead from major record companies, Hollywood studios have prepared a host of lawsuits against people who illegally use copyrighted movies obtained via filesharing networks. Dan Glickman, president of the Motion Picture Association of America (MPAA), says that what's needed to combat piracy is "a holistic approach" -- including educational efforts, criminal prosecution, and lawsuits against infringers. "You need the stick and you need the carrot both. You can't just have one without the other." But film producer Ross Grayson Bell says that the industry's focus should be on providing legal ways to buy movies on the Internet -- and that Apple iTunes Music Store is the right model because it lets people download songs quickly and at a reasonable price: "There is a need that is not being met. I think the real way to curb piracy is to take away that need. The industry has to present a viable way to see movies in this new age." (Los Angeles Times 4 Nov 2004)

Category 19.3 Movies / TV piracy

2004-11-05 **Hollywood movie piracy MPAA RIAA lawsuits videos copyright infringement**

NewsScan; http://online.wsj.com/article/0

HOLLYWOOD THREATENS LAWSUITS AGAINST ONLINE PIRATES

The Motion Picture Association of America says its members are poised to file copyright-infringement lawsuits against digital movie downloaders, following the lead of the music industry, which has filed thousands of such lawsuits over the past year. But while the music industry has demonstrated decidedly mixed results, the movie industry may be more successful, in part because the campaign is getting underway while movie downloading is still relatively rare, representing only 2% of all online file sharing. "The studios have a little bit of a head start. By taking action now, [they] have a better chance in making a real dent in the problem," says one copyright attorney. One reason for the small number of film downloads is the size of the files -- users could download hundreds of songs in the same time it takes to download one movie. In addition, movie fans are not as disaffected with that industry, unlike music enthusiasts who resent paying $15 for a CD with only one or two songs that they really want. "The deal between you and Hollywood is pretty good. The deal between you and the music industry has been pretty lousy for a long time," notes Eric Garland, CEO of BigChampagne. (Wall Street Journal 5 Nov 2004)

Category 19.3 Movies / TV piracy

2004-11-17 **Hollywood MPAA movie piracy lawsuits Internet copyright infringement**

NewsScan; http://news.bbc.co.uk/1/hi/entertainment/film/4018755.stm

HOLLYWOOD SUES INTERNET FILM PIRATES

The Motion Picture Association of America has filed an undisclosed number of lawsuits against Internet users it suspects of swapping or downloading digital copies of films. The group says the civil suits could seek damages of up to $30,000 per film. The MPAA move follows a similar strategy by the music industry to crack down on illegal downloading, which resulted in about 5,000 lawsuits. MPAA Dan Glickman said in a statement: "The motion-picture industry must pursue legal proceedings against people who are stealing our movies on the Internet. The future of our industry, and of the hundreds of thousands of jobs it supports, must be protected from this kind of outright theft using all available means." (BBC News 17 Nov 2004)

Category 19.3 *Movies / TV piracy*

2004-12-15 **MPAA Hollywood BitTorrent pirates copyright infrincgement lawsuits**

NewsScan; http://www.usatoday.com/tech/news/2004-12-15-bittorrent-suits_x.htm

HOLLYWOOD SUES "PARASITE" BITTORRENT USERS

Hollywood movie studios have filed copyright infringement lawsuits against the operators of computer servers that BitTorrent software to relay digital movie files across online file-sharing networks. John Malcolm of the Motion Picture Association of America (MPAA) says: "Today's actions are aimed at individuals who deliberately set up and operate computer servers and Web sites that, by design, allow people to infringe copyrighted motion pictures. These people are parasites, leeching off the creativity of others. Their illegal conduct is brazen and blatant." However, Fred von Lohmann, an attorney with the Electronic Frontier Foundation, warns: "By bringing these suits, the MPAA runs the risk of pushing the tens of millions of file sharers to more decentralized technologies that will be harder to police." (AP/USA Today 15 Dec 2004)

Category 19.3 *Movies / TV piracy*

2005-01-03 **TiVo copy protection mobile viewing entertainment intellectual property copyrights legal fees video**

NewsScan; http://news.com.com/TiVo+goes+mobile+with+new+free+service/2100-1041_3-5510240.html

TIVO GOES MOBILE

TiVo has introduced a mobile option for its subscribers called TiVoToGo. The service, which requires the installation of free TiVo Desktop software on the target computer, enables users to transfer programs to their laptops, as long as copyright protections are in place. "Consumers don't want to be tied to their living room to watch their favorite entertainment," says TiVo chief marketing officer Matt Wisk. "With TiVoToGo, subscribers can take their favorite shows with them to enjoy on business trips or family vacations." The TiVo Desktop software is designed for the Windows XP and 2000 operating systems, and avoids content that uses Macrovision copy protection technology, including pay-per-view and video-on-demand programming and commercial DVDs. (CNet News.com 3 Jan 2005)

Category 19.3 *Movies / TV piracy*

2005-01-04 **piracy movie BitTorrent eDonkey source monitoring surveillance movies intellectual property copyright infringement file-sharing**

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/10561389.htm

THE CONTINUING FIGHT AGAINST ONLINE PIRATES

A company called BayTSP of Los Gatos, California, has developed a monitoring system to identify the sources of bootleg copies of movies transmitted over file-sharing networks such as eDonkey and BitTorrent. BayTSP chief executive Mark Ishikawa explains, "Pirated copies of movies and software typically appear online within hours of release. Identifying and taking action against the first uploaders can greatly slow the distribution of illegally obtained intellectual property and might make users think twice before doing it." Ishikawa says the technology not only identifies the hard-core pirates who contribute to massive online piracy, but is also able to quantify the number of illegal copies made from the original bootleg (information necessary when a copyrightinfringement lawsuit is subsequently filed).(San Jose Mercury News 4 Jan 2005)

Category 19.3 *Movies / TV piracy*

2005-02-11 **movie industry anti-piracy campaign MPAA prosecute illegally files lawsuits copyright LokiTorrent BitTorrent**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4256449.stm

MOVIE INDUSTRY CONTINUES ANTIPIRACY CAMPAIGN

The Motion Picture Association of America (MPAA) continues its legal efforts to prevent movie piracy and prosecute those who engage in illegally sharing movie files. The trade group filed another undisclosed number of lawsuits against individuals for alleged copyright violations, and it succeeded in closing down LokiTorrent, one of a number of sites that use the BitTorrent application to help file traders find desired files on the Web. Although sites that use BitTorrent do not host files--instead providing "trackers" that locate requested files--a court in Dallas said the movie industry could access LokiTorrent's server records to identify individuals who traded copyrighted movie files. The permanent closure of LokiTorrent follows similar closings of Supernova.org and Phoenix Torrent in the past two months.

Category 19.3 *Movies / TV piracy*

2005-02-18 **UK Australia TV television piracy copyright infringement**

NewsScan; http://australianit.news.com.au/articles/0

U.K., AUSTRALIA TOP TV PIRACY LIST

Australia and Britain have been revealed as the world's biggest markets for pirate TV downloads. The trend is being driven by tech-savvy fans who are unwilling to wait for popular U.S. shows such as 24 and Desperate Housewives. Australia ranked as second largest downloader of TV programs after Britain in a study of the phenomenon by U.K. technology consultancy Envisional. The U.S. was in third position. (The Australian 18 Feb 2005)

Category 19.3 *Movies / TV piracy*

2005-08-05 **movie piracy camcorder law charges filed MPAA peer-to-peer P2P file sharing**

EDUPAGE; http://news.com.com/2100-1030_3-5819976.html

FIRST CHARGES FILED UNDER CAMCORDER LAW

A 19-year-old man from Missouri has become the first person charged under a recently enacted federal law banning the use of camcorders to tape movies in theaters and then make them available online. According to the Motion Picture Association of America, such camcorder piracy accounts for more than 90 percent of movies that are available online prior to their release outside theaters. Curtis Salisbury is charged with taping two movies in theaters and placing them on so-called warez networks, where many pirated movies and songs find their way onto the Internet. From there, pirated content typically ends up on P2P networks. Unlike the majority of people who upload copyrighted content to such networks, Salisbury tried to profit financially from the movies he posted. He is charged with conspiracy, copyright infringement, and two violations of the law banning camcorders in theaters. He faces up to 17 years in prison. Reuters, 5 August 2005

19.4 Books / e-books piracy

Category 19.4 *Books / e-books piracy*

2000-07-20 **intellectual property IP copyright infringement piracy lawsuits auctions Web sales**

NewsScan

Sega . . . shut down more than 60 illegal Web sites and 125 auction sites selling pirated versions of its Dreamcast games, which until recently had been viewed as a "Fort Knox of online intellectual properties" — protected by far more sophisticated technology than the relatively simple music, film and video files targeted by services like Napster and Scour. Despite the security precautions, several dozen Dreamcast titles were released this month on the Internet and have been traded via networks like Internet Relay Chat (IRC). Charles Bellfield, Sega's director of communications, says his company's actions mark one of the first times that the Digital Millennium Copyright Act of 1998 has been invoked to go after the Web-hosting companies and ISPs used by pirate traders. "It is the first time that this act has been used not just to stop piracy, but also physical sales over the Internet. It is the first time that Web-hosting companies and Web auction sites are being held accountable for the contents of what is being sold." (Reuters 20 July 2000)

Category 19.4 *Books / e-books piracy*

2001-08-21 **copyright intellectual property library distribution**

NewsScan

LIBRARY PACT SIGNALS NEW CHAPTER IN E-BOOK LENDING
California State University system is working with NetLibrary to provide simultaneous access to electronic books for multiple borrowers -- a significant change in how subscription models generally work. Previously, a single copy of an e-book could be borrowed by only one reader at a time -- just like a print version. Under the new rules, half of the 1,500 e-books owned by Cal State will be available to multiple readers at the same time, at no extra cost. Libraries need to exert more influence in the ongoing debate over the fledgling e-book industry, says Evan Reader, of the CSU Chancellor's office. "They accept what's put on the plate. We don't want to do that." The Cal State system has 23 campuses and 370,000 students. "I suspect (NetLibrary) went along with it because of our size," says Reader. (Wired.com 21 Aug 2001)
http://www.wired.com/news/culture/0,1284,46160,00.html

Category 19.4 *Books / e-books piracy*

2001-08-23 **e-book piracy facsimile scanner peer-to-peer distribution copyright intellectual property**

NewsScan

DIGITAL PIRACY SPREADS FROM MUSIC TO BOOKS
Book publishers are beginning to see the same kind of piracy tactics recently experienced by the recording industry, and Internet monitoring firm Envisional predicts that the illegal downloading of books could become as big a problem as Napster. Envisional found nearly 7,300 copyrighted titles available for free through file-sharing networks such as Gnutella, including more than 700 individual copies of J.K. Rowling's Harry Potter books. In most cases, the book has been scanned and converted into downloadable text, but in a few instances hackers had cracked the copyright protection codes to e-books and made them available. Envisional says the files it found are simply the tip of the iceberg. "It's a relatively conservative estimate of the number of illegal books out there," says an Envisional executive. (Financial Times 23 Aug 2001)
http://news.ft.com/news/industries/internet&e-commerce

Category 19.4 *Books / e-books piracy*

2006-04-20 **publisher copyright lawsuits settlement intellectual property rights issues textbooks**

EDUPAGE; http://chronicle.com/daily/2006/04/2006042001t.htm 23

PUBLISHERS SETTLE COPYRIGHT LAWSUITS, MORE PENDING

Two academic publishers have settled six of 20 lawsuits filed against individuals for selling copies of instructors' manuals online. The manuals accompany specific textbooks but are intended for faculty only because they include answers to homework and quiz questions in the texts. The individuals involved in the settlements were accused of making copies of instructors' manuals and selling them online, according to William Dunnegan, an attorney representing Pearson Education and John Wiley & Sons. Terms of the settlement were not released, nor were the names of the defendants. Other cases are still pending, and the publishers involved said the lawsuits are just one part of a larger campaign to address the problem of illegal online sales of copyrighted academic texts. Dunnegan said he hopes other academic publishers will join Pearson and Wiley, saying, "It will be easier to enforce as part of a group effort."

19.5 Games piracy

Category 19.5 *Games piracy*

2000-01-29 **credit card fraud theft counterfeit shoulder surfing confidentiality**

RISKS 20 77

The Japanese department store, Takashimaya, was victimized by counterfeiters who passed so many forged store credit cards that the chain issued 300,000 new credit cards to customers to reduce the thefts. There was some evidence that criminals systematically engaged in shoulder surfing to collect card numbers.

Category 19.5 *Games piracy*

2000-03-14 **cryptanalysis cracking smart card forgery**

The Guardian (London)
http://www.guardianunlimited.co.uk/international/story/0,3604,230435,00.html

After Serge Humpich was punished by the French courts for demonstrating that he could fool smart-card terminals into giving him Paris subway tickets, criminal hackers released an algorithm on the Internet which they claimed would allow anyone to forge bank cards. However, Roland Moreno, a cryptographer who worked on the smart-card algorithms that slashed French bank-card fraud by 90%, described the claims as fraudulent and offered a 1M FF reward (~U$150,000) to anyone demonstrating that the supposed formula actually worked.

Category 19.5 *Games piracy*

2003-10-07 **gaming piracy steal popular Half-Life code online**

NewsScan

VANDALS STEAL SOURCE CODE OF POPULAR COMPUTER GAME
Network vandals have stolen the source code of the new computer game "Half-Life 2" and are circulating it on the Internet. The company that owns the game spent five years developing it, a fact that prompted Dave Kosak, executive editor of GameSpy.com, an online gaming service provider, to see the silver lining in this criminal act, which is that it "points out that game developers have really valuable property. They spend years coding this engine, and the bigger you are, the bigger target you are." (AP/San Jose Mercury News 7 Oct 2003)

Category 19.5 *Games piracy*

2004-06-11 **Valve Half-Life 2 game code theft arrest piracy hackers customer credit**

NewsScan

ARREST MADE IN VIDEOGAME CODE THEFT

The FBI-led Northwest Cyber Crime Task Force has made arrests in "several countries" as part of its investigation into the theft of Valve Corp.'s Half-Life 2 videogame code last year. The task force declined to give details on the arrests, but Valve chief executive Gabe Newell credited a "core group" of the company's customers for sending and analyzing information that helped lead to the arrests. "Gamers were able to unravel what are traditionally unsolvable problems for law enforcement related to this kind of cyber-crime," says Newell. Following the theft, Valve was forced to rewrite parts of its programming, delaying the game's launch by almost a year from its original release date. Some industry insiders say the delay has caused something of a backlash against hackers. "Gamers really want to play Half Life 2, and they really, really resented the delay," says the founder of a videogame news site called GameSpot. Fan Darrin Schrader agrees: "It hurts the community when people do this. I just hate cheaters, and hackers are cheaters." (Washington Post 11 Jun 2004)

Category 19.5 Games piracy

2004-11-08 **video games piracy P2P peer-to-peer**

NewsScan; http://apnews.excite.com/article/20041108/D867MSU80.html

PIRATES SEE VIDEO GAMES BEFORE PAYING CUSTOMERS DO

Pirated copies of the sci-fi action title "Halo 2" and games such as "Grand Theft Auto: San Andreas" and "Half-Life 2" have been circulating on file-sharing networks, news groups and Web sites even before their official release to consumers. Brian Jarrard of Microsoft's Bungie Studio, which produced "Halo 2," complains: "You spend three years of your life pouring everything you have into this project, and then somebody gets their hands on the game and gives it away to the world for free. We made this, and these guys had no right to give it out to the public." Douglas Lowenstein, president of the Entertainment Software Association, admits: "The problem and challenge with piracy is that there are people out there on a worldwide basis who've identified piracy as a very profitable enterprise. You don't end this problem overnight." (AP 8 Nov 2004)

Category 19.5 Games piracy

2005-06-15 **game system digital rights copy protection vulnerability exploit**

RISKS; http://www.eepi.org/archives/eepi-discuss/msg00100.html 23 90

EXPLOIT OF SONY PSP RAPIDLY DEVELOPED

Lauren Weinstein wrote two excellent postings in the Electronic Entertainment Policy Initiatiave discussion list and pointed to them in a summary for RISKS.

>As we know, often even the most elaborate attempts at controlling access to hardware and software, even using the very latest technologies, may be less than entirely successful.

An example is the just-announced "exploit" of Sony's powerful and popular new "PSP" portable gaming system (which includes WiFi and other advanced capabilities). The unit employs digital signing and hardware AES encryption to try prevent the running of "unofficial" applications.

However, … the PSP exploitation door has apparently been opened quite wide both for piracy and a vast array of homebrew applications….

The powerful new PSP -- based on the MIPS R4000 CPU -- complete with a gorgeous color display and WiFi capability, became an obvious target for homebrew applications, ranging from game emulators to Linux projects. However, the device was designed to refuse the execution of programs that had not been "signed" by Sony, primarily as a control against game piracy, we assume.

However, it was soon discovered that the earliest PSP units, released only in Japan, contained a firmware flaw allowing the running of properly manipulated unsigned code. Immediately, homebrew applications began to appear. By the time the PSP was released in the U.S. Just a few months ago, the early Japanese version 1.0 firmware had been replaced with version 1.5, and the execution hole appeared to be closed. A high premium on the early Japanese units resulted.

The U.S. PSP fans stayed busy by discovering a Web browser included in a popular PSP game for update purposes ("Wipeout Pure"), that could be manipulated to reach arbitrary sites via various DNS tricks. Meanwhile, various hacking groups worked at finding a way to open an unsigned execution path on the 1.5 firmware.<

In his follow-up article, Weinstein reported

>…[T]he exploit for Sony's PSP … was released as "advertised" this morning and has already been tested by many users around the world. Reports indicate that it provides the functionality previously discussed, and it has been confirmed that it will not run on PSP firmware later than the 1.5 version. All but the earliest (firmware 1.0) PSP units in Japan, and all U.S. Units, have so far been shipped at firmware level 1.5. Sony has recently released firmware versions 1.51 and 1.52, which block the exploit, that some users have already flashed to their units via Web downloads.

While the exploit apparently works, it is not by itself a terribly practical long-term procedure, since it involves the rapid swapping of memory sticks during the startup of each unsigned application.

However, the camel's nose is now in the tent, and the exploit, by allowing the execution of arbitrary unsigned code (including the ability to reflash the unit's firmware), will likely lead *very* rapidly to more "user-friendly" and far-reaching exploitations and homebrew applications."<

In a posting in RISKS 23.92, Weinstein continued, >It only took around a week for the exploit to evolve from unwieldy but powerful hack, to user-friendly production program, but the "signed-code" security system of the Sony PSP Portable running 1.5 firmware, designed to prevent the execution of pirated or other "unofficial" (e.g. Homebrew) code, appears to have been obliterated.<

19.6 Counterfeit currency, credit-cards, other negotiable tokens

Category 19.6 *Counterfeit currency, credit-cards, other negotiable tokens*

2000-12-05 **counterfeit government agency corruption insider fraud arrests criminal**

RISKS 21 14

Paul Nowak wrote in RISKS about another contributor to identity theft: counterfeit drivers' licenses and photo IDs: "Thus far, 14 people have been indicted — including four AZ Motor Vehicle Division customer service employees and an Arizona Department of Transportation computer information worker. Several more arrests are expected, with more arrests expected. Four groups are accused of issuing bogus licenses and ID cards, at a cost over $1000 each. `Buyers apparently included criminals, illegal immigrants and motorists with suspended or revoked licenses.' [Source: Article by Senta Scarborough, *The Arizona Republic*, 25 Nov 2000]"

Category 19.6 *Counterfeit currency, credit-cards, other negotiable tokens*

2001-12-27 **RF radio frequency I&A identification authentication Euro bank note currency forgery counterfeit**

RISKS 21 84

Ben Rosengart wrote in RISKS:
>I hardly know where to begin even thinking about the RISKS involved."The European Central Bank is working with technology partners on a hush-hush project to embed radio frequency identification tags into the very fibers of euro bank notes by 2005. Intended to foil counterfeiters, the project is developing as Europe prepares for a massive changeover to the euro, and would create an instant mass market for RFID chips, which have long sought profitable application.<

http://www.eetimes.com/story/OEG20011219S0016

Category 19.6 *Counterfeit currency, credit-cards, other negotiable tokens*

2002-01-10 **credit-card fraud clone counterfeit hack**

RISKS 21 86

David Farber wrote in RISKS:
>Homemade machines costing about $50 are being used to read credit-card mag-stripes, without having to steal the cards. The information is then e-mailed abroad, where cloned cards are fabricated. This has become a billion-dollar-a-year enterprise.<

Category 19.6 *Counterfeit currency, credit-cards, other negotiable tokens*

2003-07-14 **hacking fraud vandalism universities vending machines**

NewsScan

STUDENTS ADMIT TO OVERSTATING THEIR FEATS OF VANDALISM
Two student hackers have finally admitted that they never finished a device that was intended to cheat university campus debit card systems out of food, laundry machine use or sports tickets. In view of the admission, the manufacturer of the vending machine system used on more than 200 colleges nationwide has agreed to drop its lawsuit against the two students, one from Georgia Tech and the other from the University of Alabama. The device was intended to manipulate the amount of money on a debit card used in the system, but a spokesman for Blackboard, the vending machine company, says: "They actually didn't do a lot of the things they were claiming to do. They knew full well the claims they were making were silly. They're obviously bright young guys, but a little misguided in where they were focusing their attention." (AP/Washington Post 14 Jul 2003)

19.7 Counterfeit legal or business documents

Category 19.7 *Counterfeit legal or business documents*

2000-01-19 **plagiarism forgery theft intellectual property attribution detection plagiarism**

Edupage, New York Times
http://www.nytimes.com/library/tech/00/01/circuits/articles/20chea.html

EDUPAGE pointed to a report in the New York Times in January 2000 that provided good information on the problem of academic forgery. A variety of anti-plagiarism sites have popped up on the Web to help academics pounce on students who plagiarize material for their essays, term-papers and theses. Some of the useful services are < http://www.plagiarism.org/ >, < http://www.canexus.com/ >, < http://www.cs.berkeley.edu/~aiken/moss.html >, and < http://www.integriguard.com/ >. The engines variously compare student texts (submitted online, of course) with databases of papers, including other student papers and those available on plagiarism sites. Identical or similar passages are highlighted in a written report for the teacher. The technology should not be used as the sole basis for an accusation of plagiarism. [As a university professor back in 1978, I spotted obvious plagiarism when a dull-witted male student submitted his essay with a cover page that used a different font from that of the rest of the paper. Confronted with my skepticism, he blustered that he had written every word — even though he could not remember the exact title or any of the content of the paper. But the clincher was language: the French-language paper used the _feminine_ form for all reflexive terms. At that point he broke down.]

Category 19.7 *Counterfeit legal or business documents*

2001-03-23 **digital certificates fraud impersonation counterfeit**

NewsScan

MICROSOFT WARNS OF HACKER THREAT
Microsoft says that hackers have gained possession of two digital certificates that would allow them to distribute malicious code masquerading as official Microsoft software. Digital certificates serve as proof that software code was written by a particular company and is safe. Microsoft said the criminals tricked VeriSign into issuing two of the certificates back in January, and the software giant is warning users to be suspicious of any program that arrives with a certificate claiming Microsoft's authority. The firm is working on a downloadable patch to fix the problem, but it won't be ready for about a week. "Anything that says it was issued on the 29th and 30th of January is bogus. Do not trust it," says a Microsoft spokesman. (MSNBC 22 Mar 2001)
http://www.msnbc.com/news/548228.asp

Category 19.7 *Counterfeit legal or business documents*

2002-03-22 **intellectual property rights SLAPP strategic lawsuit against public participation free speech copyright infringement search engine**

NewsScan

GOOGLE PULLS, THEN RESTORES, LINK TO ANTI-SCIENTOLOGY SITE
Caught between the Church of Scientology (which says it was protecting its own copyrighted material) and the Electronic Frontier Foundation (which says it was protecting free speech), the Google search service first removed, then replaced, reference to a site critical of Scientology. The Church of Scientology has accused the site Xenu.net of "wholesale, verbatim copyright infringement" for posting large quantities of copyrighted material; Xenu and the Electronic Frontier Foundation have charged that the Church was using copyright laws to stifle criticism. (Reuters/San Jose Mercury News 21 Mar 2002)
http://www.siliconvalley.com/mld/siliconvalley/2910195.htm

Category 19.7 *Counterfeit legal or business documents*

2002-03-29 **counterfeit confidentiality identity theft forgery fraud**

RISKS 22 02

Someone has been circulating a fraudulent "W-9095" form claiming to be from the US Internatl Revenue Service (IRS). The counterfeit form, entitled, "Application Form For Certificate Status/Ownership For Withholding Tax," asks for all kinds of detailed information perfect for perpetrating identity theft. The fraud was discovered when a potential victim brought it in to a bank for clarification.

Category 19.7 *Counterfeit legal or business documents*

2004-01-10 **anti counterfeit technology Adobe Photoshop**

NewsScan

ADOBE ACKNOWLEDGES ANTI-COUNTERFEITING TECHNOLOGY

Adobe Systems admits that the latest version of its popular Photoshop graphics software includes technology that generates a warning message when someone tries to make a digital copy of some currencies. The technology was added at the request of government regulators and bankers and was designed by the Central Bank Counterfeit Deterrence Group, a consortium of 27 banks in the U.S., Canada, Europe and Japan. "We sort of knew this would come out eventually," says an Adobe spokesman. "We can't really talk about the technology itself." Angry consumers have flooded Adobe's message boards with complaints over censorship and concerns over future restrictions that could include adult-oriented or copyrighted material. "This shocks me," says the president of the Photoshop users group in San Diego. "Artists don't like to be limited in what they can do with their tools. Let the U.S. government or whoever is involved deal with this, but don't take the powers of the government and place them into a commercial software package." (AP/Washington Post 10 Jan 2004)

19.8 Plagiarism & cheating

Category 19.8 *Plagiarism & cheating*

2000-01-15 **counterfeit fake computer equipment mouse mice organized crime**

Los Angeles Times

Police in the Los Angeles area seized 23,000 fake Microsoft computer mice worth around $1M. Investigators were pursuing leads that pointed towards involvement of organized crime. The devices looked authentic (except for one batch with "Certificates [sic] of authenticity"), down to serial numbers, bar codes and boxes with authentic logos.

Category 19.8 *Plagiarism & cheating*

2001-05-08 **penetration identification authentication I&A term paper plagiarism pattern recognition**

RISKS 21 39

Richard Kaszeta, a seasoned systems administrator in a college department, commented on a report about how a University of Virginia professor used a computer to catch 122 plagiarists using the professor's own home-grown program. "The program basically compares papers and looks for phrases shared between papers." However, noted Mr Kaszeta, "The risk is that some of the students are probably innocent, merely being guilty of having their own papers copied without their knowledge. Indeed, some of the students claim towards the end of the article that exactly that has happened. Unfortunately, the technology of online composition and submission of papers (as typically done at most Universities) lacks sufficient security, encryption, and authentication standards."

Category 19.8 *Plagiarism & cheating*

2001-06-28 **plagiarism cheating dishonesty software biometric identification schools**

NewsScan

SCHOOLS ADOPT HIGH-TECH ANTI-CHEATING TOOLS [11 Jun 2001]
Secondary and post-secondary schools are increasingly trying to defeat high-tech cheaters by using high-tech tools to search out plagiarism, exam manipulation, and other forms of dishonesty. Some examples: software from turnitin.com will be used at 1,800 schools to compare term papers with text on the Internet and in publications; more than 100 schools will use software that prevents students from using e-mail or the Web to cheat on computer-based tests; national testing centers will use thumbprint scanners and digital cameras to monitor students and prevent imposters from taking tests under other names. The tools seem to work: an anti-plagiarism service tested at UCLA this year detected "significant instances of plagiarism" in student papers and lab reports submitted. (USA Today 11 Jun 2001)
http://www.usatoday.com/life/cyber/tech/2001-06-11-tech-tools-nab-cheaters.h tm

THEIR CHEATIN' TECHNO HEARTS: HS STUDENT PLAGIARISM [28 Jun 2001]
According to a survey of 4,500 high school students by Rutgers management professor Donald McCabe, who has studied cheating on college campuses, plagiarism from Web sites is even worse a problem at the secondary level than at the university level. More than half of the high school students surveyed admitted either downloading and reusing an entire paper from the Web or at least copying parts of a paper without citation. Of college students surveyed, only 10-12% have admitted doing such things. But plagiarists often get caught, and the Internet sometimes taketh away what the Internet hath given... as can happen when a teacher enters the five or so words from a student paper and plugs them into a search engine. Then the game is over. (New York Times 28 Jun 2001)
http://partners.nytimes.com/2001/06/28/technology/28CHEA.html

---

Category 19.8 *Plagiarism & cheating*

2002-08-08 **plagiarism intellectual property professors students essays**

NewsScan

ANTIPLAGIARISM SOFTWARRE: 'WHOSE ESSAY IS IT, ANYWAY?'
Various academic institutions now use antiplagiarism software to catch student cheaters -- but some critics say such software tramples on student rights, specifically their copyrights. Example: the antiplagiarism product Turnitin.com expands its database by keeping copies of scanned student papers without getting the permission from the student; the papers can then be used for comparison with new submissions as they are received in the future. Is this a permissible practice? Sure, says Turnitin -- this use of the papers doesn't threaten any potential commercial value of the papers and is well within "Fair Use" rules. [Antiplagiarism aficionados will enjoy Bernard Malamud's 1961 novel "A New Life," in which faculty members work frantically but unsuccessfully to expose a student.] (IEEE Computer Aug 2002)

Category 19.8 *Plagiarism & cheating*

2004-01-21 **copyright law plagiarism university student**

http://www.cnn.com/2004/LAW/01/21/ctv.plagiarism/

STUDENT WINS FIGHT AGAINST TURNITIN USE

A McGill University student refused to allow his professors to submit his essays to the Turnitin.com plagiarism checker on the grounds that it was violating his intellectual property rights. The senate committee reviewing his case agreed with him.

Category 19.8 *Plagiarism & cheating*

2004-02-05 **electronic copyright distortion corruption modification attribution source Google search engine plagiarism authenticity**

RISKS 23 18

PLAGIARISM TOO EASY

Jim Griffith complained about the distortion of a 1997 article he wrote that was recently modified without his permission, stripped of attribution, and widely circulated and even printed in otherwise reputable astronomy publications. He wrote, "As moderator of RHF, I understand the difficulties of identifying the original source of a piece, and the ease with which people remove attributions. I'm disturbed by the casual way so many publications blindly printed the piece without doing a serious attempt to identify the source or the original version. Granted, that source isn't immediately obvious, but a reasonable Google search or a date-sorted Google Groups search would have definitively identified both the author and the original wording. In effect, Google Groups is now my primary hope for preserving my original copyright (although I did have the foresight to encode in the piece an in-joke that only I know -- and the plagiarized versions preserve that in-joke). Had I originally distributed the piece via e-mail, I'd now have no hope of ever claiming credit or preserving the original version." He added, "I'm mainly disturbed by the ease with which the original piece was corrupted, and that that corruption was blindly accepted and propagated. It is now the case that corrupted version is more prevalent than the original. This is disappointing, given that an advantage of electronic communications is supposed to be the way it preserves information. I wonder if we'll find that in a hundred years, the most popular Internet version of "Romeo and Juliet" is one with a new, happier ending?"

Category 19.8 *Plagiarism & cheating*

2004-04-06 **plagiarism filters artificial intelligence pattern matching industry**

NewsScan

PLAGIARISM SOFTWARE DETECTS NEW MARKET IN CORPORATE WORLD

Software designed to detect plagiarism is moving from academia, where it's been used for years to flag phony term papers, to the corporate world. Newspapers, law firms and even the U.N. Security Council are using the data-sifting tools to ensure their documents are original works, and companies such as iParadigm, Glatt Plagiarism Services, MyDropBox and CFL Software Development have moved quickly to meet the new demand. And while some businesses have been reluctant to deploy such software, iParadigm president John Barrie predicts that soon the number of corporate clients will outstrip academics. "The stakes are 100 times greater. We're not talking about grades anymore," he says. (AP/Washington Post 6 Apr 2004)

Category 19.8 *Plagiarism & cheating*

2005-03-14 **study online citation sources plagiarism copyright infringement Iowa State University**

EDUPAGE; http://chronicle.com/prm/daily/2005/03/2005031402n.htm

STUDY SHOWS ONLINE CITATIONS DON'T AGE WELL

A study conducted by two academics at Iowa State University has shown a remarkably high rate of "decay" for online citations. Michael Bugeja, professor of journalism and communication, and Daniela Dimitrova, assistant professor of communication, looked at five prestigious communication-studies journals from 2000 to 2003 and found 1,126 footnotes that cite online resources. Of those, 373 did not work at all, a decay rate of 33 percent; of those that worked, only 424 took users to information relevant to the citation. In one of the journals in the study, 167 of 265 citations did not work. Bugeja compared the current situation to that of Shakespearean plays in the early days of printing, when many copies of plays were fraught with errors due to the instability of the printing medium. Anthony T. Grafton, a professor of history at Princeton University and author of a book on footnotes, agreed that citation decay is a real and growing problem, describing the situation as "a world in which documentation and verification melt into air." Chronicle of Higher Education, 14 March 2005 (sub. req'd)

Category 19.8 *Plagiarism & cheating*

2005-05-19 **software plagiarism uncovering self-plagiarism Cornell University intellectual property rights violation copyright infringement**

EDUPAGE; http://chronicle.com/prm/daily/2005/05/2005051901t.htm

JOURNALS USING SOFTWARE TO UNCOVER PLAGIARISM

Software designed to uncover plagiarism is increasingly being used not only for student papers, where it got its start, but also for academic journals, where it is turning up instances of self-plagiarism as well. Although some dismiss self-plagiarism as unimportant relative to plagiarizing another's work, the practice of republishing one's own work in various venues strikes others as similarly objectionable. Christian Collberg, assistant professor of computer science at the University of Arizona, characterized self-plagiarism as vita padding and said that self-plagiarists who are funded from public sources are misusing taxpayer money. Collberg is working on a software application specifically designed to uncover instances of self-plagiarism. Though not as concerned about self-plagiarism, Cornell University is testing a plagiarism-detection application on an archive it maintains of articles in physics, math, and computer science. Among the 300,000 articles in the archive, the tool has found a few thousand instances that warrant further investigation. Chronicle of Higher Education, 19 May 2005 (sub. req'd)

Category 19.8 *Plagiarism & cheating*

2006-03-26 **technology cell phone cheating exams UK concern**

EDUPAGE; http://news.bbc.co.uk/2/hi/uk_news/education/4848224.stm 23

PHONE CHEATING INCREASING

According to the Qualifications and Curriculum Authority (QCA), cheating on examinations in the United Kingdom is increasing, due in part to the number of cell phones being taken into exams. Although the incidence of cheating remains relatively low, officials from the country's testing agencies have begun to separate the kinds of cheating they discover. New data indicate that in 60 percent of the cases reported, the infraction involved bringing a cell phone into a test. Despite acknowledging that many times the phones were brought accidentally, the QCA said in its report that "it is essential that [the cheating] is actively addressed to ensure that learners, parents, and employers can continue to have confidence in the examination system." A spokesperson from the Department for Education and Skills echoed those sentiments, saying, "We expect schools to maintain high standards of discipline." The spokesperson continued, "There is no place for mobile phones in the classroom, let alone in the examining hall."

19.9 Counterfeit products (hardware, clothing etc.)

Category 19.9 *Counterfeit products (hardware, clothing etc.)*

1998-12-23 **e-commerce fraud counterfeit risks consumers warnings**

InternetWeek
http://www4.zdnet.com/intweek/stories/news/0,4164,2178151,00.html

An article by Connie Guglielmo in Inter@ctive Week for December 23, 1998 summarized the non-technical risks of online shopping. Some criminals are selling counterfeit goods through their Web sites. Brand-holders are using the services of professional firms to sweep the Net looking for unauthorized use of their trademarks.

Category 19.9 *Counterfeit products (hardware, clothing etc.)*

2002-04-14 **data integrity authenticity illusion virtual reality fraud pretence simulation VR**

NewsScan

VIRTUAL NEWS SETS
More than 40 U.S. television stations and many production studios are now using virtual newsrooms that give the impression that newscasters are broadcasting from gigantic, futuristic sets when the truth is that they are actually in cramped, narrow rooms. How is it done? Just about everything in the room is painted a certain shade of blue, and when the TV camera records that particular color it substitutes digital imagery to make people and any objects not in that color appear superimposed on the digital set. So when you see a news anchor standing in front of a huge wall of video monitors, you're just seeing "smoke and mirrors" (or maybe just mirrors -- unless the anchor's excitement set his pants on fire). (New York Times 14 Mar 2002)
http://www.nytimes.com/2002/03/14/technology/circuits/14HOWW.html

---

Category 19.9 *Counterfeit products (hardware, clothing etc.)*

2005-01-04 **AMD microprocessor chip manufacturer warning counterfeit PC server chips Athlon XP**

DHS IAIP Daily; http://www.internetnews.com/ent−news/article.php/3454481

AMD WARNS ABOUT COUNTERFEIT PC AND SERVER CHIPS

AMD is warning customers of potentially mislabeled PC and server chips after helping foil a counterfeit ring in Taiwan. The company alerted authorities to a problem in Taipei late last month. Raids at four sites led to multiple arrests for "re-marking" or reselling re-marked AMD Athlon, Athlon XP and Opteron processors. Re-marked processors have been tampered with and may have been illegally re-labeled with inaccurate frequencies, model numbers, or both. "We strongly recommend consumers and businesses buy AMD processors only from authorized distributors and certified resellers," AMD spokesperson Catherine Abbinanti said. AMD said customers can identify genuine AMD products by a so-called "Processor-in-a-Box" sticker. The label, which has been in place since 2003, includes a unique serial number and a 3-D hologram used for tracking, distribution, authenticity and warranty service.

1A Criminal hacker scene (conventions, meetings, testimony, biographies, publications)

Category 1A *Criminal hacker scene (conventions, meetings, testimony, biographies, publicati*

1997-01-14 **sabotage infowar information warfare**

EDUPAGE

Gateway2000 discovered that 20,000 copies of a promotional video promoted more than its new PC; the tape included 30 seconds of pornography. Officials guess that it's a case of industrial sabotage by a disgruntled employee in the company that made the tape.

Category 1A *Criminal hacker scene (conventions, meetings, testimony, biographies, publicati*

1997-05-02 **sabotage**

RISKS 19 12

According to Peter Neumann, "Wilson Chan Chi-kong, 29, the former employee of Reuters financial information agency who had sabotaged the dealing-room systems, was apparently motivated by revenge after a dispute with his superior. The damage control took more than 1,700 man-hours, and the estimated cost was HK$1.3 million. He has been jailed."

Category 1A *Criminal hacker scene (conventions, meetings, testimony, biographies, publicati*

1997-05-05 **criminal hackers revenge sabotage**

Netly News

Both Jonathan Littman and Joshua Quittner have been harassed by enraged criminal hackers and their supporters for daring to write opinions critical of hacker icons Kevin Mitnick and Kevin Poulson. Interference has included disconnection of ISP access, interference with e-mail, and attacks on Web pages promoting Littman's book. Quittner suffered damage to his e-mail services and extensive rerouting of his home phone: to a long-distance answering machine, to a phone-sex number and to 1-800-EAT-SHIT.

Category 1A *Criminal hacker scene (conventions, meetings, testimony, biographies, publicati*

1997-06-27 **backhoe denial of service sabotage Net**

OTC

In another "backhoe attack," a construction crew inadvertently sliced through a major component of the Internet backbone in Florence, NJ. WorldCom's service to UUNet Technologies and MFS Communications as well as several other ISPs were severely affected. Many users were unable to access the Net and e-mail transfers were erratic throughout the U.S.

Category 1A *Criminal hacker scene (conventions, meetings, testimony, biographies, publicati*

1997-07-17 **libel e-mail infowar sabotage**

PA News

In England, Western Provident Association Ltd sued Norwich Union Healthcare Ltd in 1995 over rumors that WPA was insolvent and under investigation by the Department of Trade and Industry. Norwich Union executives admitted that its employees had circulated internal e-mail with these false allegations and agreed in July to pay WPA £45,000 (about $75,000) in damages out of court. Moral: apply the same standards of ethical judgement to e-mail communications as to any other communication.

Category 1A *Criminal hacker scene (conventions, meetings, testimony, biographies, publicati*

1997-07-20 **sabotage**

EDUPAGE

An enraged computer user shot his PC four times in the hard drive and once in the monitor. The Issaguah, WA resident was arrested by police.

Category 1A *Criminal hacker scene (conventions, meetings, testimony, biographies, publicati*

1997-08-10 **ISP availability disaster**

EDUPAGE

In early August, an explosion interrupted electrical power around Boston; a resulting fire at MIT blocked access to the Net for BBN Planet subscribers.

Category 1A *Criminal hacker scene (conventions, meetings, testimony, biographies, publicati*

1997-08-12 **hacker spam vandalism Web hacktivism**

C|Net http://www.news.com/News/Item/0,4,13296,00.html

A hacker attacked "Spamford" Wallace's Cyber Promotions site in August, causing several hours of downtime. Anti-spam activists generally condemned the use of illegal tactics to harass the King of Spam.

Category 1A *Criminal hacker scene (conventions, meetings, testimony, biographies, publicati*

1997-08-22 **online voting fraud rigging farce**

Netly News

When Cool Site of the Day announced that nominations for Cool Site of the Year were open to the 365 winners of the daily contest, they didn't expect one of their former winners to try to rig the election. However, managers of Zug, a comedy site, asked the 364 other participants to vote for Zug in the Cool Site of the Year category; in return, they would nominate cooperators in whatever other category they wanted. Cool Site of the Day managers were terribly offended, even though the practicality of honest online voting is currently zero.

Category 1A *Criminal hacker scene (conventions, meetings, testimony, biographies, publicati*

1997-11-25 **sabotage disgruntled employee**

EDUPAGE, Newsbytes, RISKS 19 47

A disgruntled former help-desk operator at Forbes Magazine was accused of sabotaging the company's computers and causing more than $100,000 in damages. In a similar case brought at the same time, an enraged consultant for Art Assets of Manhattan allegedly deleted files and databases on his client's systems after being insulted at a meeting to discuss a billing dispute. The accused faced up to five years in jail and fines of up to $250,000 if convicted of the respective crimes.

Category 1A *Criminal hacker scene (conventions, meetings, testimony, biographies, publicati*

1998-06-30 **sabotage penetration data diddling deletion crash insider**

EDUPAGE

In a scenario worthy of a pulp thriller or of a B-movie, Shakuntla Devi Singla was a US Coast Guard civilian data processing worker who thought that one of the contractors servicing her employer's computer systems was breaking the law. When her warnings were disregarded, she went ballistic and wiped out the USCG's personnel database, crashing the system to boot and forcing them to boot (as it were). According to the EDUPAGE editors, "It took 115 Coast Guard employees 1,800 hours to restore the data. . . ." Singla was sentenced to five months imprisonment followed by five months of home detention and fined $35,000 in restitution to the USCG. It may all have been, in the words of Mrs Alberta Simms of Kipling Road, "Better than bottlin' it up, i'n'it?"* but one wishes the poor woman had found a less drastic way of expressing her frustration.

* An obscure but irresistible reference to the equally obscure but irresistible "Ethel the Frog" program by Monty Python about the notorious Piranha Brothers.

Category 1A *Criminal hacker scene (conventions, meetings, testimony, biographies, publicati*

1999-09-29 **criminal hacker vulnerability sabotage demonstration**

Scotsman

In early August 1999, a criminal hacker calling himself "Red Attack" (Frans de Vaere) threatened Belgian firms with electronic sabotage in a misguided attempt to draw attention to security vulnerabilities. A few weeks later, a different person claimed _he_ was the _real_ Red Attack and said that he would switch Belgian electrical power off for a couple of hours on September 29th as well as breaking into the Belgian Prime Minister's e-mail account. After earnest conversations with a company director of the Electrabel utility, the idiot agreed that maybe his demonstration wasn't such a great idea after all. In the event, the threats all evaporated. Was this yet another hoax perpetrated on gullible journalists and officials?

Category 1A *Criminal hacker scene (conventions, meetings, testimony, biographies, publicati*

1999-09-30 **availability service disruption cable Internet traffic slow backhoe**

New York Times

An Ohio gas company worker accidentally cut a 40 Gbps east-west optic fiber cable at the end of September (an example of the notorious "backhoe attack"). Internet traffic was slowed as much as 50 times as terabits of data were rerouted through alternate connections. Repairs took about a day.

Category 1A *Criminal hacker scene (conventions, meetings, testimony, biographies, publicati*

1999-10-16 **backhoe attack denial of service accident fiber optic cable cut**

RISKS 20 64

On 1999-10-16, a backhoe accident destroyed a major fiber-optic cable in Massachusetts. AT&T, MCI Worldcomm, and the Mass Turnpike Authority lost channels, resulting in major problems for people on the East coast of the US.

Category 1A *Criminal hacker scene (conventions, meetings, testimony, biographies, publicati*

1999-11-26 **backhoe attack denial of service accident fiber optic cable cut**

RISKS 20 13

In Canada, a railway backhoe operator severed an AT&T Canada optic fiber cable on 1999-11-26, causing computer crashes, shutdown of phone lines and communications problems throughout southern Ontario. The Bank of Nova Scotia was without computer services and Internet services were slow because rerouted connections went through the US on the Thanksgiving holiday there.

Category 1A *Criminal hacker scene (conventions, meetings, testimony, biographies, publicati*

1999-12-13 **information warfare sabotage hacktivists political anti-corporate**

Globe and Mail (Canada), http://www.rtmark.com

The battle between etoys (www.etoys.com) and etoy (www.etoy.com) brought to light a remarkable group of saboteurs calling themselves ®™mark (pronounced "artmark") who organized all kinds of shenanigans normally associated with criminal hacking (denial of service attacks on eToys.com servers in a "virtual sit-in") and information warfare (depressing the value of eToys.com stock using propaganda). See < http://www.rtmark.com >.

1A1 Criminal hacker conventions and meetings

Category 1A1 *Criminal hacker conventions and meetings*

2003-04-14 **student hacking demonstration intellectual property systems disallowed Georgia**

NewsScan

COURT BLOCKS PRESENTATION ON HACKING UNIVERSITY SYSTEMS
A Georgia state court has issued a restraining order prohibiting two students from making a conference presentation on how to break into and modify a university electronic transactions system. Blackboard, an education software company, argued that the information in the presentation was gained illegally and would have harmed the company's commercial interests and those of its clients, but Interz0ne conference organizers argued that the students' free speech rights were abridged. "The temporary restraining order pointed out that the irreparable injury to Blackboard, our intellectual property rights and clients far outweighed the commercial speech rights of the individuals in question," said a Blackboard spokesman. The information was gleaned after one of the students had physically broken into a network and switching device on his campus and subsequently figured out how to emulate Blackboard's technology. Because that alleged act was illegal, publication of the resulting information should be blocked, said the court. The court's decision was grounded largely in federal and Georgia state antihacking laws and a state trade secrets act, rather than the Digital Millennium Copyright Law, which has been invoked in several similar cases. (CNet News.com 14 Apr 2003)

Category 1A1 *Criminal hacker conventions and meetings*

2003-07-31 **manifesto superworm Cide Red Brandon Wiley Curious Yellow bandwidth sapphire worm cybersecurity**

NIPC/DHS

July 31, Government Computer News — Superworm Manifesto unveiled at cybersecurity briefings.

Typical worms, such as Code Red, use random scanning to propagate, wasting bandwidth and competing with themselves once released. The Sapphire worm, an example of a theoretical worm concept called Warhol, succeeded in infecting 90 percent of vulnerable machines within about 10 minutes, but continued trying to spread randomly, drawing attention to itself and quickly running out of bandwidth. Brandon Wiley of the Foundation for Decentralised Research unveiled a guide for creating a new generation of worms this week at the Black Hat Briefings security conference in Las Vegas, NV. He also offered a way for systems to be inoculated. Wiley's superworm concept, called Curious Yellow, would combine the fast-spreading characteristics of a Warhol worm with an algorithm that would let the worms coordinate their activities to avoid overlap, multiple infections and competition. The result is a large, robust network of exploited machines that can be continually updated to carry out tasks, benign or malicious.

Category 1A1 *Criminal hacker conventions and meetings*

2004-08-03 **computer hacking contest Singapore HackAttack 2004**

DHS IAIP Daily; http://www.usatoday.com/tech/news/2004−08−03−singapore−hacke rs_x.htm

August 03, Associated Press — Singapore to hold computer hacking contest.

Singapore said Tuesday, August 3, it would organize a contest to find the tech-savvy city-state's best computer hacker. Six pairs will compete in the August 20 "BlackOPS: HackAttack Challenge 2004," organized by the government-funded National Infocomm Competency Center, said its marketing manager Yvonne Choo. They will "penetrate, exploit, gain access and obtain privileged information from the other teams' servers, for the purpose of corporate espionage," the center said on its Website. Teams will also have to defend their organization's networks against hacking from other teams in the daylong event, it added. Choo said he hoped the contest would help shed light on ways to prevent actual computer attacks. The prize for the best hacker will be a DVD burner and free computer classes. Asia has been the root of some of the worst attacks by hackers in recent years. Close to 80% of Singapore's four million citizens own personal computers and the island is largely considered to be the most technologically advanced in Southeast Asia.

Category 1A1 *Criminal hacker conventions and meetings*

2004-08-03 **Defcon 12 Meet the Feds presentation talk recruitment NSA US government criminal hacker**

DHS IAIP Daily; http://www.pcworld.com/news/article/0,aid,117226,00.asp

August 03, PC World — Government seeks a few good hackers.

A well-attended session at the recent Defcon 12 hackers' conference in Las Vegas, NV, was "Meet the Feds," a recruitment presentation by a group of federal cybercrime law enforcement agents, who fielded questions from would-be cybercops. September 11, 2001, marked a turning point for government recruitment, says former NSA Director of Information Assurance Mike Jacobs, who now works in the private sector. Before the terrorist attacks, the NSA typically received about 200 applications monthly, he adds. In the three months following the attacks, more than 20,000 people applied for employment at the NSA. In the presentation, he urged computer-savvy patriots to put their skills to use defending the country from spies, terrorists, and other criminals. One hitch, of course, is a security clearance--elusive for some hackers. Jim Christy, director of the Department of Defense's Cyber Crime Center, and Tim Huff, a special agent with the FBI's Computer Analysis Response Team, fielded questions about so-called gray-hat hackers, who sometimes break the law but aren't charged. Christy and Huff made it clear that cybercriminals--even those who haven't been caught--are not likely to be invited to join the ranks of cybercops.

Category 1A1 *Criminal hacker conventions and meetings*

2004-08-20 **computer hacking contest Singapore HackAttack 2004 techniques**

DHS IAIP Daily;
http://story.news.yahoo.com/news?tmpl=story&cid=562&ncid=738&e=7&u=/ap/20040820/ap_on_hi_te/singapore_hacking_contest

August 20, Associated Press — Computer experts vie in hacking contest.

Twelve computer experts hunkered down Friday, August 20 for a seven-hour contest to find the best hacker in tech-savvy Singapore. Divided into six two-person teams, the contestants participating in "BlackOPS: HackAttack challenge 2004" have to defend their networks and servers from hacking while attacking other teams' systems. The contestants hailed from Brunei, China, Myanmar and Singapore, but their identities couldn't be revealed because they all work in the computer security business, organizers said. Teams were not allowed to use the Internet as a hacking tool, only computers and modems. Asia has been the root of some of the worst attacks by hackers in recent years. Singapore has said it is increasingly concerned about cyber security in the highly wired city-state where eight in 10 households own personal computers. Hackers can be jailed for up to three years or fined up to $5,852 under Singapore's Computer Misuse Act. Organizers had said they hoped the contest would help shed light on ways to prevent actual computer attacks.

1A2 Criminal hacker testimony in court or committees

Category 1A2 *Criminal hacker testimony in court or committees*

2003-02-21 **criminal hackers sentencing study analysis**

NewsScan

LAWYERS SAY HACKERS ARE GETTING BUM RAP
The National Association of Criminal Defense Lawyers has joined with the Electronic Frontier Foundation and the Sentencing Project in publishing a position paper that argues people convicted of computer-related crimes tend to receive harsher sentences than perpetrators of comparable non-computer-related offenses. "The serious nature of the offenses is overplayed," says Jennifer Granick, author of the paper and clinical director at Stanford University's Center for Internet and Society. "The (majority) of the offenses are generally disgruntled employees getting back at the employer or trying to make money." In a review of 55 cases prosecuted under the most-often used computer crime statute, only 15 involved harm to the public and only one resulted in a threat to safety. Those convicted "are receiving sentences based on the fear of the worst-case scenario rather than what the case may really be about," says Granick. The paper was submitted in response a request for public comment by the U.S. Sentencing Commission as required by the Homeland Security Act of 2002. Cybercrime legal expert Scott Frewing says he agrees with many points raised in the paper, but recommends a two-tiered sentencing threshold: "I would be comfortable in a situation where the code addresses the discrepancy between those who cause bodily injury and those that don't. If that results in the law being unfair to a virus writer, maybe that's enough to put them on notice." (CNet News.com 20 Feb 2003)
http://news.com.com/2100-1001-985407.html

Category 1A2 *Criminal hacker testimony in court or committees*

2003-09-10 **hacker arrested Adrian Lamo FBI new York Times Yahoo Google WorldCom ExciteAtHome**

NewsScan

HACKER ARRESTED
Twenty-two-old hacker Adrian Lamo turned himself in to federal marshals — with the surrender filmed by an independent camera crew that had been following him for days for a documentary film. He has publicly acknowledged involvement in some dramatic computer break-ins at large corporations during the past several years, including The New York Times, Yahoo!, WorldCom and ExciteAtHome, and captured the Social Security numbers of celebrities and government officials who contributed to the op-ed pages of the Times. In the past, Lamo has offered to work for free with his hacking victims after each break-in to improve the security of their networks. (AP/San Jose Mercury News 10 Sep 2003)

Category 1A2 *Criminal hacker testimony in court or committees*

2003-09-17 **blaster teen innocent case court Jeffrey Parson**

NewsScan

TEEN PLEADS INNOCENT IN BLASTER CASE
In an appearance yesterday before a federal court in Seattle, high school senior Jeffrey Parson entered a plea of innocence to a charge that he had unleashed the Blaster.B worm that infected more than 7,000 computers. If convicted, the young man faces a maximum sentence of 10 years in prison. Parson's contention is that the government overstated its case to try to make an example of him. (AP/San Jose Mercury News 17 Sep 2003)

Category 1A2 *Criminal hacker testimony in court or committees*

2003-09-18 **FBI bust hackers David Smith Melissa Virus creator helps AP Associated Press 1999 arrest track viruses senders DeWit Netherlands**

NIPC/DHS

September 18, Associated Press — Virus sender helped FBI bust hackers.

Federal prosecutors credited the man responsible for transmitting the Melissa virus — a computer bug that did more than $80 million in damage in 1999 — with helping the FBI bring down several major international hackers. Court documents unsealed Wednesday, September 17, at the request of The Associated Press show that David Smith began working with the FBI within weeks of his 1999 arrest, primarily using a fake identity to communicate with and track hackers from around the world. According to the court document, Smith helped the FBI bust virus senders abroad and stop viruses in the U.S. The letter says that two months after his arrest, Smith gave the FBI the name, home address, e-mail accounts and other Internet data for Jan DeWit, the author of the so-called Anna Kournikova virus in the Netherlands. The FBI passed the information on to authorities in the Netherlands. DeWit was arrested and later sentenced to probation. The federal prosecutor also said that Smith was working with the FBI to develop an investigative tool that theoretically could help identify an e-mail sender who was trying to mask his or her identity.

Category 1A2 *Criminal hacker testimony in court or committees*

2005-07-05 **Sasser worm author confession Germany prosecution Sven Jaschen**

EDUPAGE; http://www.nytimes.com/reuters/technology/tech-crime-germany-sasser.html

AUTHOR OF SASSER WORM CONFESSES

Prosecutors in Germany have announced that Sven Jaschan, on trial for writing the Sasser computer worm, this week confessed to all charges against him. Regarded as possibly the most damaging computer worm ever released, Sasser and its several versions are blamed for crashing as many as one million computers around the world, affecting home users and companies including the European Commission and Goldman Sachs. Jaschan, who is 19 now and was a minor when he committed some of his crimes, had previously admitted to writing the worm; this week, he also confessed to data manipulation, computer sabotage, and interfering with public corporations. He faces up to five years in prison and paying restitution to those affected by Sasser. Monetary damages from the worm have only reached about $150,000, but that number could easily rise into the millions if all those affected reported the damage. New York Times, 5 July 2005 (registration req'd)

1A3 Biographical notes on individual criminals (including arrests, trials)

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2000-01-21 **criminal hacker incarceration prison jail release probation**

DOW JONES BUSINESS NEWS

Criminal hacker icon Kevin Mitnick was released from prison on 2000-01-21 on parole, instructed to stay away from computers, software, modems, cell-phones and Internet-connected devices for the next three years. These conditions would make it difficult for Mitnick to enroll in college for a degree in computer science, as he desired.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2000-07-13 **criminal hacker parole restrictions censorship**

NewsScan, CNet http://www.nytimes.com/cnet/CNET_0_4_1951220_00.html, ://news.cnet.com/news/0-1005-200-2250843.html?tag=st.ne.ron.lthd.ni

Ex-convict network hacker Kevin Mitnick, out on parole but forbidden by the court to write or speak about the computer industry, is being represented by New York attorney Floyd Abrams, an expert on the First Amendment to the Constitution, which guarantees freedom of speech. Abrams has been retained by publisher Steven Brill, who wants to use Mitnick as a columnist for the Contentville Web site. (CNet/New York Times 25 May 2000)

[In July,] Kevin Mitnick. . . won the right to pursue computer-related work. . . . [A] federal judge agreed that the restrictions were overly broad. Among the jobs now approved are: writing for Steven Brill's online magazine Contentville, speaking in Los Angles on computer security, consulting on computer security, and consulting for a computer-related TV show. Mitnick spent five years in prison after the FBI fingered him in a series of attacks on companies, including Motorola, Novell, Sun Microsystems and the University of Southern California. (AP/CNet 13 Jul 2000)

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2000-09-21 **criminal hackers penetration civil law indictment conviction sentencing settlement court law legal proceedings judgement punishment fine pump-and-dump stock fraud interception wiretapping**

RISKS 21 06

Peter G. Neumann summarized three legal cases involving computer fraud and abuse:

On 20 Sep 2000, Jonathan Lebed, 15, settled a federal civil-fraud process, agreeing to pay $272,826 for perpetuating bogus information on the Internet that led to the stock fluctuations in Just Toys Inc. and The Havana Republic and profiting therefrom.

On 21 Sep 2000, Jonathan James (cOmrade), 16, pleaded guilty to two counts of juvenile delinquency and was sentenced to six months detention for having penetrated DoD and NASA computer systems, intercepting 3,300 e-mail messages and stealing passwords. (He was 15 at the time. If he had been an adult, he reportedly would have received a sentence of at least 10 years.)

On 21 Sep 2000, Jason Diekman, 20, was charged with cracking into university (including Harvard, Stanford, and Cornell) and NASA computer systems, and stealing hundreds of credit-card numbers to buy thousands of dollars of clothing, stereo equipment, and computer hardware.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2000-09-28 **criminal hacker social engineering advice legitimation**

NewsScan;MSNBC http://www.msnbc.com/news/469018.asp

Infamous hacker Kevin Mitnick, in his first public speech since his release from prison last January, warned information technology directors that the key to network security is vigilance, detection and quick reaction. "You should adopt the mantra, 'In God we trust. Everybody else is suspect.' People are the weakest link when it comes to security, and an important question to ask yourself is not if, but when, is your e-business going to be targeted?" (ZDNet 28 Sep 2000)

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2001-01-19 **criminal hacker trial plea guilty distributed denial of service DDoS**

NewsScan

MAFIABOY PLEADS GUILTY
A 16-year-old Montreal network vandal has pled guilty to 56 charges related to attacks last February on a number of major Web sites around the world, including Amazon, CNN, eBay, Yahoo and Dell, in a rampage causing US$1.7 billion in damage according to FBI estimates. The young man said "I would be very surprised if it would that high," and showed no remorse. An officer of the Canadian Mounted Police said: "He was fairly proud of what he did, how he committed the crimes and what tools he used. He bragged that the FBI. was unable to catch him, that the FBI were fools, and that he would commit these crimes again. He boasted that he would make lots of money with the case and that he would become famous." The boy has quit school and taken a job as busboy in a steakhouse; because he is a minor, the maximum penalty he faces is two years in prison and a $650 fine. (New York Times 19 Jan 2001)
http://www.nytimes.com/2001/01/19/technology/19CANA.html

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2001-02-14 **worm writer excuses exculpation culture psychology**

NewsScan

HACKER DEFENDS HIS VANDALISM, BLAMES THE VICTIMS
Defending his vandalism as an attempt to do good, a 20-year-old Dutch student arrested for creating the so-called Anna Kournikova computer virus that jammed Internet traffic throughout the world justified his action by saying he "never wanted to harm the people" whose computers he infected. He claims he intended only to issue them a warning to tighten their Internet security, and insisted that "after all it's their own fault they got infected." (AP/New York Times 14 Feb 2001)

In September, a contributor to RISKS 21.67 reported, "The 20-year-old creator for the Kournikova virus, J. de W. from Sneek, was sentenced to 150 hours of community service by the court of Leeuwarden this Thursday. The prosecution demanded the maximum of 240 hours of community service. In February De W. released on the Internet the so-called wormvirus, which spread itself as an e-mail message. The virus was activated by clicking the e-mail which was titled Anna Kournikova (the tennis player). This lead to inconvenience of Internet users all over the world. When determining the sentence, the court took into consideration that the boy had no previous run-in with justice, that he turned himself in, and that material damages were limited. The American investigation service FBI reported an amount of [$166,827] in damages."
http://www.volkskrant.nl/nieuws/nieuwemedia/1001567916953.html (in Dutch).

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2001-10-21 **criminal hacker phreak opinion surveillance terrorism privacy**

NewsScan

MITNICK SAYS TERRORISTS AREN'T "SUBTLE LITTLE HACKERS"
Infamous phone-system hacker Kevin Mitnick, who served more than four years of jail-time for breaking into telephone company computer systems, is critical of new antiterrorist legislation that makes government surveillance easier. "Terrorists," says Mitnick, "have proved that they are interested in total genocide, not subtle little hacks of the U.S. infrastructure, yet the government wants a blank search warrant to spy and snoop on everyone's communications." Mitnick, forbidden from using information technology without the permission of his probation officer, now plays a CIA computer expert in the TV spy drama "Alias." (Observer 21 Oct 2001)
http://www.observer.co.uk/international/story/0,6903,577846,00.html

---

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2002-03-04 **criminal hacker virus writer subculture personality teenager adolescent rebellion reputation woman girl female stereotype e-mail enabled worm**

NewsScan

GIRLS JUST WANT TO HAVE HACKER FUN [4 Mar 2002]
An unidentified hacker who claims to be a 17-year-old girl says she was motivated to write the "Sharpei" worm to dispel the notion that there aren't any female virus writers and to annoy Microsoft, rather than to have it spread to actual computer users. Going by the name "Gigabyte," she says on her Web site that she's a high-school senior who takes kick-boxing classes and likes techno and trance music. A consultant for Sophos, the U.K. based security company that reported the worm says, "I just don't know what she's accomplishing by this. She's neither hurting nor helping people." The worm was written to spread via Outlook Express e-mail, with a subject line reading, "Important: Windows Update." (Reuters/New York Times 4 Mar 2002)
http://www.nytimes.com/reuters/technology/tech-tech-feminist.html

---

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2002-05-02 **virus writer prosecution judgement sentence jail prison fine**

NewsScan

MELISSA VIRUS WRITER NETS JAIL TIME
David L. Smith, creator of the "Melissa" virus, was sentenced Wednesday to 20 months in prison and a $5,000 fine for his role in unleashing the destructive program that caused more than $80 million worth of damage worldwide in 1999. Smith, who is among the first people ever prosecuted for creating a computer virus, called the act a "colossal mistake." "My curiosity got the better of me, as I soon began to write the 'Melissa Virus,'" he wrote in a letter to U.S. District Judge Joseph A Greenaway Jr. "It didn't take me too long as I borrowed a lot of the code from other viruses that I found on the Internet." Smith could have received up to five years in prison, but prosecutors suggested the shorter sentence, saying he had given authorities extensive assistance in thwarting other virus creators. (AP 1 May 2002)
http://apnews.excite.com/article/20020501/D7J85S3O0.html

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2002-08-06 **worm prosecution charge court Trojan**

C|Net News http://news.com.com/2100-1001-948596.html

In Augusst 2002, five Israeli teenagers from grades 8, 10 and 11 were charged in Haifa with creating the Goner worm (aka Pentagone and Gone), a trivial piece of work that disabled some firewalls and antivirus tools and spread through ICQ and e-mail. The worm did cause some servers to crash at various organizations around the world including NASA computer centers.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2002-09-20 **virus writer arrest Linux operating system**

NewsScan

ARRESTS: . . . . VIRUS CREATION
In London, law enforcement officials at Scotland Yard have arrested a 21-year-old programmer they say created the T0rn (with a zero) virus, which was designed to do malicious damage to Linux computer systems. . . . (Reuters and New York Times 19 Sep 2002)

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2002-10-07 **international criminal hacker consultants fraud conspiracy sting entrapment monitoring surveillance sniffing keystroke logging court trial prosecution sentence prison**

NewsScan

RUSSIAN CAUGHT BY FBI STING GOES TO JAIL FOR COMPUTER CRIMES
Twenty-seven-year-old Russian computer hacker Vasily Gorshkov came to the U.S. for a job interview, but the interview was part of a sting operation to apprehend Gorshkov and another programmer for computer crimes, fraud and conspiracy. The two Russians complied with a request by the bogus interviewers to demonstrate their hacking skills, and when they used their passwords to hack into a computer network in Russia the FBI secretly logged those passwords to gather evidence against the pair. Gorshkov has just been sentenced to three years in a U.S. federal prison. (VNUnet 7 Oct 2002)
http://www.vnunet.com/News/1135691

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2003-01-06 **Xbox hacking mastermind Microsoft Linux Lindows rivalry**

NIPC/DHS

January 03, CNN — Mystery man named in Xbox hack contest.

A longtime Microsoft opponent has emerged as the mystery backer and mastermind behind a contest that offers $200,000 to anyone who successfully hacks into the software giant's Xbox video game console, a top technology news site reported. Michael Robertson, a former dot-com entrepreneur and now chief executive of U.S. software company Lindows.com, revealed himself as the anonymous donor and contest's creator in an interview on Thursday with CNET News.com. Last July, Robertson anonymously dangled the prize money to any programmers who could successfully hack into the Xbox and adapt it so that it would run on the Linux operating system, an emerging competitor to Microsoft's Windows operating system. Robertson recently extended the deadline as no group has fully mastered the challenge. The hack contest goes beyond a sporty challenge. Linux proponents have long charged that its freely distributed operating system, designed and modified by mainly unaffiliated groups of programming enthusiasts, is an important step for the future development of computing devices. They argue that the market dominance of Windows, which is the operating system on more than 90 percent of all PCs, gives Microsoft and a small number of its business partners unfair and anti-competitive control in the design of the growing number of devices that come equipped with computing capabilities. Robertson's firm Lindows.com is a start-up that aims to promote the use of the Linux open-source operating language in computer systems, a move that would challenge Microsoft's dominant Windows operating system.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2003-01-06 **criminal hacker sentencing Web defacement vandalism government Websites**

NIPC/DHS

January 03, Government Computer News — Hacker of federal Websites could spend a decade in jail.

NASA's inspector general has announced that William Douglas Word of Pelham, Alabama faces up to ten years in prison after pleading guilty to defacing sites of NASA, Defense Department agencies, Interior Department and the International Trade Commission, among others, according to a grand jury indictment handed down in the U.S. District Court for the Northern District of Alabama. Much of the criminal activity occurred in late 1999, the inspector general said. The NASA Office of Inspector General (OIG) investigated the crime together with the Defense Criminal Investigative Service, the Naval Criminal Investigative Service and the FBI. James E. Phillips, U.S. attorney for the Northern District of Alabama, prosecuted the case. Word "was rolled up in a group of hackers that decided to turn themselves in after we got close to confronting them," a NASA official said. "This was the typical hacker case where they were demonstrating their skills." Word is to be sentenced April 24.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2003-01-21 **punishment criminal hacker sentence law**

NewsScan

BANNED FOR LIFE ON THE NET?
Kevin Mitnick, once tagged by the government as "the most-wanted computer criminal in U.S. history," is now ending his probation and will once again be free to start using the Internet. (He intends to set up shop as a computer security consultant.) Legal experts disagree about whether computer criminals can be banned from Internet activity even after they have served sentences and finished their probationary periods. Jennifer S. Granick of the Stanford Center for Internet and Society says no: "Computers are everywhere. The A.T.M. is a computer; the car has a computer; the Palm Pilot is a computer. Without a computer in this day and age, you can't work, you can't communicate, you can't function as people normally do in modern society." Ross Nadel of the U.S. Attorney's office in Northern California says yes, arguing that banning someone from the Internet may be necessary if in a particular case Internet use was integrated and inseparable from the crime that was committed. The courts are similarly divided on the issue, and legal observers don't expect the question to be fully resolved for many years. (New York Times 21 Jan 2003)

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2003-01-24 **virus writer criminal prosecution trial judgement sentence prison**

NewsScan

COMPUTER VIRUS WRITER GETS TWO YEARS IN PRISON
Simon Vallor, from Llandudno, Wales, was sentenced two years in prison by a London magistrate who said that Vallor's actions "cried out for the imposition of a deterrent sentence." The judge brushed aside Vallor's request for leniency, saying: "These offenses were planned and very deliberate. Frankly, when you go to this trouble to make a sophisticated virus, programmed to leave damage this week, next week and the week after, it is absurd to claim you do not intend to do harm. These were by no means isolated offenses and they were committed over a period of time." Vallor wrote the viruses called Admirer, Redesi B, and Gokar, and was judged to be responsible wreaking damage in at least 46 countries. (The Western Mail, Wales, 22 Jan 2003)

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2003-02-07 **computer virus writers held England hacking organization**

NIPC/DHS

February 07, silicon — Two held in computer virus raid.

Two men from northeast England are being interviewed today by the National Hi-Tech Crime Unit (NHTCU). The move follows the execution of search warrants this morning in County Durham, United Kingdom (UK). Two addresses were searched and evidence retrieved relating to computer and drugs offences. The operation was jointly conducted with officers from Durham Constabulary and the United States multi-agency CATCH team (Computer and Technology Crime Hi-Tech Response Team), which is based in Southern California. A simultaneous search warrant was executed at an address in the state of Illinois where additional evidence in the case was seized. The two UK-based men have been identified as members of an international hacking group known as "THr34t-Krew". The NHTCU claims this group is behind a worm called the TK which has infected approximately 18,000 computers worldwide.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2003-02-07 **criminal hacker indictment impersonation fraud theft college university student penetration**

NewsScan

BOSTON COLLEGE STUDENT INDICTED FOR ONLINE VANDALISM
Boston College computer science major Douglas Boudreau has been indicted for hacking into dozens of campus computers and using stolen identities to charge food, books, and services to the accounts of other students. An assistant attorney general said that the scheme "required technical aptitude and an enormous amount of time." Boudreau, who has been suspended from school, is being charged with wiretap violations, hacking and larceny. (Boston Globe 7 Feb 2003)

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2003-02-28 **DVD DeCSS decryption copyright infringement intellectual property piracy lawsuit trial indictment DMCA international jurisdiction**

NewsScan

TEENAGER "DVD-JON" CHARGED AS CRIMINAL FOR BREAKING DVD CODE [11 Jan 2002]
Norwegian prosecutors have lodged a criminal indictment against Jon Lech Johansen, who three years ago when he was 15 years old, wrote and distributed on the Internet software that could break the code protecting DVDs from being copied by individuals who did not pay for them. Johansen says he wrote the software to be able to use his computer to play movies he had purchased. A lawyer for the Electronic Frontier Foundation, which is defending the young man, says the law under which he's being prosecuted was intended to protection financial institutions, rather than to prevent an individual from accessing his own property. The prosecution is charging that in the three months after the young man (now widely known as "DVD-Jon" posted the software on the Internet, it was downloaded by more than 5,000 individuals. (AP/San Jose Mercury News 11 Jan 2002)
http://www.siliconvalley.com/docs/news/svfront/034227.htm

'DVD JON' ACQUITTED BY NORWEGIAN COURT
Jon Lech Johansen (also known as DVD Jon), who was accused of illegally developing and distributing the DeCSS program for breaking the digital copy-protection mechanism on DVDs, has been acquitted in a Norwegian court. The rationale for the judge's decision was that the software could be used for legal purposes as well as illegal ones. "If a person's motive is to solely encourage or solicit illegal actions, then it would be illegal to distribute it" — but the court made the judgment that Johansen was not motivated in that way. (PC World 7 Jan 2003)
http://www.pcworld.com/news/article/0,aid,108462,00.asp

NORWEGIAN DVD-PIRACY CASE TO BE RETRIED
What's going on, property theft or the exercise of intellectual freedom? Norwegian teenage programmer Jon Johansen was acquitted last month of using software he developed to steal DVD movies, but an appellate court in Oslo has ruled that the case needs to be reexamined. The software involved is known as DeCSS. What it does is unscramble manufacturers' security locks on DVDs, much to the distress of the Hollywood movie studios. (Reuters/USA Today 28 Feb 2003)

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2003-03-17 **computer criminal hacking Web defacement prosecution conviction Pakistani**

NIPC/DHS

March 14, Associated Press — Pakistani pleads guilty to hacking U.S. Web sites.

A hacker who breached the computer network at Sandia National Laboratories and posted an anti-Israeli message on the Eglin Air Force Base Web site pleaded guilty to computer and credit card fraud charges, the U.S. attorney's office said Thursday. There were no known political or terrorist overtones to the breaches of four computer networks by 18-year-old Adil Yahya Zakaria Shakour of Los Angeles, said Patty Pontello, a spokeswoman for federal prosecutors. Shakour penetrated the Florida air base's computer server repeatedly in April and May 2002, altering the Web page to denounce the Israeli advancement into Palestine and crediting the defacement to the "Anti India Crew." Shakour is a Pakistani who could face deportation after he completes a prison term of up to 15 years, to be set at his June 12 sentencing. He agreed to make restitution of approximately $100,000 for damage to the computer networks. More than $2,700 in damage was done to the Sandia Labs unclassified Web site in Livermore.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2003-04-29 **U.K. Fluffi Bunni hacker Lynn Htun FBI 9/11 cyberprotest war terrorism SAND institute**

NIPC/DHS

April 29, Associated Press — U.K. Arrests 'Fluffi Bunni' hacker.

Lynn Htun, the man thought to be the leader of a group of hackers known as "Fluffi Bunni," was arrested Tuesday by British authorities. Fluffi Bunni captured the attention of the FBI just days after the September 11 terror attacks, when thousands of commercial Web sites were vandalized with a single break-in that included the message, "Fluffi Bunni Goes Jihad." The FBI characterized the act in a November 2001 report as an anti-American cyberprotest against the war on terrorism. Victims have included the Washington-based SANS Institute, Security Focus, and Attrition.org, a site run by experts who formerly tracked computer break-ins.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2003-05-22 **KINGPIN Ukranian cracker arrested thailand Maksym Vysochansky microsoft adobe back door buyers financial reports credit cards**

NewsScan

'KINGPIN' CRACKER ARRESTED IN THAILAND
Thai officials arrested a Ukrainian man described by a U.S. embassy spokesman as a "kingpin" of international computer crime. Maksym Vysochansky, 25, is accused of selling counterfeit versions of flagship software products by major companies such as Microsoft and Adobe. Vysochansky, who used a number of aliases, is thought to have been involved in fraudulent schemes worth up to $1 billion. "This guy was on the U.S. Secret Service's 10 most wanted list. He's definitely a big shot," said the embassy official. Authorities allege that Vysochansky also built a "back door" into the software he sold that allowed him to hack into buyers' financial and credit card information. "It was a very complicated and sophisticated fraudulent scheme," said the embassy official. Vysochansky likely will be extradited to the U.S. where he'll face charges of copyright violations, trafficking in counterfeit goods and money-laundering. (News24.com 22 May 2003)

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2003-05-22 **incorrect stocks fraud UCLA false identities**

NewsScan

EX-STUDENT FINED MORE THAN $500,000 FOR STOCK FRAUD ON NET
Former UCLA student Refael Shaoulian has been ordered by a federal judge to pay $534,000 in fines for using university computers and false identities to post intentionally incorrect about stocks so that he could profit from the buying and selling sprees he caused. The civil suit was brought by the Securities and Exchange Commission. (APOnline/USA Today 22 May 2003)

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2003-06-12 **Al-Jazeera hacker John William Racine DNS Servers Let Freedom Ring court password Network Solutions**

NIPC/DHS

June 12, The Register — Al-Jazeera hacker charged.

Web designer John William Racine, of Norco, CA, has been charged with breaking into DNS servers and rerouting surfers visiting the Web site of Al-Jazeera to a "Let Freedom Ring" patriotic Web site he created. Racine is also accused of intercepting 300 emails sent to the Arab satellite TV network between March 25 and 27. The 24 year-old is out on bail pending a Monday court appearance when he will face charges of unlawful interception of an electronic communication and wire fraud. Prosecutors allege that Racine obtained a password for Al-Jazeera's Web site by posing as a representative of the station in forged requests faxed to Network Solutions, who handed over the vital information without verifying his identity.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2003-06-13 **Sandia Laboratories hacker sentenced Adil Yahya Zakaria Shakour pakistan israeli palestine web page debounce air base eglin AFB**

NIPC/DHS

June 13, The Mercury News (CA) — Hacker sentenced for breaching Eglin AFB, Sandia lab.

An 18-year-old hacker who breached computers at Sandia National Laboratories and posted an anti-Israeli message on the Eglin Air Force Base Web site was sentenced Thursday to a year and a day in federal prison. Adil Yahya Zakaria Shakour also was ordered to pay $88,253 in restitution, and his computer use was restricted during the three years he will spend under supervised release after his prison term. Shakour, a Pakistani national who lives in Los Angeles, pleaded guilty in March to computer and credit card fraud charges. Shakour penetrated the Florida air base's computer server repeatedly in April and May 2002, altering the Web page to denounce the Israeli advance into Palestine. Damage to the air base computer system was estimated at $75,000, while more than $2,700 in damage was done to the Sandia Laboratories Web site.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2003-07-10 **DOE Department Energy cracker 1-year Londoner UK police unauthorized access computers**

NIPC/DHS

July 10, The Register — London police quiz suspected DOE cracker.

An 18 year-old Londoner suspected of commandeering U.S. Department of Energy (DOE) computers to store illicitly obtained music and video files was arrested and questioned by UK police Wednesday. Officers from the Metropolitan Police's Computer Crimes Unit were asked to investigate unauthorized access to 17 unclassified computers at a U.S. Department of Energy research laboratory in Batavia, IL, during June 2002 after the trail of the attacker led back to the UK. The teenager was released on police bail until mid-August pending further enquiries, including a forensic examination of a PC seized from his home. Police are working on the belief that no sensitive information was seized during the June 2002 attack on the U.S. DOE's network. Officers from the Metropolitan Police's Computer Crimes Unit are been assisted in their enquiries by representatives from the Office of the Inspector General of the U.S. Department of Energy.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2003-07-10 **teenage hacker violate 2000 sites french student DKD web technical skill prison**

NIPC/DHS

July 10, Associated Press — Teenage hacker suspected of violating 2,000 sites.

A French high school student is being investigated on suspicion of breaking into and defacing some 2,000 Web sites police said Thursday. The 17-year-old boy, who went by the pseudonym "DKD," hacked into sites and often replaced their welcome pages with political slogans, said Eric Voulleminot of the Regional Service of Judicial Police in Lille, France. The teenager is accused of attacking sites in France, Britain, Australia and the United States, Voulleminot said. The boy allegedly concentrated on government office and military sites, including that of the U.S. Navy. Suspected of attacks over 14 months, he was arrested June 24 at his parents' home outside of Paris and released under surveillance. Investigators think his goal was showing off technical skill rather than spreading a political message. The suspect faces a maximum sentence of three years in prison and a fine $50,850.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2003-08-29 **worm Blaster network spread FBI teenager vandal**

NewsScan

TEENAGER IDENTIFIED AS 'BLASTER' VANDAL
An 18-year-old man has been identified as one author of the Blaster and LovSan computer worms that have slowed corporate networks throughout the world. The FBI says he will be arrested today. Another individual apparently alerted authorities after seeing the man testing the code. All the Blaster virus variants took advantage of a flaw in that part of Windows software that's used to share data files across computer networks. Infected computers were programmed to automatically launch an attack on a Web site operated by Microsoft, windowsupdate.com, where Microsoft customers will find software patches to ward off attacks by computer vandals. (AP/San Jose Mercury News 29 Aug 2003)

Jeffrey Lee Parson, 18, of Hopkins, MN was arrested iand charged with creating a particularly nasty version of the Blaster virus, Blaster.B, by modifying the code of the original virus.
[NYT http://www.nytimes.com/2003/08/30/technology/30VIRU.html]

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2003-08-29 **MsBlaster creator copycat teenager hacker worm house detention monitored electronically Blaster.B FBI Symantec**

NIPC/DHS

August 29, TechWeb — Accused MSBlaster creator placed under house detention.

A teenager has admitted creating a copycat of the MSBlaster worm, Seattle-based U.S. Attorney John McKay said Friday, August 29. Jeffrey Lee Parson, 18, of Hopkins, MN, was arrested early Friday morning on one count of intentionally causing or attempting to cause damage to a computer. Parson was placed under house detention and is being monitored electronically, said McKay. All computers in his home were seized by the FBI, and he has been denied access to the Internet. Parson is accused of modifying the original MSBlaster worm, and a variant, Blaster.B. The variant shared the same destructive characteristics as its parent, attacking PCs which had not been patched against a vulnerability in the Windows operating system. The worm, which according to security firm Symantec infected more than 500,000 systems worldwide, caused some computers to constantly reboot, snarled enterprise network and Internet traffic, and forced Microsoft to take the unusual step of disabling one of the addresses used to connect with its WindowsUpdate service. Estimates by analysts as to the damage done by MSBlaster and its follow-ups range as high as $1.3 billion.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2003-09-15 **Adrian Lamo hacker NY Times Sacramento employee records phone numbers SSN Social Security Excite Home Corp Yahoo Inc WorldCom**

NIPC/DHS

September 09, Reuters — New York Times hacker surrendered, booked.

Hacker Adrian Lamo, 22, turned himself in to federal authorities in Sacramento, CA, on Tuesday, September 9, to face charges related to breaking into the internal network of The New York Times newspaper. Lamo could face fines and prison time under the Computer Fraud and Abuse Act of 1986, which outlaws unauthorized access to computer networks. Lamo hacked into the New York Times network in February 2002 and accessed employee records, phone numbers, and Social Security numbers of editorial page contributors. In the past Lamo has also discovered holes in corporate networks of Excite@Home Corp., Yahoo Inc., and WorldCom, among others, often through laser printers and other unlikely entry points. Lamo's defense is likely to be the "white-hat hacker" defense, said Mark Rasch, former head of the computer crime unit at the U.S. Department of Justice. White-hat hacker is a term used for people who work to protect computers from attack while "black-hat hackers" are those who attempt to break into them. However, the law focuses on the intent to break into the computer, not the motive, said Rasch.

September 15, CNET News.com — Restrictions lifted on NY Times hacker. A federal judge on Friday, September 12, said Adrian Lamo, the so-called "homeless hacker," could go free on bail with only limited restrictions on his computer use until his next court date in October. U.S. Magistrate Judge Debra Freeman kept Lamo's bail at the earlier amount of $250,000 but lifted the restrictions that barred him from using a computer at all. Instead, Freeman said, the 22-year-old California resident can use a computer for email and to apply for a job or a college program. Lamo is facing two criminal charges. One claims he illegally entered the network of The New York Times, viewed confidential employee records and created a false administrator account; the other says he ran up about $300,000 on the paper's Lexis-Nexis account.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2003-10-17 **evidence trial exculpation defense criminal hacker compromise Trojan horse**

NewsScan; http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/3202116.stm

In England, 19-year-old Aaron Caffrey was charged with crashing computers and networks at the port of Houston, TX after breaking into its systems in September 2001. In October 2003, a jury acquitted the young man because they accepted his defense that criminal hackers had taken control of his computer and used it to attack the port even though he admitted being a member of the criminal hacker organization, admitted breaking into other computer systems, and was unable to provide a shred of evidence that his computer contained any remote-control software or other indications that his computer had been taken over by others.

NEW DEFENSE: THE COMPUTER DID IT
Prosecutors in computer hacking cases are facing a new defense strategy that likely will become more prevalent in the age of hijacked PCs: the computer did it. Defense lawyers in three cases recently tried in the U.K. successfully argued that the crimes committed by their clients were, in fact, the results of "Trojan" programs placed on their computers without their knowledge. While it is relatively easy to trace a hack back to a particular computer, it's much more difficult to prove that the owner of that computer committed the crime. "On the one hand, this is 100% correct that you can not make that jump from computer to keyboard to person," says Bruce Schneier, chief technology officer for Counterpane Internet Security. "On the other hand, this defense could be used to acquit everybody. It makes prosecuting the guilty harder, but that's a good thing." But computer security consultant Dave Morrell says the defense also gives the green light to hackers. "It sets a precedent now in the judicial system where a hacker can just claim somebody took over his computer, the program vanished and he's free and clear." The Trojan defense has not yet been put to the test in the U.S. (Reuters/CNN.com 28 Oct 2003)

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2003-10-21 **airport security test amateur box cutters jets charges criminal trial**

NYT http://www.nytimes.com/2003/10/20/national/20PLAN.html?th

Nathanial T Heatwole, North Carolina college student who turned himself in after placing box cutters and other banned items aboard two Southwest Airlines jets to demonstrate gaps in airport security, was charged with breaching airport security in one count of carrying a dangerous weapon onto an aircraft.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2003-11-25 **hacking criminal hacker indictment prosecution Aventis unauthorized access**

NIPC/DHS

November 20, Associated Press — Kansas City man indicted for computer hacking.

A man from Kansas City, MO, was indicted by a federal grand jury for allegedly hacking into Aventis Pharmaceuticals computers. Thomas S. Millot was charged in a single-count indictment of unauthorized computer intrusion. Millot was employed as an information technology security officer at Aventis' office in Kansas City until October 2000. The federal indictment alleges that Millot gained unauthorized access to the Aventis computer network on nine separate occasions between December 16, 2000, and August 26, 2002, including five times after Millot left the company. The indictment also accuses Millot of deleting an Aventis associate's account from the computer network.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2004-01-09 **hacking database New York Times loss jail**

NewsScan

PRISON TERM FOR NETWORK VANDAL

Under a plea deal with federal prosecutors, a 22-year-old California man agreed to serve a prison term of six months to one year for hacking into a database of the New York Times. The database contained personal information about the newspaper's opinion/editorial page contributors, and the Times calculated that the intrusion caused it more than $5,000 in losses. (Reuters/Los Angeles Times 9 Jan 2004)

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2004-02-14 **virus writer Belgium arrest cyber crime 19-year-old student Gigabyte**

DHS IAIP Daily; http://securityfocus.com/news/8048

February 14, Associated Press — Belgium police arrest female virus-writer.

Belgian police arrested a 19-year-old female technology student who gained international notoriety for creating computer viruses, it was reported Saturday, February 14. The woman, identified only by her nickname "Gigabyte," was charged with computer data sabotage under legislation introduced in 2000 to deal with cyber-crime, the daily La Libre Belgique reported. If convicted, she faces up to three years in prison and fines of up to $127,000. Police reportedly released the woman after 24 hours, confiscated her five computers and shut down her Website. She was arrested Monday in her hometown of Mechelen, 20 miles north of Brussels. "She was preparing to publish new viruses on this site," Inspector Olivier Bogaert of the Belgium police was quoted as telling La Libre Belgique. Her youth and gender helped gain Gigabyte notoriety in the male-dominated world of computer hackers. In a 2002 interview Gigabyte defended her work, saying she herself never spread the viruses she created and published on her Website. "When people make guns, can you blame them when somebody else kills with them?" she was quoted asking. "I only write them. I don't release them."

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2004-03-12 **music movie piracy case Australia extradition intellectual property rights issues**

NewsScan

PIRACY EXTRADITION CASE ADJOURNED

A Sydney, Australia court is to decide if Hew Raymond Griffiths, 41, who is alleged to have headed an international software piracy ring known as "Drink or Die," should be extradited to face charges in the U.S. Griffiths had been indicted by a grand jury in the state of Virginia with one count of criminal copyright infringement and one count of conspiracy to commit criminal copyright infringement. If convicted he faces up to 10 years imprisonment and a $500,000 (US) fine. Griffith's barrister argued the U.S. had not made out a case for extradition, having failed to prove dual criminality — that what his client allegedly did in the U.S. would also have been a crime in Australia. However, the Commonwealth DPP refuted that argument, saying it had made a valid case for extradition in relation to both criminal copyright and conspiracy. (The Australian 12 March 2004, rec'd from John Lamp, Deakin University)

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2004-03-25 **federal wiretapping keylogger California arrest**

NIPC/DHS

March 23, Reuters — Feds charge California man for using keystroke logger.

A California man who prosecutors say planted an electronic bugging device on a computer at an insurance company was indicted on Tuesday, March 23, on federal wiretapping charges. Larry Lee Ropp, a 46-year-old former insurance claims manager, is the first defendant charged with a federal crime for using a "keystroke logger," which tracks the activities on a computer and feeds the information back to its owner, a spokesman for the U.S. Attorney's Office in Los Angeles said. Prosecutors did not say what they believe Ropp hoped to gain by bugging the computer, which was being used by a secretary to executives at the company where he worked, Bristol West Insurance Group. But an affidavit filed with the indictment suggests he intended to supply information to attorneys representing a class of people who were suing the company. Investigators were tipped to Ropp after he was fired from the company and asked another employee to remove the keystroke logger, which records every keystroke made on a computer, from the secretary's machine.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2004-03-26 **Internet blacmailer arrest Holland Netherlands Net-harm credit card fraud**

NIPC/DHS

March 24, The Register — Dutch Internet blackmailer gets ten years.

A 46-year-old Dutch chip programmer who tried to blackmail dairy company Campina has been jailed for 10 years by a Dutch court on blackmail charges and five counts of attempted murder. The blackmailer put agricultural poison in Campina Stracciatella desserts in a bid to extort money. The man forced Campina to open a bank account and asked them to deposit $242,750. Campina was issued with a credit card for the account which the blackmailer intended to use to withdraw the cash. But to avoid breaking cover, he asked Campina to buy a credit card reader and extract the information from the card's magnetic stripe. The output, together with the card's pin code, was sent to him electronically via steganography. Campina received an envelope containing a floppy with a stego program and some instructions. The company then had to encode the credit card data into a picture. The blackmailer downloaded the picture, decoded the information it contained, created his own copy of the card, and finally went to withdraw the cash. To download the online picture, he used the Anonymizer.com service, believing the company's privacy policy would protect him. However, he was caught red-handed last year when he withdrew the money from a cash machine using his copy of the credit card.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2004-05-08 **worm virus malicious code malware Microsoft Windows vulnerability Sasser**

DHS IAIP Daily; http://www.chron.com/cs/CDA/ssistory.mpl/world/2558235

May 08, Reuters — Police: Microsoft helped catch suspect.

German police were led to the home of an 18-year-old man suspected of creating the "Sasser" computer worm after a tip-off from Microsoft, police said Saturday, May 8. Spokesman Frank Federau for Lower Saxony police said that German police were certain they had the man behind one of the Internet's most costly outbreaks of sabotage. "We are absolutely certain that this really is the creator of the Internet worm because Microsoft experts were involved in the inquiry and confirmed our suspicions and because the suspect admitted to it," he said. Microsoft had received anonymous tip-offs about the worm's creator and then contacted the FBI and German police, Federau said. All three worked together to find the suspect. The teenager's computers were confiscated by police but the suspect himself was not in custody, Federau said. Since appearing a week ago, Sasser has wreaked havoc on personal computers running on Microsoft Windows 2000, NT and XP operating systems, but is expected to slow down as computer users download anti-virus patches. The computing underground responsible for hatching worms and viruses has proved a difficult ring to crack for law enforcement and security experts were surprised at the rapid arrest.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2004-05-13 **agobot trojan author gerrman sabotage worm computer malicious**

NewsScan

SUSPECTED AGOBOT TROJAN AUTHOR ARRESTED

A 21-year-old German man has been arrested and charged under the country's computer sabotage law for creating the Agobot Trojan, a malicious computer worm. (This case is unrelated to the Sasser worm, which was also traced to a young German man). Five other Germans have also been charged in connection with the distribution of these Trojan programs. (The Age 13 May 2004) rec'd from John Lamp, Deakin U.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2004-05-18 **phishing email scam fraud**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/articles/A37406−2004May 18.html

May 18, Washington Post — E-mail scammer gets four years.

An Internet scammer who used e-mail and a fraudulent Website to steal hundreds of credit card numbers was sentenced to almost four years in jail Tuesday, May 18, one of the stiffest-ever penalties handed down for online fraud. Houston, TX federal court Judge Vanessa Gilmore sentenced Houston resident Zachary Hill to 46 months in jail for his role in duping consumers into turning over 473 credit card numbers. Hill used a "phishing" scheme to make his e-mail look like it came from America Online, the nation's largest Internet service provider, or PayPal, the online 4 payment subsidiary of auction giant eBay. The message told victims that their accounts had lapsed and that the companies required their credit card numbers and passwords to restart them. Hill prompted recipients to enter their information into Web forms designed to look like pages run by the companies, the Justice Department said. Hill then used the credit card numbers to buy $47,000 in goods and services.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2004-05-27 **Trojan Horse hacker sharing peep data theft Taiwan engineer**

DHS IAIP Daily; http://www.nytimes.com/aponline/international/AP−Taiwan−Chin a−Cyber−Attack.html

May 27, Associated Press — Taiwan engineer accused in cyber attack.

A Taiwanese computer engineer was arrested on charges he had designed a virus-like Trojan horse that Chinese hackers found and used to attack the island's business and government systems, police said Thursday, May 27. Wang Ping-an, 30, designed "Peep," which earlier this year allowed the attackers to steal information and retain control of infected computer systems, police said. "He placed his program on popular hackers' Web sites and encouraged people to download it," said Lin Chieh-lung, an official from an Internet crime investigation task force. "He might have wanted only to show off his skills, but he should be aware what harm this could cause." If convicted on charges of vandalizing public and corporate property, he could face up to five years in prison, police said. Police said they began a probe months ago after noticing hackers had stolen confidential government data. They then discovered "Peep" was responsible for the theft of data from hundreds of Taiwanese schools, companies and government agencies. The attacks were traced back to mainland China, police said. In recent years, fears have grown that China might enforce its claim of sovereignty over self-ruled Taiwan by shutting down the island's heavily computerized society with a cyber-attack instead of a conventional invasion.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2004-07-15 **hacker New York Times Adrian Lamo hacking intrusion LexisNexis**

http://www.informationweek.com/story/showArticle.jhtml?articleID=23901163

Adrian Lamo Cuts Deal With Feds

Adrian Lamo, the "Homeless Hacker," broke into the New York Times' computer network in early 2001. He surrendered to the FBI in September 2003. His modus operandi was to break into large companies networks without authorization and then offer to help them fix their security holes for free. Then he would call news reporters to boast about his exploits. In January 2004 he pled guilty in federal court to charges of computer trespass and claimed that he was remorseful about his actions. In July 2004, he was sentenced "to two years probation, with six months to be served in home detention," and also "to pay $65,000 in restitution."

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2004-07-22 **data theft lawsuit federal spammer spam stealing personal data fraud**

NewsScan

DATA THEFT FEDERAL LAW SUIT

Federal charges have been filed against Scott Levine, the Florida spammer who ran Snipermail.com, for allegedly stealing personal data about "a great number of individuals." He is not accused of using the information for identity fraud. Prosecutors say Levine and other Snipermail employees got into the databases of Acxiom Inc. to take 8.2 gigabytes of consumer files in 2002 and 2003. Levine now stands indicted on 144 counts, including unauthorized access of a protected computer, conspiracy, access device fraud, money laundering and obstruction of justice. (AP/San Jose Mercury News 22 Jul 2004)

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2004-08-05 **network hacking vandalism penetration credit card system Michigan Lowes indictment**

NewsScan

NETWORK VANDALS FACE PRISON SENTENCES

Pleading guilty to attempts to hack into the national computer system of the Lowe's home improvement chain and steal credit card information, three Michigan men now face sentences of up to 25 years in prison. In the indictment, federal prosecutors had said that the men accessed the wireless network of a Lowe's store and used that connection to enter the chain's central computer system and eventually to reach computer systems in Lowe's stores across the country. Lowe's executives say the men did not gain access to the company's national database and that all customers' credit card information are secure. (San Jose Mercury News 5 Aug 2004)

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2004-08-06 **hacking e-commerce fraud theft online Internet Romanian lawsuit grand jury indictment**

NewsScan

INDICTMENT FOR THEFT-BY-HACKING

A Romanian and five U.S. citizens have received grand jury indictments charging them with a $10-million scheme to steal goods by hacking into the online ordering system of computer equipment distributor Ingram Micro Inc. The Romanian, who is now in that country and not in custody, is accused of posing as a customer to place more than 2,000 orders over four years. The man is well known as a computer hacker who uses the pseudonyms "Dr. Mengele" and "Metal." After Ingram Micro blocked shipments to Romania, he allegedly recruited Americans to accept the merchandise. (AP/Los Angelese Times 6 Aug 2004)

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2004-08-12 **Minnesota teenager guilty Blaster worm attack jail sentence Microsoft involvement**

DHS IAIP Daily;
http://www.cnn.com/2004/TECH/internet/08/12/internet.attack. ap/index.html

August 12, Associated Press — Teen pleads guilty in Internet attack.

A Minnesota high school senior pleaded guilty Wednesday, August 11, in federal court to unleashing a variant of the "Blaster" Internet worm, which crippled more than a million computers last summer. Jeffrey Lee Parson, 19 is likely to face 18 months to three years behind bars after pleading guilty to one count of intentionally causing or attempting to cause damage to a protected computer. He also could be ordered to pay millions of dollars in restitution, Assistant U.S. Attorney Annette Hayes said. Parson had pleaded not guilty after his arrest last August, but told U.S. District Judge Marsha Pechman on Wednesday: "I downloaded the original Blaster worm, modified it and sent it back out on the Internet." Different versions of the Blaster worm, also known as the LovSan virus, crippled computer networks worldwide last summer. Parson's variant launched a distributed denial-of-service attack against a Microsoft Corp. Windows update Website as well as personal computers. The government estimates Parson's version alone inundated more than 48,000 computers. Parson was charged in Seattle, WA, last August because Microsoft is based in suburban Redmond, WA.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2004-09-20 **Sasser worm virus creator writer employment security company Germany Securepoint**

NewsScan

SASSER CREATOR HIRED BY SECURITY FIRM

A German teenager accused of creating the Sasser worm that infected millions of computers around the world is being trained as a security software programmer, the company that hired him said on Friday. Eighteen-year-old Sven Jaschan has been taken on by the Securepoint computer firm based in Lüneburg, in northern Germany, and is being trained to make firewalls to stop suspect files from entering computer systems. "He has a certain know-how in this field," a company spokesman said. Jaschan has been charged with computer sabotage, data manipulation and disruption of public systems for allegedly hatching the Sasser worm. (The Age 20 Sep 2004) Rec'd from John Lamp, Deakin U.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2004-11-08 **Nigerian scam Australia Marinellis sentencing crime 4-1-9 advance-fee fraud prosecution trial**

NewsScan; http://australianit.news.com.au/articles/0

NIGERIAN SCAMMER JAILED

The Australian mastermind of a global Internet scam was today sentenced to at least four years behind bars. Nick Marinellis pleaded guilty in the New South Wales District Court to 10 counts of fraud and one count of perverting the course of justice over the so-called Nigerian or West African scam. The ruse fleeced victims of $5 million. Judge Barry Mahoney sentenced Marinellis to five years and three months jail with a nonparole period of four years and four months. (The Australian 8 Nov 2004)

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2004-12-21 **judgement spam AOL New York CAN-SPAM insider crime**

NewsScan ;

FORMER AOL EMPLOYEE FACES JAIL FOR HELPING SPAMMERS

Virginia software engineer Jason Smathers, formerly employed by America Online, has pleaded guilty to stealing 92 million screen names and e-mail addresses and then selling them to spammers. The spammers in turn used them to generate seven billion unsolicited e-mail messages. The 24-year-old Smathers now faces from 18 months to two years in prison and mandatory restitution of between $200,000 and $400,000, the estimated amount of what AOL had to spend as a result of the e-mails. Authorities said he used another employee's access code to steal the list of AOL customers in 2003 from its headquarters in Dulles, Va. He was promptly fired by the company. (AP/San Jose Mercury News 7 Feb 2005)
http://www.siliconvalley.com/mld/siliconvalley/10827690.htm

JUDGE REJECTS GUILTY PLEA IN AOL SPAM CASE

A federal judge in New York has refused to accept a guilty plea from a former AOL software engineer accused of stealing 92 million subscriber e-mail addresses and selling them to spammers. Judge Alvin Hellerstein said he was not convinced that Jason Smathers had actually committed a crime under the new "CAN-SPAM" legislation passed by Congress this fall. The technicality hinges on whether Smathers deceived anyone -- a requirement of the CAN-SPAM law. "Everybody hates spammers, there's no question about that," said Hellerstein, who told federal prosecutor David Siegal: "I'm not prepared to go ahead, Mr. Siegal. I need to be independently satisfied that a crime has been created." Prosecutors allege that Smathers sold the list to Las Vegas resident Sean Dunaway, who then resold it to spammers, netting Smathers more than $100,000 from the deal. (Wall Street Journal 21 Dec 2004)
http://online.wsj.com/article/0,,SB110365400892306111,00.html (subscription required)

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2005-01-04 **spam spyware Wallace FTC**

NewsScan;
http://www.cnn.com/2005/TECH/internet/01/04/spyware.ap/index.html

'SPAM KING' AGREES TO CEASE-FIRE

Under an agreement with the Federal Trade Commission, a man dubbed the "Spam King" will stop distributing spyware until a federal lawsuit is resolved. In addition, Sanford Wallace has agreed to send online ads only to people who visit the Web sites of companies -- SmartBot.net of Richboro, Pennsylvania and Seismic Entertainment Productions of Rochester, New York. "The commission does believe this is great relief for consumers until the matter is ultimately resolved in the courts," says FTC lawyer Laura Sullivan. "This provides wonderful protection for consumers in the interim." Wallace's most recent exploits included sending pop-up messages to Microsoft Word users offering to sell software that would block the pop-ups (but according to the government, didn't work). In the 1990s he earned the nickname "Spam King" after spewing out as many as 30 million junk e-mails per day to consumers. (AP/CNN.com 4 Jan 2005)

[MK notes: This creep is widely known as "Spamford" Wallace. He started his direputable career as a junk faxer in the 1980s and went on from there. See for example "Sanford Wallace: Back to the Fax?" in WIRED (1998) < http://wired-vig.wired.com/news/culture/0,1284,9847,00.html >.]

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2005-02-14 **vandal jail prison WebTV hacking 911 guilty plea court trial fraud**

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/10902507.htm

NETWORK VANDAL FACES 10 YEARS IN PRISON

David Jeansonne, a 44-year-old Louisiana man, faces up to ten years in prison for hacking into WebTV. Jeansonne has pleaded guilty to having sent e-mail messages to about 20 subscribers in 2002, advising the recipients that they could change the display colors on their screens -- but in fact secretly resetting their dial-in telephone number so that they called 911 instead of the local modem telephone number when they tried to access WebTV. (San Jose Mercury News 14 Feb 2005)

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2005-02-17 **Arizona student sentences copyright violations guilty movies music prison probation community service property felony**

EDUPAGE; http://kvoa.com/Global/story.asp?S=2934754

ARIZONA STUDENT SENTENCED FOR COPYRIGHT VIOLATIONS

A student at the University of Arizona who pleaded guilty to unauthorized possession of copyrighted movies and music has been sentenced to three months in prison, three years' probation, and 200 hours of community service. The 18-year-old student, Parvin Dhaliwal, was also fined $5,400. Andrew Thomas, attorney for Maricopa County, noted that illegal possession of intellectual property is a felony. Thomas said some of the movies Dhaliwal had copies of were, at the time, only being shown in theaters. Dhaliwal was also ordered to take a copyright course at the University of Arizona and not to use file-sharing programs.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2005-05-06 **UK Britain Drink-or-Die criminal hacker cracker group software piracy conspiracy fraud charge**

EDUPAGE; http://news.zdnet.co.uk/software/0,39020381,39197662,00.htm

DRINK-OR-DIE CONSPIRATORS HEADED TO PRISON

A British court has sentenced three men to prison for their involvement in the so-called Drink-or-Die group, which cracked the copy protections on software and then distributed it over the Internet. The three men received sentences ranging from 18 to 30 months, while a fourth man received a suspended sentence; all were charged with conspiracy to defraud. Prosecutors alleged that the piracy ring cost software companies millions of dollars in lost sales, and the verdicts were seen by some as a strong, clear message to software pirates. Others were critical of the government's case, however, saying that the men should have been charged with copyright violations rather than conspiracy. Security expert Peter Sommer, who served as a witness for the defense, said the government has no way of proving how much the ring cost software makers. He said the conspiracy case cost the government significantly more money and took much longer to try than a copyright case. A spokesperson from the British Crown Prosecution Service said the charges were appropriate, commenting that the authorities do "not determine cases on the basis of how much they will cost to prosecute." ZDNet, 6 May 2005

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2005-06-08 **criminal hacker US military targets Pentagon Washington DC UK British national extradition**

EDUPAGE; http://www.theregister.com/2005/06/08/brit_hack_suspect_arrest/

PENTAGON HACKER ARRESTED, FACES EXTRADITION

A British man suspected of hacking into more than 50 computer systems operated by the U.S. government has been arrested in London and faces extradition to the United States. Gary McKinnon is accused of exploiting security weaknesses in computer systems at the Pentagon, NASA, and a number of military sites between February 2001 and March 2002. In one attack, McKinnon is said to have blocked access to 2,000 individual military computers in the Washington area. U.S. authorities said they spent $1 million fixing the damage from the attacks, and a grand jury indicted McKinnon in 2002. McKinnon has been released on bail, and Karen Todner, McKinnon's attorney, said he would "vigorously" fight the extradition. "As a British national," she said, "he should be tried here in our courts by a British jury." The Register, 8 June 2005

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2005-06-13 **data theft computer program personal information disclosure Social Security Numbers University of Texas Austin**

EDUPAGE; http://chronicle.com/prm/daily/2005/06/2005061301t.htm

FORMER STUDENT CONVICTED OF STEALING DATA

A former student of The University of Texas at Austin has been found guilty of writing a computer program that stole names and Social Security numbers from about 37,000 students, faculty, and others associated with the university. The jury found Christopher Andrews Phillips not guilty, however, of intending to profit from the data he stole. Phillips, who is now a senior at the University of Houston, said he wrote the program as part of his computer training and never had any intention of using the information. The theft took place in 2002 and 2003, when Phillips's program made more than 600,000 inquiries to a UT database, trying to match names with Social Security numbers. UT officials detected the activity and traced it to Phillips, whose computer was seized with the program he wrote and the data it had harvested. Phillips faces up to six years in prison; had he been convicted of the other charges, he would have faced close to 30 years. Chronicle of Higher Education, 13 June 2005 (sub. req'd)

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2005-08-15 **e-mail marketer data theft conviction fraud Acxiom Corp**

EDUPAGE; http://online.wsj.com/article/0,,SB112406416615412935,00.html

SPAMMER SCOTT LEVINE CONVICTED OF STEALING 1.6 BILLION NAMES

A jury in Arkansas has convicted Scott Levine of stealing 1.6 billion computer records from Little Rock-based data vendor Acxiom Corp. The records included names, addresses, phone numbers, and other personal information that Levine's company, Snipermail.com, sought to use in direct e-mail marketing campaigns. In the case, the government presented evidence that Levine had used illegally obtained passwords of about 300 legitimate Acxiom customers to fraudulently access the records. Levine was convicted of 120 counts of unauthorized access to a computer, two counts of fraud for cracking passwords, and one count of obstruction of justice for trying to destroy evidence stored on Snipermail computers. Levine will be sentenced in January. Acxiom said that since the intrusion, it has improved security procedures for protecting data, including strengthening encryption systems and the company's ability to detect when unauthorized access takes place. Wall Street Journal, 15 August 2005 (sub. req'd)

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2005-08-27 **worm malicious code two arrests investigation Microsoft operating system OS FBI cybercrime**

EDUPAGE; http://www.siliconvalley.com/mld/siliconvalley/12488476.htm

TWO MEN NABBED IN WORM INVESTIGATION

Two men have been arrested in connection with an investigation into the Zotob worm, which surfaced in August and took advantage of a flaw in the Microsoft operating system. The worm affected computers at organizations including The New York Times, ABC, CNN, the Associated Press, and the Immigration and Customs Enforcement bureau. According to Louis M. Riegel, assistant director for cyber crimes at the FBI, Farid Essebar was arrested in Morocco, and Atilla Ekici was arrested in Turkey. Riegel said that Ekici had paid Essebar to write the worm, and the pair are also suspected of writing the Mytob worm, which was released in February. Zotob is able to infect computers even if users do not open any applications. As a result, some users are struck by the worm without knowing about it. Still, experts believe the damage from the worm has been relatively minor, given that the operating system most affected, Windows 2000, is more than five years old and that most organizations quickly patched the flaw that Zotob exploits. San Jose Mercury News, 27 August 2005

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2005-08-29 **international arrest US computer worm probe Morocco Turkey FBI**

DHS IAIP Daily; http://cnn.netscape.cnn.com/ns/news/story.jsp?flok=FF−APO −PL S&idq=/ff/story/0001/20050826/1558760757.htm&related=off&ewp =ewp_news_computer_virus

TWO ARRESTED IN U.S. COMPUTER WORM PROBE

Authorities in Morocco and Turkey have arrested two people believed responsible for a computer worm that infected networks at U.S. companies and government agencies earlier this month. Farid Essebar, 18, was arrested in Morocco, while Atilla Ekici, 21, was arrested in Turkey on Thursday, August 25, Louis M. Riegel, the FBI's assistant director for cyber crimes, said Friday. They will be prosecuted in those countries, Riegel said. Essebar wrote the code that attacked computers that run Miscrosoft operating systems and Ekici paid him for it, Riegel said. It's unclear they ever met, "but they certainly knew each other via the Internet," he said. Riegel said he does not know how much money changed hands. Miscrosoft and FBI officials also declined to estimate the monetary damage done by the Zotob worm and its variations. The worm disrupted computer operations in mid-August at several large news organizations, including The Associated Press, ABC, CNN, and The New York Times; such companies as heavy-equipment maker Caterpillar Inc.; and the federal Immigration and Customs Enforcement bureau. Official FBI statement: http://www.fbi.gov/pressrel/pressrel05/zotob_release082605.htm

---

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2005-09-07 **hacking sentence University of Texas conviction**

EDUPAGE; http://www.chron.com/cs/CDA/ssistory.mpl/metropolitan/3342919

UT HACKER GETS FINE, PROBATION

A former student at the University of Texas at Austin has been sentenced for hacking into the university computer system, a charge on which a federal jury convicted him in June. Christopher Andrew Phillips has been ordered to pay $170,000 in restitution for his crimes and to serve five years of probation. Phillips was found guilty of damaging the university's computers and of illegally possessing close to 40,000 Social Security numbers. The jury acquitted him of intending to profit from the personal information he obtained. In addition to the fine and probation, Phillips is forbidden from using the Internet for five years except for school or for work and only under the supervision of his parole officer. In a statement, U.S. Attorney Johnny Sutton said, "[Phillips] found out the hard way that breaking into someone else's computer is not a joke." Houston Chronicle, 7 September 2005

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2005-10-25 **file sharing peer-to-peer P2P Sweden music movie piracy conviction intellectual property rights violation copyright infringement**

EDUPAGE; http://news.bbc.co.uk/1/hi/technology/4376470.stm

FILE SHARER CONVICTED IN SWEDEN

For the first time, a file sharer has been convicted in Sweden, a country long seen as soft on digital piracy. Indeed, the country only this past July passed a law against downloading copyrighted material. The conviction stems from a case prior to passage of the downloading law, when Andreas Bawer uploaded a movie to the Internet. Although the court found Bawer not guilty of downloading the film because the new law had not been put into place, it found him guilty of violating copyright law for distributing the film online. In its ruling, the court said, "Illegal material can in this way be spread quickly and reach many people, which can lead to heavy economic losses for the copyright owners." Because Bawer did not try to profit from his actions, the court decided to fine him rather than sentence him to prison. Bawer's attorney said his client had not yet decided whether he would appeal the verdict. Henrik Ponten of the Swedish Anti-piracy Agency praised the ruling, saying that Sweden has "taken the first step toward a functioning copyright law." BBC, 25 October 2005

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2006-01-16 **criminal hacker penetration military base arrest**

RISKS 24 15

SPANISH CRIMINAL HACKER SUSPECT ARRESTED

An 18-year-old suspected Spanish hacker who allegedly breached the top-secret computer security of a U.S. Navy base in San Diego has been arrested in his home town of Malaga, Spain, according to the Spanish Civil Guard. He reportedly "seriously compromised the correct operations and security of a maintenance dry dock for nuclear submarines.

[Abstract by Peter G. Neumann]

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2006-01-27 **legal sentence Microsoft source code theft Connecticut man**

DHS IAIP Daily; http://news.yahoo.com/s/ap/20060128/ap_on_hi_te/microsoft_source_code;_ylt=Am2Q37WFib1DhYnAQZ9D.JEjtBAF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−− 23

"ILLWILL" SENTENCED FOR STEALING MICROSOFT CODE.

A Connecticut man known on the Internet as "illwill" was sentenced to two years in prison Friday, January 27, for stealing the source code to Microsoft Corp.'s Windows operating software, among the company's most prized products. William Genovese Jr., 29 of Meriden, CT, was sentenced by U.S. District Judge William H. Pauley, who called Genovese "a predator who has morphed through various phases of criminal activity in the last few years." Genovese pleaded guilty in August to charges related to the sale and attempted sale of the source code for Microsoft's Windows 2000 and Windows NT 4.0. The code had previously been obtained by other people and unlawfully distributed over the Internet, prosecutors said. Source code is the blueprint in which software developers write computer programs. With a software program's source code, someone can replicate the program. Industry experts expressed concern that hackers reviewing the Microsoft software code could discover new ways to attack computers running some versions of Windows. Prosecutors said in an indictment in February 2004 that Genovese posted a message on his Website offering the code for sale on the same day that Microsoft learned significant portions of its source code were stolen.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2006-02-07 **Spanish criminal hacker sentence distributed denial-of-service DDoS attack IRC**

DHS IAIP Daily; http://itvibe.com/news/3912 23

SPANISH HACKER SENTENCED TO TWO YEARS IN JAIL AND FINE OF $1.6 MILLION.

Experts at Sophos have welcomed the news that a hacker who stopped over a third of Spanish computer users from using the Internet has been sentenced to two years in jail. Santiago Garrido, 26, used a computer worm to launch Distributed Denial-of-Service (DDoS) attacks after he was expelled from the popular "Hispano" IRC chat room for not following rules. The attacks disrupted an estimated three million users of the Wanadoo, ONO, Lleida Net and other Internet service providers, amounting to a third of all of Spain's Internet users at the time of the offence in 2003. Garrido, who went by the aliases "Ronnie" and "Mike25", was sentenced at a court in La Coruña and also faces a $1.6 million fine.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2006-02-14 **UK computer hacker penetration US govt computer fraud penetration fight extradition**

DHS IAIP Daily; http://today.reuters.com/news/newsArticle.aspx?type=domesticNews&storyID=2006−02−14T145400Z_01_L14737329_RTRUKOC_0_US−BRITAIN−USA−HACKER.xml&archived=False 36. February 14, Tech Web — Microsoft: IE zero−da 23

BRITISH COMPUTER HACKER FIGHTS EXTRADITION TO THE U.S.

A British computer enthusiast accused by the U.S. government of the world's "biggest military hack of all time" began his court fight against extradition to the United States on Tuesday, February 14. Gary Mckinnon was arrested in June last year on charges of computer fraud issued by U.S. prosecutors claiming he illegally accessed 97 U.S. government computers -- including Pentagon, U.S. Army, U.S. Navy and NASA systems. Prosecutors say he hacked into sensitive equipment over a one-year period from February 2002 and caused $700,000 worth of damage, after crippling U.S. defense systems in the wake of the September 11 attacks. If found guilty, Mckinnon could face up to $1.75 million in fines and 60 years in jail.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2006-02-22 **spammer sentence personal data theft Acxiom data broker**

EDUPAGE; http://news.zdnet.com/2100-1009_22-6042290.html 23

SPAMMER SENTENCED FOR STEALING PERSONAL DATA

A federal judge in Arkansas has sentenced a well-known spammer to eight years in prison for illegally accessing and downloading more than one billion records from data broker Acxiom. Prosecutors alleged that in 2003, Scott Levine stole a password file from Acxiom, which claims to have the world's largest database of consumer information. Levine then used those passwords to download other sensitive information. Levine operated Snipermail.com, an e-mail operation that was repeatedly accused of sending spam and claiming that it was doing so with "opt in" authorization from recipients. Although there was no evidence that Levine used the information he stole from Acxiom for identity theft, a federal jury found Levine guilty in August of 2005 of unauthorized access to a computer connected to the Internet. Levine was also fined $12,300 and may be forced to pay restitution.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2006-03-22 **online attack Internet hacking arrest Melbourne Australia IRC**

DHS IAIP Daily; 23
http://www.heraldsun.news.com.au/common/story_page/0,5478,18
562814%5E661,00.html

MAN ARRESTED OVER ONLINE ATTACKS.

A man charged with over a series of high-profile international Internet hacking attacks was arrested in Melbourne, Australia, early Wednesday, March 22, after a joint state and federal investigation into the sophisticated attacks on Internet relay chat servers in Australia in 2005. The Belgian Federal Computer Crime unit tipped Australian authorities off to the attacks, which used botnets.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2006-04-20 **University of Southern California USC hacking charges filed network administrator cybercrime**

EDUPAGE; http://news.zdnet.com/2100-1009_22-6063470.html 23

CHARGES FILED IN USC HACK

Charges have been filed against a network administrator in San Diego related to a June 2005 incident in which a server at the University of Southern California (USC) was compromised. Federal authorities have charged Eric McCarty with gaining unauthorized entry to a USC computer system for applications that contained information on more than 275,000 applicants dating back to 1997. Michael Zweiback, an assistant U.S. attorney in the cybercrimes and intellectual property unit, said, "Universities are becoming bigger and bigger targets to the hacker community," adding that "hackers always want to see if they can beat the technical people on the other side." If found guilty of the alleged hacking, McCarty could be sentenced to 10 years in federal prison.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2006-05-02 **Vietnamese distributed denial-of-service DDoS hacking suspect arrest www.vietco.com Trojan Horse Microsoft Internet Explorer IE vulnerability flaw exploit**

DHS IAIP Daily; 23
http://www.sophos.com/pressoffice/news/articles/2006/05/viet ddos.html

VIETNAMESE DISTRIBUTED DENIAL-OF-SERVICE HACKING SUSPECT ARRESTED.

Sophos has announced news that a man has been arrested in Vietnam for launching a distributed denial-of-service attack against a commercial Website. The attack on Vietco's Website caused huge losses to the company. Nguyen Thanh Cong is suspected of beginning an attack on the Vietnamese e-commerce site, www.vietco.com, in March 2006. The Website, which has 67,000 regular members, auctions cell phones and other consumer electronics products. Cong faces charges for creating a Trojan horse that exploited a flaw in Microsoft's Internet Explorer. The Trojan horse, which is said to have been planted on a pornographic Website, turned unpatched computers into zombie PCs which were then ordered to repeatedly hit the Vietco site -- overwhelming its servers.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2006-05-03 **Russian student conviction malware exchange Website**

DHS IAIP Daily; 23
http://www.sophos.com/pressoffice/news/articles/2006/05/russianvx.html

RUSSIAN STUDENT CONVICTED FOR RUNNING VIRUS DISTRIBUTION WEBSITES.

Sophos has reported the sentencing of a man who not only created his own malware, but ran two Websites distributing over 4000 different computer viruses. Sergey Kazachkov, a Russian science university student from Voronezh, was found guilty of making available thousands of pieces of malware via two virus exchange Websites. He was also said to have created and spread his own malicious software. Kazachkov has been given a two year suspended sentence, and will have to abide by conditions laid down by the court during a one year probation period.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2006-05-05 **California man bot attack guilty plea zombie computer network**

DHS IAIP Daily; 23
http://news.com.com/California+man+pleads+guilty+to+bot+atta ck/2100−7348_3−6069238.html?tag=alert

CALIFORNIA MAN PLEADS GUILTY TO BOT ATTACK.

Christopher Maxwell, a Vacaville, CA, resident, was accused of intentionally damaging a computer he was not authorized to access and using it to commit fraud. He made the guilty plea on Thursday, May 4, in federal district court in Seattle. Back in mid-2004, Maxwell and a group of co-conspirators created a network of bots using more than 13,000 zombies. Maxwell used the bot network to install adware on compromised computers, reaping commissions of approximately $100,000 for himself and his co-conspirators, according to the initial complaint.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2006-05-05 **Christopher Maxwell computer crime botnet zombie computer networks guilty plea**

EDUPAGE; http://news.zdnet.com/2100-1009_22-6069238.html 23

GUILTY PLEA IN COMPUTER ATTACK

Christopher Maxwell has pleaded guilty to charges that he and a group of conspirators used a network of zombie computers to install adware on unsuspecting users' computer. Maxwell is said to have earned about $100,000 in commissions from the adware. The scheme involved using a bot network of 13,000 zombie computers, which Maxwell controlled using powerful computers at California State University at Northridge, the University of Michigan, and the University of California at Los Angeles. Maxwell's bot network swamped the computers at Northwest Hospital in Seattle, causing disruptions to communications among hospital staff. Costs for the hospital to address the issue were estimated to be $150,000. Maxwell will be sentenced August 4.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2006-05-09 **Jeanson James Ancheta Botmaster Underground guilty plea**

DHS IAIP Daily; 23
http://news.yahoo.com/s/nm/20060509/tc_nm/crime_botmaster_dc ;_ylt=AuAzPlcqryDNlBx5rov1ohkjtBAF;_ylu=X3oDMTA5aHJvMDdwBHNl YwN5bmNhdA−−

BOTMASTER GETS NEARLY FIVE YEARS IN PRISON.

Jeanson James Ancheta, a well-known member of the "Botmaster Underground" who pleaded guilty in January to federal charges of conspiracy, fraud and damaging U.S. government computers, was sentenced Monday, May 8, to nearly five years in prison for spreading computer viruses. Prosecutors say 11 the case was unique because Ancheta was accused of profiting from his attacks by selling access to his "bot nets" to other hackers and planting adware into infected computers.

Category 1A3 *Biographical notes on individual criminals (including arrests, trials)*

2006-06-04 **spammer civil lawsuit settlement asset forfeiture student penalties**

RISKS 24

TEXAS MEGA-SPAMMER SETTLES WITH STATE, MICROSOFT

The Associated Press reported, "One of the world's most notorious spammers has settled lawsuits with the state of Texas and Microsoft Corp. that cost him at least $1 million, took away most of his assets and forced him to stop sending the nuisance e-mails. Ryan Pitylak, 24, who graduated from the University of Texas[in May 2006], has admitted sending 25 million e-mails every day at the height of his spamming operation in 2004…. Pitylak, who plans to help Internet companies fight spam, said he would sell his $430,000 house and a 2005 BMW to help pay his fines and legal bills."

1A4 Criminal hacker publications

Category 1A4 *Criminal hacker publications*

2000-01-06 **criminal hacker phone phreak physical security social engineering lying cheating misrepresentation forgery trickery deceit**

HackCanada http://www.hackcanada.com/ice3/misc/telaccess.txt

A criminal hacker calling itself "~Wizbone '99" published a new edition in January 2000 of an unfortunately excellent guide to social engineering that, I regret to say, bears reading by security specialists. "Gaining physical access to Server and Telecom rooms (v2.1)" < http://www.hackcanada.com/ice3/misc/telaccess.txt > summarizes the ways criminals can fool security and other personnel and gain access to restricted areas in the workplace. The writer recommends forging documents, having work shirts embroidered with the name of a fictitious firm, and other ways of lying convincingly. One of the obviously missing elements in the document is any sign that the author realizes that what (s)he is doing is wrong. The well-known principles of physical security are reinforced by the experience of this criminal: choose and train your security guards well, keep employees aware of their responsibility to report suspicious activity, communicate among different sectors of the organization, and accompany visitors and contractors at all times in secure areas.

Category 1A4 *Criminal hacker publications*

2000-02-18 **criminal hackers psychology script kiddies motivations culture denial-of-service attacks**

WASHINGTON POST

Libby Copeland published an interesting overview of the culture clash between older criminal hackers who espouse the hacker ethic and the script kiddies they think are ruining hacking's image. She interviews some hackers who claim never to actually use the techniques they invent — it's all an intellectual game, they say. One hacker is quoted as saying, "The people who are developing attacks and posting them, I don't consider them evil. . . . They're really doing quality control."

Category 1A4 *Criminal hacker publications*

2005-07-11 **Phrack magazine publication ending computer security mischief information exchange**

EDUPAGE; http://software.silicon.com/security/0,39024655,39150241,00.htm

SECURITY COMMUNITY BEMOANS LOSS OF HACKER MAGAZINE

Long-time hacker magazine "Phrack" will stop being published this year after nearly 20 years as an information exchange for computer mischief, and at least some computer security experts believe computer users will be less safe after it is gone. Hackers have routinely undermined their own efforts by revealing their successes at compromising systems or causing other damage. Pete Simpson of computer security firm Clearswift noted that although the magazine makes computer exploits available to those who would use them to cause harm, by definition it also makes them available to the community of users working to protect computers from hackers. Simon Perry, vice president of security strategy at Computer Associates, said that security experts will still be able to find information about new exploits but that "Phrack was great as a one-stop shop" for such information. Simpson commented that after Phrack shuts down, younger hackers are likely to develop new vehicles to tell the world about their triumphs, once again leveling the playing field. Silicon.com, 11 July 2005

1A5 Criminal hacker organizations

Category 1A5 *Criminal hacker organizations*

2003-09-02 **spammers internet e-mailers Bilk Club message board Damon Decrescenzo junk**

NewsScan

CALLING ALL SPAMMERS
Who would ever have thought? It turns out that spammers need online community, too, and they can find it at The Bulk Club — a support group for junk e-mailers. The overnight success of The Bulk Club (159 members signed up since its launch six months ago) belies the stereotype of the spammer as lone sociopath, lurking in the Internet's shadows. In fact, the club's rapidly swelling membership signals a move on the part of spammers to circle the wagons in an effort to protect and legitimize the embattled bulk e-mail industry. And what do members get for their $20 per month fee? Access to a variety of how-to articles (such as "How to Spoof"), spamming software, a members' message board and "300,000 FRESH e-mails/week." Also, thanks to a Web site security flaw uncovered last week, they received a bit of unwanted publicity — the entire Bulk Club membership roster was revealed, including some of the biggest names in bulk e-mailing: Damon Decrescenzo, a Florida junk e-mail who's been sued by both Microsoft and Amazon; Internet porn king Seth Warshavsky; and John Milton — an alias used by former neo-Nazi Davis Wolfgang Hawke — and Jon Thau, both of whom are responsible for many of those penis enlargement ads you might have received. (Wired.com 2 Sep 2003)

Category 1A5 *Criminal hacker organizations*

2004-05-06 **IRC viruses worms malware child pornography warez copyright infringement piracy**

http://www.nytimes.com/2004/05/06/technology/circuits/06chat.html?th=&page wanted=print&position=

Seth Shiesel of the New York Times published a good review of the sociology of the IRC. He characterized the culture of the IRC in largely uncomplimentary terms. Some of the criminal activities supported by some IRC users include

* software and movie piracy
* child pornography
* virus exchange
* distributed denial of service attacks.

Law enforcement officials are very interested in the IRC but it's extremely difficult to track users, especially criminals, because of the ease with which users can switch channels.

Category 1A5 *Criminal hacker organizations*

2004-10-07 **cybersecurity conference globalization privacy organized crime federal research investment lacking Eugene Spafford CERIAS**

DHS IAIP Daily; http://searchsecurity.techtarget.com/originalContent/0,28914 2,sid14_gci1012829,00.html

October 07, SearchSecurity — Globalization, privacy and organized crime to drive security.

Organized crime is pouring massive amounts of resources into phishing, online extortion and other malicious activities by exploiting a U.S. weakness -- the lack of federal research and law enforcement investment in cybercrime, warned one of the nation's most influential infosecurity leaders Wednesday, October 6. "We are beginning to face well-financed, well-organized groups of professional criminals, and as far as I can tell, there's been little federal funding invested in this at all," Eugene Spafford said at the Information Security Decisions conference in Chicago. Spafford, the executive director of the Center for Education and Research in Information Assurance and Security (CERIAS), said less than $50 million in federal funding currently is being invested in basic cybersecurity research. Attacks will come in the form of extortion, protection rackets and threats to business availability via denial-of-service attacks. Spafford said nations around the world are subsidizing hacker training programs in an effort to obtain confidential information that can benefit their businesses and citizens. Some examples include China, India, Brazil, North Korea, South Korea and Cuba.

Category 1A5 Criminal hacker organizations

2006-02-01 **computer hacking charge UK billionaire Scotland Yard investigation trial**

DHS IAIP Daily; http://www.theregister.co.uk/2006/02/01/tycoon_hacking_charge/ 23

UK TYCOON CHARGED WITH COMPUTER HACKING.

Matthew Mellon, the heir to a $11.7 billion oil and banking fortune, has been charged with a computer hacking offense over his alleged involvement in a snooping, bugging and blackmail ring in the United Kingdom. Mellon will appear alongside 17 other defendants in court later this month. Members of the group were arrested after a year long investigation by the Met Police into a detective agency run by a former policeman. Scotland Yard's probe unearthed evidence that suspects also broke into the National Health Service computers and stole medical files in order to facilitate blackmail. Investigators said members of the group donned false uniforms in order to gain access to premises where they left bugs. Mellon, chief designer at upmarket shoe firm Harry's, a company he created five years ago, is charged with conspiracy to cause unauthorized modification of computers. Another wealthy entrepreneur, Adrian Kirby, who made an estimated fortune of $115 million chiefly by running a waste disposal unit business, faces phone tapping, computer hacking and conspiracy to pervert the course of justice charges. Scott Gelsthorpe of Kettering, Northamptonshire, a former policeman in Essex, faces 15 charges. All 18 suspects face an appearance in court on Thursday, February 23.

Category 1A5 Criminal hacker organizations

2006-02-03 **WMF exploit code sale Russian hacker criminals Kaspersky Labs**

DHS IAIP Daily; http://www.newsfactor.com/news/WMF−Exploits−Sold−by−Russian− Hackers/story.xhtml?story_id=01200162XEHO 23

WMF EXPLOITS SOLD BY RUSSIAN HACKERS.

According to Moscow-based antivirus firm Kaspersky Labs, Russian hackers propagated the Windows Meta File (WMF) exploit that wreaked so much havoc on computers in December 2005 by selling it to Internet criminals for $4,000. The exploit took advantage of a bug in Windows' rendering of WMF images, putting PC users at risk when they visited Websites that had been infected by the exploit. In a posting on its Website, Kaspersky said that over a thousand instances of malicious code based on the exploit were detected in a week. But because of the Christmas holiday season, less damage occurred than might have happened otherwise, Kaspersky said. According to Kaspersky researchers, the person who discovered the exploit in early December began selling it by the middle of that month to anyone prepared to pay $4,000. But the antivirus community only identified the exploit on December 27.

Category 1A5 Criminal hacker organizations

2006-03-30 **criminal gang computer criminal hacker recruiting SANS extortion fraud denial-of-service extortion**

DHS IAIP Daily; http://software.silicon.com/security/0,39024655,39157704,00.htm 23

CRIMINAL GANGS RECRUITING HACKERS.

Speaking at the e-Crime Congress in London Thursday, March 30, Alan Paller, director of research for SANS, said weak digital security in businesses is helping hackers fund criminal activity. Paller said he had recently seen cases of criminal gangs recruiting hackers by threatening to harm their families unless they agree to carry out denial-of-service extortion attacks. Paller said the FBI is currently receiving more than one report of cyber extortion every day.

1A6 Criminal hacker psychology

Category 1A6 Criminal hacker psychology

1999-04-01 **virus writers sociology psychology information warfare**

THE DALLAS MORNING NEWS, TEXAS

An article in the Dallas Morning News for April Fool's day quoted Peter Tippett, Sarah Gordon, Winn Schwartau and others discussing the motivations of virus writers and criminal hackers. The experts thought that motivations were complex and varied, that the current crop of virus writers were largely young and less technically sophisticated than the first generation of virus-writing idiots, and that most were probably not malicious — at least, their intentions were not malicious. Their products often are.

Category 1A6 Criminal hacker psychology

2002-03-05 **criminal hacker psychology worm social engineering**

NewsScan

GIRLS JUST WANT TO HAVE HACKER FUN
An unidentified hacker who claims to be a 17-year-old girl says she was motivated to write the "Sharpei" worm to dispel the notion that there aren't any female virus writers and to annoy Microsoft, rather than to have it spread to actual computer users. Going by the name "Gigabyte," she says on her Web site that she's a high-school senior who takes kick-boxing classes and likes techno and trance music. A consultant for Sophos, the U.K. based security company that reported the worm says, "I just don't know what she's accomplishing by this. She's neither hurting nor helping people." The worm was written to spread via Outlook Express e-mail, with a subject line reading, "Important: Windows Update." (Reuters/New York Times 4 Mar 2002)
http://www.nytimes.com/reuters/technology/tech-tech-feminist.html

---

Category 1A6 Criminal hacker psychology

2003-03-18 **virus writer psychological profile study**

NewsScan

PROFILE OF A VIRUS WRITER
According to the UK's Sophos, one of the world's largest antivirus companies, about 1,000 viruses are created every month, and in almost all cases the perpetrators are computer-obsessed males between the ages of 14 and 34. "They have a chronic lack of girlfriends, are usually socially inadequate and are drawn compulsively to write self-replicating codes. It's a form of original graffiti to them," says Sophos CEO Jan Hruska. Virus writers tend to explore known bugs in existing software or look for vulnerabilities in new versions in order to create and spread their infections, and Hruska notes that the next target for the virus writing community could be Microsoft's .Net platform for Web services. To boost the impact of their creations, virus writers also tend to share information to create variants of the same infection, such as the infamous Klez worm, which has been among the world's most prolific viruses in the last year. (Reuters/CNet News.com 18 Mar 2003)
http://news.com.com/2100-1002-993023.html

Category 1A6 Criminal hacker psychology

2003-04-28 **hackers e-commerce white hats exploit software systems IBM Global Services Ontario Canada global security**

NIPC/DHS

April 28, National Post (Canada) — Ethical hackers uncover system problems.

With the proliferation of e-commerce activity, a new breed of hacker has come along: "white hats," or ethical hackers, who dedicate themselves to identifying and exploiting flaws in supposedly impregnable software systems. Interest in hiring white-hat security investigations is on the rise. Some people point to the realities of the world after September 11, 2001, as the reason. "9/11 told us that virtually anything is possible now," says Trevor Townsend, national principal, critical infrastructure protection systems, IBM Global Services, in Ontario, Canada. "There's a new global security posture because terrorists will stop at nothing to achieve their ends...It has changed things for technology as a whole."

Category 1A6 *Criminal hacker psychology*

2003-08-26 **virus Sobig network vandal motivation attacker**

NewsScan

MORE THEORIES ABOUT SOBIG VANDAL'S MOTIVATION
Is money the real motivation for the spread of the Sobig virus? Sobig is transmitted as an e-mail attachment and is the sixth variant of the malicious code by an unknown attacker. Mikko H. Hypponen, director of antivirus research at F-Secure corporation in Finland says: "I think the motivation is clear: it's money. Behind Sobig we have a group of hackers who have a budget and money." Computer security expert Russ Cooper suggests that the vandal is acting out comic book fantasies: "You can liken this guy to Lex Luthor and we're all Supermen. Luckily, we've been able to get the kryptonite from around our necks each time so far." One popular theory is that Sobig is the work of an e-mail spammer who is aggressively trying to build a clandestine infrastructure for blitzing the Internet with junk e-mail. Antivirus software researcher Joe Hartman of TrendMicro says, "If machines remain infected they could be used in any kind of attack. The question we ask ourselves is, What is he trying to achieve? We don't think it's planned for a specific threat, rather its more likely a money-making spam scheme." And Bruce Hughes of Trusecure points out: "There is some evidence that he's been tied in with spammers." Sobig spreads further only when a computer user selects the attached program that then secretly mails itself to e-mail addresses stored in the user's computer. The Computer Emergency Response Team at Carnegie Mellon University says, "Our current advice is: Don't open an attachment unless you are expecting one." (New York Times 26 Aug 2003)

Category 1A6 *Criminal hacker psychology*

2003-09-28 **Torvalds kids dates script kiddies geeks teenagers**

NewsScan

TORVALDS: GEEKY KIDS NEED DATES
Asked how to end virus and worm attacks, Linux creator Linus Torvalds told an interviewer: "When you have people who hook up these machines that weren't designed for the Internet, and they don't even want to know about all the intricacies of network security, what can you expect? We get what we have now: a system that can be brought down by a teenager with too much time on his hands. Should we blame the teenager? Sure, we can point the finger at him and say, 'Bad boy!' and slap him for it. Will that actually fix anything? No. The next geeky kid frustrated about not getting a date on Saturday night will come along and do the same thing without really understanding the consequences. So either we should make it a law that all geeks have dates — I'd have supported such a law when I was a teenager — or the blame is really on the companies who sell and install the systems that are quite that fragile." (New York Times Magazine 28 Sep 2003)

Category 1A6 *Criminal hacker psychology*

2004-01-14 **Internet addict stereotype refuted digital divide decreasing**

NewsScan

NEW STUDY REFUTES NET 'GEEK' STEREOTYPE

The typical Internet user has plenty of friends, an active social life and would rather read a good book or log on than watch TV, according to a report by UCLA's World Internet Project, which surveyed Net users and non-users in 14 countries to come up with its results. The image of Net users as socializers contradicts the stereotype of propeller-head "geeks" who spend their days (and nights) hunched over their keyboards, shunning human contact. The study did, however, reinforce some other demographic trends, including the fact that wealthier people tend to be more avid users, and that men outnumber women on the Net, although those figures vary by country, with Italy exhibiting the largest gender gap and Taiwan the smallest. Meanwhile, the digital divide — the phrase widely used to describe the disparity in Internet usage between rich and poor — appears to be narrowing around the world. Sweden, Korea and the U.S. had the largest number of low-income users. (Reuters/CNet News.com 14 Jan 2004)

Category 1A6 *Criminal hacker psychology*

2004-02-20 **RSA security conference computer vandals social engineering hacking**

NewsScan

VANDALS: BETTER AT LYING THAN AT HACKING

At a security conference last week sponsored by the security firm RSA, 10,000 computer security experts showed up — and chances were good that some of them were vandals. Ira Winkler, an expert on corporate espionage, said: "They're definitely here," in a disdainful reference to hackers whose technical skills are as meager as their personal ethics: "All you have to do is be a good liar." Some lie by stealing passwords or PIN numbers simply by looking over a user's shoulder ("shoulder surfing," it's called); others by creating spam that purposely uses misspelled words to evade spam filters. Winkler says: "They think what they're doing is special," even though it's "more difficult to learn how to protect a computer than to break into one." (San Jose Mercury News 20 Feb 2004)

Category 1A6 *Criminal hacker psychology*

2004-03-04 **network virus worm writers fight online MyDoom Bagle Netsky**

NewsScan

VIRUS WRITERS SQUABBLE ONLINE

The writers of Internet plagues MyDoom, Bagle and Netsky have ratcheted up their competition, embedding insults and threats against each other in the coding of the latest versions of their computer bugs. For example, "MyDoom.f is a thief of our idea!" and "Bagle — you are a looser!" both appear in the code of the latest Netsky worm [no one ever said worm writers were literate!]. Ken Dunham, director of malicious code at iDefense, says the spat appears to exemplify the rivalry between the authors of MyDoom and Bagle, both of which attempt to take control of infected computers, while the Netsky worm attempts to deactivate the other two. "There's a huge pool of computers that are always infected," says Dunham, who estimates that number at somewhere in the low hundreds of thousands. Virus writers "want to make sure they have complete control of those computers." Meanwhile, the new versions just keep on coming — there've been 11 versions of Bagle, seven of MyDoom and six of Netsky, which appeared only last month. "We are just seeing variation after variation," says a VP of one antivirus company. (Washington Post 4 Mar 2004)

Category 1A6 *Criminal hacker psychology*

2004-10-21 **hackers Ballmer Microsoft security**

NewsScan; http://apnews.excite.com/article/20041021/D85RQQJ00.html

BALLMER SAYS HACKERS GETTING SMARTER

Microsoft chief executive Steve Ballmer says the battle against hackers has gotten harder because the hackers have gotten smarter, too. However, as a sign of the company's progress in the fight, Ballmer points to Microsoft's planned security enhancements to Windows Server 2003: "I think we've learned a lot more about security basically than anyone else in the world. That's kind of the good news and bad news, being the position we've been in with our kind of market share."(AP 21 Oct 2004)

Category 1A6 *Criminal hacker psychology*

2005-01-13 **web vandalsim hackers Bruce Schneier crime psychology**

NewsScan; http://tech.nytimes.com/pages/technology/index.html

SECURITY III: THE CRIMINAL CLASS

In an interview with journalist John Markoff of the New York Times, security expert Bruce Schneier suggests that the problem of Web vandalism has fundamentally changed in the last several years. Previously, hackers were mainly kids, engaging in hacking as a kind of intellectual challenge or a sport, but more recently hackers are coming mainly from criminals "in Third World countries, from Africa, South America, Asia, and the former Soviet Union" -- a development that makes life much harder for security officials. Schneier, whose latest book is "Beyond Fear," is founder and chief technology officer of Counterpane Internet Security. (New York Times 13 Jan 2005)

Category 1A6 Criminal hacker psychology

2005-06-08 **criminal hacker penetration government computers damage estimate extradition flying saucers UFOs theory jail charge allegations accusations**

RISKS; http://tinyurl.com/b6x5e 23 89

CRIMINAL HACKER "SOLO" ACCUSED OF BREAKING INTO US GOVT COMPUTERS TO FIND EVIDENCE OF UFO COVERUP

Rob Singh reported on the case in the London _Evening Standard_ newspaper:

Gary McKinnon, 39, was seized by the Met's extradition unit at his Wood Green home.

The unemployed former computer engineer is accused of causing the US government $1billion of damage by breaking into its most secure computers at the Pentagon and Nasa. He is likely to be extradited to America to face eight counts of computer crime in 14 states and could be jailed for 70 years….

Most of the alleged hacking took place in 2001 and 2002…. Friends said that he broke into the networks from his home computer to try to prove his theory that the US was covering up the existence of UFOs. He is accused of a series of hacking offences including deleting "critical" files from military computers. The US authorities said the cost of tracking him down and correcting the alleged problems was more than £570,000. The offences could also see him fined up to £950,000 if found guilty on all charges…. [T]he US first issued an indictment against him in November 2002.

Prosecutor Paul McNulty alleged that McKinnon, known online as "Solo," had perpetrated "the biggest hack of military computers ever". He was named as the chief suspect after a series of electronic break-ins occurred over 12 months at 92 separate US military and Nasa networks.

McKinnon was also accused of hacking into the networks of six private companies and organisations. It is alleged that he used software available on the internet to scan tens of thousands of computers on US military networks from his home PC, looking for machines that might be exposed due to flaws in the Windows operating system.

Many of the computers he broke into were protected by easy-to-guess passwords, investigators said. In some cases, McKinnon allegedly shut down the computer systems he invaded.

The charge sheet alleges that he hacked into an army computer at Fort Myer, Virginia, where he obtained codes, information and commands before deleting about 1,300 user accounts….

Category 1A6 Criminal hacker psychology

2006-04-13 **NASA hacker Gary McKinnon speaker Infosecurity Europe Guantanamo Bay stay unauthorized access penetration**

DHS IAIP Daily; http://news.zdnet.co.uk/internet/security/0,39020375,39263341,00.htm 23

NASA HACKER TO SPEAK AT SECURITY SHOW.

NASA hacker Gary McKinnon will be joined by other hackers and security experts on a panel discussion at the Infosecurity Europe conference Thursday, April 27, in London. McKinnon faces the prospect of an indefinite stay in Guantanamo Bay, but this won't prevent him from appearing on the Infosecurity panel and discussing hacking at a UK security conference. The NASA hacker is currently fighting extradition to the U.S. in what has been a protracted trial. He is charged with gaining unauthorized access to 97 U.S. government computers, including machines belonging to NASA and the Department of Defense. He claims he was searching for evidence of UFOs.

1B Pornography, Net-harm, cyberstalking, gambling, online auctions

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1997-02-26 **hacker**

AP, Reuter

Chris Zboralski, a 21 year-old French criminal hacker, was fined $8,500 and given an 18-month suspended sentence in Paris for using the FBI's phone system to place $250K of AT&T international phone calls at US government expense in 1994. According to AP, Judge Francis Bruty called Zboralski "a computer genius with a lamentable morality." However, his expertise consisted largely of impersonating an FBI agent and convincing a bureaucratic dupe to give him the access numbers for the FBI's conference-call account. Zboralski showed no remorse; on the contrary, he signed a book deal with a French publisher and announced that he was going into business as a security consultant. Better watch your phones if you hire him.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1997-05-20 **hacker intrusion**

AP, InfoSecurity News

In Greeneville, TN, convicted criminal hacker Wendell Dingus was sentenced to six months of home monitoring and ordered to pay $40,000 in restitution to the Air Force Information Warfare Center and other military organizations for the 1995 intrusions he perpetrated against them. He also admitted to cracking into NASA computers.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1997-06-02 **hacker psychology**

C!Net http://www.usnews.com:80/usnews/issue/970602/2crac.htm

David Freedman and Charles Mann published _At Large_ (Simon & Schuster), an analysis of the curious case of Matt Singer, known in the computer underground as "phantomd." This maladjusted and unfortunate youngster broke into accounts at MIT, Los Alamos and Livermore National Laboratories, Intel, and many other sites. He tried to use the supercomputers at NASA sites to run Crack, a password-guessing program for determining passwords encrypted in UNIX password files. The FBI's National Computer Crime Squad, founded ion 1992 by Agent Jim Settle, obtained warrants for wiretaps on their key suspect, Matt Singer. By this time, the youngster was attempting to break into the main Internet backbones to run a high-speed sniffer program. With an accomplice, he snagged 60 Mb of data in break-ins of a few minutes at a time, accumulating untold numbers of logins and unencrypted passwords. In December 1992, the FBI burst into the Singers' home and found a poverty-stricken, brain-damaged, schizophrenic 19-year old barely aware of the world around himself but addicted to the joys of criminal hacking. The Department of Justice declined to prosecute and the case sank into obscurity, as did Matt Singer, who was living on Social Security disability payments when the authors completed their book about him.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1997-06-17 **hacker sentencing Mitnick**

LA Times

Kevin Mitnick was sentenced to 22 months in prison for cellular phone fraud and for violation of the terms of his probation. The feckless fugitive hacker faced additional charges from a 25-count federal indictment for software theft. The judge also ordered the computer addict to stay away from all computers, cell phones or software when he is released from prison. Mitnick was also prohibited from being employed in any job that would allow him to have access to computers without approval from a probation department officer. In November, Mitnick's lawyer appealed for funds to help protest the conditions under which Mitnick was allegedly held, including solitary confinement, freezing temperatures in his cell, and being manacled for his trips to the showers.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1997-06-19 **hacker culture information warfare**

TechWire

The UK's Defence Evaluation and Research Agency warned that "The hacker community is splitting into a series of distinct cultural groups — some of which are becoming dangerous to businesses and a potential threat to national security." Alan Hood, a research scientist in the information warfare section of DERA, said that information brokers coordinate attacks by ordinary hackers and then sell the information to governments or competing organizations. Meta-hackers observe ordinary hackers and then silently take advantage of the vulnerabilities discovered by the blabbermouth hackers. "Elite" hackers stick to their own class of hacker and sneer at those who use widely-available tools and scripts. "Dark-side" hackers attack systems for financial gain or to do harm, violating the much-vaunted standards of the hacker world. Most importantly, Hood urged network managers to stop trying to prevent all attacks; instead, focus on deterrence, protection, detection and reaction. Make it difficult enough for hackers that they will move on to another target; encrypt sensitive data and prevent social engineering; install intrusion-detection software; and respond to all attacks or oddities on your systems.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1997-07-12 **hackers convention**

AP

In Las Vegas, computer hackers staged yet another DefCon — the fifth annual and largest yet, with 1500 people packed into a second-rate hotel convention hall. Participants included legitimate firms prospecting for possible employees, hoping that their candidates could manage the transition from cyber-desperado to honest security expert.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1997-07-14 **hacker convention Black Hat Microsoft L0pht**

ELECTRONIC ENGINEERING TIMES; Computerworld 31 28

Microsoft reversed its usual policy and sent staff to the Black Hat Briefings in Las Vegas to meet hackers who demonstrated flaws in Windows NT security. Despite the scepticism of more conservative security experts such as your editor, NT marketing director Carl Karanan said, "It's good to look at things in perspective; this conference does that. We've opened up a dialogue. The hackers do a service. We're listening and we're learning." Other audience members at the Briefings came from Cisco, ESPN, Toyota, Price-Waterhouse, the Defense Department and the National Security Agency. At a Meet the Enemy session, several system administrators expressed scepticism about the supposedly good intentions of the hackers. Key NT hackers presenting at the conference included "Mudge" from the L0pht; Yobie Benjamin of Cambridge Technology Partners; and Dominique Brezinski.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1997-07-16 **hackers convention Hack-Tic HIP**

Scotsman, Wired, Agence Presse France

The Hacking in Progress hacker convention took place in August in a field near Amsterdam. Some of the topics of discussion suggest that the hacker underground may be moving towards a more mainstream approach to technology. For example there were talks about Internet censorship, spam, and cryptography. Many of the hackers now work for corporations, including the Dutch ISP XS4All, which was itself founded by reformed hackers. However, the criminal side of hacking was also well represented. Many of the discussions focused on how to abuse systems rather than on how to repair them. There was also an embarrassing incident when telephone engineers for the Netherlands PTT discovered a break-in by a cellular phone user at the camp who fraudulently tried to place free international calls.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1997-07-22 **fraud hackers insiders theft fraud diddling**

The Futurist via Times of India

One of the Masters of Deception, John Lee, was reported in July as boasting about his ability to break into systems and steal products and services. Despite his one-year prison term, Lee is said to have "admitted that he would certainly be tempted to do it all again." However, wrote Gene Stephens in _The Futurist_, "a far greater threat to businesses than hackers are disgruntled and financially struggling employees. As internal theft from retail stores has always been many times greater in volume than theft from shoplifters, robbers, and burglars, theft by employees armed with inside information and computer access is and will continue to be a much larger problem than intrusion by hackers, crackers, and terrorists combined."

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1997-08-04 **hackers hiring**

Computerworld

Matthew Harrigan, founder of MicroCosm, a San Francisco security company that specializes in Tiger Team attacks, is an ex-hacker who hires only ex-hackers as security consultants. Author William Spain interviewed him for an article in Computerworld and analyzed the risks of hiring people who have fun breaking the law. Russ Hailey, president of Lawrence, Kan.-based Secure Network Systems, was not keen on this strategy: "I would not hire an ex-thief to protect a warehouse, and I won't employ any ex-hackers, period," he said.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1997-08-08 **hackers convention meeting**

AP

At the Beyond HOPE (Hackers on Planet Earth) meeting in New York sponsored by 2600 Magazine in August, hackers expressed the Party Line on how useful and knowledgeable they are: "Hackers actually design the systems and show how they work, how to make them better, and how to make them secure, said Emmanuel Goldstein [Eric Corley], an editor of [2600] a hacker magazine." David Kalish of Associated Press quoted a hacker known as Chesire: "Crashing the system should not be your objective. It had been in the past. That's the playground bully. Now it's no longer cool. Anyone can crash a system. It's more clever to find out how to make it NOT crash." For all the positive spin, however, organizers of the meeting asked the hotel to disconnect all the phone jacks in their rooms for the duration of the conference.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1997-11-26 **hacking penetration intrusion court case**

RISKS, Times (London), PA News 19 48

Matthew Bevan (AKA "Kuji"), an alleged associate of Richard Pryce (the "Datastream Cowboy") walked free in November when charges of unauthorized access and data modification (into the Griffiss AFB and Lockheed) were dropped.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1998-01-21 **criminal hacker lenient pornography penetration laws**

Reuters

Despite having vandalized a Swedish government Web site by advertising pornography on it and admitting to breaking into NASA computers, two young Swedish criminal hackers were released without charge after a year-long hunt. Police explained their inaction by stating that "no economic crime had been committed." Sounds like time for some new laws. . . .

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1998-02-12 **crackers criminal hackers seminars excuses rationale ideolog**

New York Times

Matt Richtel wrote an extended review for the New York Times of the series of seminars organized by retired Army colonel Fred Villella. These seminars feature criminal hackers in starring roles. Their opinions about the role and importance of criminal hackers are valuable insights into their motivations and rationalizations. Notorious criminal hacker Christian Valor, for example, sneered, "Who do you want to learn how to protect your system from?" Valor said. "Some corporate guy, or me — a guy who's actually hacked into your computer network?" "Crackers have contributed more to computer security than any other person from any company," he insisted.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1998-02-15 **criminal hacker KGB Russian Soviet fraud crime ISP**

Scotland on Sunday

Mary Picken, a Scots CompuServe user, was hopping mad when she was charged £1,800 for 1000 hours of access charges racked up in Eastern Europe. She adamantly denies ever having been to eastern Europe, let along using that much connect time overseas, but CompuServe insists that she must be responsible for the charges. The ISP claims she must have given away her access code and password, but she denies this accusation as well. Supporters argue that there is mounting evidence that CompuServe's practice of sending passwords in the clear allows organized criminal rings in the former Soviet bloc to cheat consumers on a large scale.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1998-02-26 **criminal hackers hire consultants Tiger team**

Guardian

Supposedly reformed criminal hackers in the UK set up their own consulting firm to offer Tiger Team penetration testing to British clients. The team leader was Mathew Bevan, who admitted hacking into a US Air Force base at the age of 19.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1998-03-05 **criminal hackers Soviet Russian ISPs fraud theft impersonate**

International Herald Tribune

CompuServe, tired of the amount of fraud perpetrated by criminals in the former Soviet bloc, withdrew from Russia and from Bulgaria. Orphaned CompuServe subscribers would henceforth have to access the service via their own ISPs.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1998-03-05 **criminal hackers crackers toolkits danger threat patches**

San Jose Mercury News

David Wilson of the San Jose Mercury News argued that the current spate of criminal hacker attacks pose little threat to society. "While the universe of computer hackers includes some brilliant operators, most intrusions are simple trespass by relatively unsophisticated "crackers," as malevolent hackers are known. For them, unauthorized visits are not designed so much to gain access to data as to score points with fellow crackers; that's how they accumulate status in the tribe." Security experts emphasized that keeping up-to-date on patches would bar at least the amateurs who typically use hacking-toolkits without understanding the details.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1998-03-31 **criminal hackers glorify praise positive television Web**

ICSA http://www.discovery.com/area/technology/hackers/hackers.html

ICSA's Director of Research, Dave Kennedy, spotted an old Web page from Discovery Channel that glorified criminal hackers. When your editor called Discovery to discuss the issue, the Corporate Communications department declined to return my call.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1998-06-04 **criminal hackers information warfare antinuclear Web vandals**

Newsbytes

The MilW0rm criminal hacker group attacked the Bhabha Atomic Research Center (BARC) in India as punishment for the nuclear tests carried out by that country. As proof of their exploit, they posted information stolen from that site. They then announced that they would attack Pakistani systems also. This marks another step in the politicization of hackerdom.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1998-08-02 **criminal hacker conference tools techniques meeting**

http://www.defcon.org/html/defcon-6.html

DEF CON 6.0 took place at the Plaza Hotel and Casino in Las Vegas, NV. This annual criminal hacker convention includes speakers who are not themselves criminal hackers or even sympathizers. Along with hacker games, the program included serious lectures by luminaries such as Bruce Schneier, Ira Winkler and Winn Schwartau.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1998-09-04 **criminal hacker cracker FBI sentence court fine prison law**

Wired http://www.wired.com/news/print_version/politics/story/14856.html

Daryl Lindsey published a brief summary of the criminal careers and punishments of several notorious criminal hackers. The article in Wired listed Robert T. Morris, the Legion of Doom hacker crew, Kevin Poulson, the Masters of Deception gang, and Justin Petersen.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1998-11-06 **criminal hacker recidivism family upbringing values**

Milwaukee Journal Sentinel
http://www.jsonline.com/archive/oct98/news/wauk/981031brookfieldhackerinco
u.asp

Rajib Mitra, 20, was convicted of hacking into the University of Iowa's systems while on probation for having hacked into the University of Wisconsin at Milwaukee in 1996. A news report by Lisa Sink of the Milwaukee Journal Sentinel reported that ". . . Mitra gained access to others' computer accounts, created an illegal account with full administrative authorities and altered records to cover up his security breaches. . . . To enter the off-limit areas, Mitra tapped into his parents' Internet account at their Brookfield home and used it as a conduit to access Iowa's system, prosecutors said." Mr Mitra pleaded no contest to the charges. According to Sink's report, at his hearing, Mitra showed little sign of contrition: "He did not apologize for his crimes and said very little in court." His parents immediately paid his $1,000 fine.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1998-11-27 **criminal hacker death murder suicide hanging cryptography**

AP, Guardian Weekly (UK)

Boris Floriciz, a German 26 year-old "former" criminal hacker and cryptography expert, was found dead hanging from a tree in Berlin in October. Police suspected suicide; his friends in the Chaos Computer Club protested that Floriciz had no sign of suicidal tendencies and was on the contrary a happy and successful ex-hacker. Some commentators and family members hinted darkly at dirty business by espionage agencies.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1999-01-06 **criminal hacker capture fugitive escaped parole violation**

AP

Convicted criminal hacker Justin Petersen was arrested on Dec 11, 1998 in Los Angeles after three months of parole violation. The generally-reviled criminal was known as Agent Steal for his tendency to steal information, defraud victims and betray his acquaintances to the police. He tampered with a radio contest by seizing control of its telephone lines and claimed to have led the FBI to equally notorious hacker icon Kevin Mitnick. He absconded from the halfway house in which he was to have served his remaining three years of incarceration (after 3.5 years in penitentiary). He posted arrogant messages on the Internet sneering at the FBI — not a measure calculated to let the federal police lose interest in him.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1999-01-08 **criminal hackers statements hacktivism ethic propaganda**

National Post (Canada)

After the Legion of Underground (LoU) announced on the 1st of January 1999 that they would attack and disable the computer systems of the People's Republic of China and of Iraq, a coalition of criminal hacker organizations announced opposition to the move. Eric Corley (using his pseudonum "Emmanuel Goldstein"), editor of _2600: The Hacker Quarterly_, signed the statement from Cult of the Dead Cow, Chaos Computer Club, !Hispahack, LOpht, Phrack, Pulhas, and Toxyn. "This kind of threat, even if made idly, can only serve to further alienate hackers from mainstream society and help to spread the misperceptions we're constantly battling. And what happens when someone in another country decides that the United States needs to be punished for its human rights record? This is one door that will be very hard to close if we allow it to be opened," said Corley in the statement. "We strongly oppose any attempt to use the power of hacking to threaten or destroy the information infrastructure of a country, for any reason," the coalition said. "Declaring war against a country is the most irresponsible thing a hacker group could do. This has nothing to do with hacktivism or hacker ethics and is nothing a hacker could be proud of," the coalition said in the statement. "Space Rogue" (of The L0pht), wrote, "Though we may agree with LoU that the atrocities in China and Iraq have got to stop, we do not agree with the methods they are advocating."

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1999-01-15 **criminal hackers consultants white hat reformed business**

http://www.upside.com/texis/mvm/news/story?id=369e739c0

Deborah Radcliff reviewed some success stories — and some failures — for criminal hackers apparently gone legitimate. She interviewed famous (or notorious) formerly-criminal hackers Yobie Benjamin, Peter Shipley and barefooted Al Walker (Hobbit) as well as some of their employers and clients. The message in the article was mixed; some criminal hackers have failed miserably to adapt to the corporate world (and vice-versa) but a few are managing to convince at least some people in the business community that they may be trustworthy.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1999-02-17 **meta-hacking criminal script kiddies thieves Internet Web**

OTC

Script kiddies are increasingly being manipulated by meta-hackers — more experienced criminals who use the naïve kids to infiltrate systems and then collect information through their minions' activities. According to David Butler of Axent Technologies, "Cracking attempts rise by a factor or three or four during school holidays." New tools for meta-hacking include Java-based Trojans that can corrupt innocent users' browsers so that they inadvertently attack other Web sites and transmit information to the malefactors. In another meta-hacking attack, someone inserted code into the free Tcpwrapper software for authenticating logins; the Trojan version sent login records to an e-mail address. According to one of Nokia Telecommunications' marketing directors, Bob Brace, the company detected 24,000 cracking attempts between October 1998 and the end of January 1999. Many of the probes were spaced out over time in a stealth technique to avoid detection, said Brace.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1999-02-22 **criminal hackers Russia former Soviet Union fraud ISP**

Wall Street Journal

In Russia, criminal hackers were so active that many Net users lost control over their passwords and their accounts. Kimberley A. Strassel, writing in the Wall Street Journal, reported that several Russian police forces had formed cyber-police squads to patrol the Internet and help track down electronic thieves. A report in July 1999 suggested that a program code-named Moonlight Maze has been using criminal hacking techniques to steal military secrets from the US government and R&D data from US corporations.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1999-04-01 **criminal hacker punishment imprisonment protests pity**

Daily Telegraph

Wendy Grossman, writing in the _Daily Telegraph_ (1999-04-01), discussed the Kevin Mitnick case. She described how a relatively minor criminal hacker become the poster boy for a generation of criminal hackers and wannabes. Her closing remarks were particularly interesting: "The hacker community tends to follow the prison careers of all hackers and crackers as though they were political prisoners, and has rallied to support Mitnick, particularly as his time in jail without a bail hearing lengthened. The Free Kevin Web site (www.kevinmitnick.com) recounts every incident of his jail career, from his lack of access to legal books to the bizarre report that in early 1997 he was put in solitary confinement for unauthorized possession of 74 cans of tuna. No one is saying it was all right for Mitnick to break into computer systems. But nothing he did was as destructive as Robert Morris's 1988 Internet worm, a badly written bit of code that paralysed large portions the network; Morris got probation. Equally, Mitnick is not known to have profited from information he copied, unlike some hackers who served lighter sentences. Finally, the general word about Mitnick is that he is not particularly a technical genius; his skill is in "social engineering" – persuading people to give him information they're not supposed to, such as passwords. Ultimately, what Mitnick's case and the publicity surrounding it have done is widen the gap of distrust between hackers and the law."

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1999-04-13 **criminal hackers script kiddies children youngsters law enforcement detection tools penetration automated attack**

AUSTRALIAN FINANCIAL REVIEW, Canberra Times

Script kiddies pose a worsening threat to the Net, according to ex-hacker Jeff Moss, now with Secure Computing. According to John Davidson, writing in the _Australian Financial Review_, Moss warned that the number of tools allowing know-nothing kids to hack successfully is growing; in addition, he said, law enforcement is falling behind in detection and prosecutions: "It's recently become very safe to use computers for crime. You really have to screw up, or you really have to attract the attention of the FBI for some reason, for there to be any negative consequences."

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1999-04-22 **criminal hackers Y2K vulnerability attacks**

Computing (UK), Canberra Times

Many security experts warned that the Y2K transition could include a splash of criminal hacking. Stephen Cobb of Miora Systems Consulting and Neil Barrett of Bull Information Systems concurred that criminals would take advantage of the potential disruption due to non-compliant systems. In particular, everyone should be on the lookout for e-mail borne viruses and Trojans. Cobb warned everyone not to open e-mail attachments from strangers.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1999-05-19 **criminal hacker interviews publicity support**

Times of London

Morag Preston wrote a profile for the Times of London about the founder of AntiOnline, John Vranesvich. Mr Vranesvich was running his Web site about criminal hackers from the University of Pittsburgh when Ehud Tenebaum gave him an exclusive interview. When University officials forbade this use of their systems, he abandoned college and formed his own company. He admitted that his platform for criminal hackers runs the risk of glorifying activities which he dislikes (he is not a criminal hacker himself and says he has never approved of criminal hacking). He told Preston that he feels that showing kids the dangers of criminal hacking for both hackers and victims is an important educational message.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1999-05-25 **criminal hacker convention briefing conference**

PR

Secure Computing announced the 1999 Black Hat Briefings in Las Vegas for July 7-8. Participants included a mixture of security professionals and criminal hackers. Along with Peiter Zatko ("Mudge") of L0pht Heavy Industries and Peter Shipley (of 24-hour war-dialing fame) the platform included the respected cryptographer Bruce Schneier.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1999-06-05 **criminal hacker demonstration protest punishment excess justice**

Reuters

A dozen supporters of Kevin Mitnick protested his treatment by rallying before the US Supreme Court building in Washington, DC. They said they did not condone Mitnick's criminal hacking but felt that he was being punished excessively.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1999-06-14 **criminal hacker psychology biography history story adolescent teen-ager penetration gang tools subculture motivation amorality**

Wall Street Journal

John Simons of the Wall Street Journal wrote an extensive biographical sketch of Patrick Gregory, the 18-year-old who confessed to the FBI that he was "Mosthated," one of the founders of gH (Global Hell). The gH criminal hacker gang, with up to 30 members at various times, was one of the groups responsible for a wave of Web vandalism against US government and university sites in the Spring of 1999. The adolescent's story details how he became increasingly disruptive in school and finally quit school without graduating. He was arrested for possessing marijuana, lost his driver's license, and turned to full-time criminal hacking with a criminal hacker from Green Bay, WI who called himself Mindphasr. The two of the formed Global Hell and became involved in stealing credit-card numbers and abusing corporate conference-call lines. Gregory repeatedly broke into corporate systems, read internal e-mail, and vandalized systems. He then stupidly decided that a good way to get a job was to leave messages on the systems he penetrated telling administrators how to patch their security holes — so-called "gray-hat" hacking. He actually did get a job from one of his victims, Parachute Computing Systems of Austin, TX but blew it by continued criminal hacking in his spare time. He was busted by the FBI, which seized his computer. His mother immediately bought him another one and he was back online within a few days.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1999-06-24 **reformed criminal hacker security consultant trust doubt worry concern recidivist ethics**

Straits Times (Singapore)

Mathew Bevan was the subject of great concern a few years ago when he hacked into NASA, NATO and USAF computers systems. However, four years later, he describes himself as a reformed hacker and gives lectures on INFOSEC to anyone who will listen. Bevan, who was never prosecuted after his arrest at the age of 20, is now a security consultant who repudiates his past and dismisses the opinion of his erstwhile friends in the criminal hacker underground. Some of his clients expressed scepticism about his trustworthiness. Mr Sunny Tan of Singapore security company, Infinitum, asked, "Would you trust an ex-hacker with your network? He's done it once, he could do it again."

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1999-07-01 **criminal hacker biography psychology corporate policy unauthorized use CPU cycles**

PC Magazine

Bill Machrone, veteran PC Magazine writer, prepared an insightful analysis of the Aaron Blosser case. Readers will recall that Aaron Blosser, a 28-year-old consultant, was accused in 1998 of misappropriating resources on 2585 computers at his client, U.S. West (a major telephone company). In his attempt to find ever-greater prime numbers, he commandeered over 10 years of processing cycles; as a result of the extra work, directory-assistance operators found the time for retrieval of telephone numbers stretching from the usual 3-5 seconds on into the 5 minute range. Associated Press reported, "The computers were so slow in mid-May that customer calls had to be rerouted to other states, and at one point the delays threatened to close down the Phoenix Service Delivery Center." Machrone wrote that US West declined to prosecute Blosser, who has learned his lesson: "Blosser ruefully suggests that anyone looking to do something with unused computer cycles on machines that are not their own ask permission first."

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1999-07-06 **criminal hacker convention conference meeting**

South China Morning Post (Hong Kong), Birmingham Post (UK), Wall Street Journal

The annual DEFCON convention started in Las Vegas in early July 1999, complete with two camera crews filming the proceedings and interviewing criminal hackers after their presentations. Highlights (so to speak) included the release of BO2K, the new version of the BackOrifice program produced by the Cult of the Dead Cow in 1998. Along with the usual discussions of techniques used for criminal hacking, the convention featured various games such as Spot the Fed, Hacker Jeopardy (hosted by Winn Schwartau), various online games, a hacking contest, and wrestling in inflatable Sumo wrestler costumes. Some Federal officials actually spoke to the hackers (receiving some jeers at their suggestion that criminal hackers should join the good guys) and at least one security firm installed software on the hacker-target machines as a form of quality assurance: Ron Gula of Network Security Wizards, Inc. installed his intrusion-detection system on the target machines and was able to detect all attacks launched by the hackers, some of whom even suggested improvements to his program.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1999-07-06 **criminal hacker psychology biography interview**

Straits Times (Sinapore)

The Straits Times (Singapore) published an interesting interview with some non-hacker observers of the criminal hacker scene in that country. Samuel Kwan, 16, and Nathanael Ng, 19, distinguished between honorable hackers and crackers, repeating the usual propaganda about intruders who leave polite messages indicating security vulnerabilities so they can be fixed. The young people sneered at "lamers" (aka "script kiddies") who use automated attack tools to cause harm but have no understanding of security or computer science.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1999-10-13 **criminal hacker collective subculture attitudes beliefs self-justification cult club gang**

www.thesynthesis.com

Someone calling him(or her)self "Bronc Buster" circulated a long description dated 1999-10-13 about a visit to the hacker collective New Hack City. The criminal-hacker supporter provides an interesting glimpse into the hacker underground, with hints of intrigue, elitism, and a time perspective that might startle adults: "New Hack, as the people who hang out there like to call it, was an idea that started way back in 1995 on the opposite side of the country, in Boston. It started with several friends wanting to find a place to gather, where they could share their experience with each other, learn, experiment, and most importantly pool their limited resources. In the early days of the Internet, as we know it, computer equipment was expensive, and dial-up access to it was hard to come by and was also expensive." The early days of the Internet? 1995? "So five people, FreqOut, GarbageHeap, ChukE, Rosie, and Deth Veggie, start the original New Hack City in Boston in 1995." The article continues with details of the links of this "hacker think-tank" with other criminal hacking organizations: "Many members of New Hack are also in the cDc, have been associated with the L0pht or worked with 2600. Regular people that hang out include a few people from the DOC, some people with 2600, and other notable groups. When I was there, several cDc members were there that are also part of the New Hack crew; like Tweety Fish, Deth Veggie and Sir Dystic (who wrote the original Back Orifice tool)."

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1999-10-29 **hiring criminal hacker prison sentence probation job**

Australian Financial Review
http://www.afr.com.au:80/content/991023/inform/inform1.html

In March 1998, Skeeve Stevens was sentenced to 3 years in jail but parole after 18 months. Stevens, aka "Optik Surfer," pleaded guilty to stealing and publishing 1200 credit card numbers belonging to subscribers of Australian ISP AusNet in 1995. In October 1999 he was released and immediately hired as a security consultant by June Heinrich, chief executive of Baptist Community Services. She was quoted as saying, "Well, he clearly was competent, wasn't he."

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1999-11-24 **criminal hacker translation manual book instructions how-to guide children wannabe script-kiddies**

Bangkok Post

A report in the Bangkok Post in late November by Otto Sync stated that a well-known criminal hacker in Thailand published a Thai-language compilation of elementary hacking tools. Security experts should look for increased hacking activity from Thailand.

Category 1B *Pornography, Net-harm, cyberstalking, gambling, online auctions*

1999-12-12 **criminal hacker movies film plays style fashion sexy popular heroes villains journalists media stereotypes clothing**

New York Times

Jesse McKinley published an interesting review in the New York Times of the changing representation of criminal hackers in the popular media and entertainment. He pointed out that some of the early films from the 1980s (e.g., War Games, Hackers) showed hackers in a mostly positive light, whereas lately they have been shown as darker, sometimes flatly evil, characters.

1B1 Adult pornography

Category 1B1 Adult pornography

2000-07-08 **pornography wireless application protocol WAP**

NewsScan

Analysts say the appearance of the first WAP (wireless application protocol) pornography sites signals the adoption of WAP technology into the mainstream. Although the sites offer only tiny grainy images of naked Japanese models, sociologists say that the key to predicting whether a new technology will take off is to determine whether it's used for pornography: "It's inevitable, I suppose, that with any new technology people will use it for porn," . . . [said] David Birch, CEO of Consult Hyperion. "That's been the story with photography and video cameras." The news should be welcomed by wireless companies, which have reported slower growth rates than they had hoped. (The Independent 8 Jul 2000)

Category 1B1 Adult pornography

2000-08-25 **pornography scam fraud credit-card international jurisdiction criminals theft**

NewsScan, RISKS, E-Commerce Times 21 03
http://www.ecommercetimes.com/news/articles2000/000824-4.shtml

The Federal Trade Commission has filed a lawsuit against Crescent Publishing Group and 64 affiliated companies that operate adult Web sites, accusing them of charging customers for services advertised as "Free Tour Web Sites." Like many adult sites, the Crescent sites requested that users supply credit card information to verify they were of legal age to view pornographic material. Customers who'd been promised a free online peep show say they were then billed for recurring monthly membership fees ranging from $20 to $90. Included among the complainants were some people who said they'd never visited the sites at all — in fact, one woman who'd been charged a recurring fee for several months didn't even own a computer. To add to the confusion, the charges were made under different company names. Instead of finding a charge from Highsociety.com on their statements, consumers would find charges from "Online Forum," or "Hoot Owl," or "Knock Knee." The FTC has classified the scam as one of the largest it's ever seen on the Internet, generating $141 [million] in the first 10 months of 1999 alone.

RISKS correspondent Lenny Foner noted the folly of using credit cards as a form of age authentication.

Category 1B1 Adult pornography

2001-01-12 **pornography technology innovation**

NewsScan

PORN INDUSTRY A FORCE IN DRIVING INNOVATION
The world's oldest profession has been instrumental for years in driving technological innovation. The porn industry was an early force in popularizing Polaroid cameras, VCRs, and CD-ROMs, and became the first industry to make money on the Web. Now it's turning its eye toward DVD technology and has begun making DVD movies that resemble video games, allowing viewers to watch and play along. "The technology fits our product," says one cutting edge DVD producer. Meanwhile, the interactive technology now pioneered by porn purveyors likely will find its way into mainstream Hollywood studios before too long: "It has a great children's application, says David Crawford, DVD production manager for Wicked Pictures. "You can tell a nice little fairy tale and have this be the frame of it. The idea is great, whether the content is for adults or children." (Los Angeles Times 9 Jan 2001)
http://www.latimes.com/news/columns/colone/20010108/t000002277.html

---

Category 1B1 Adult pornography

2001-03-07 **pornography children peer-to-peer networking legislation effectiveness**

NewsScan

KIDS AND PORN ON THE WEB
The constitutionality of the Child Online Protection Act of 1998 has yet to be decided by the U.S. Supreme Court, but its effectiveness may be in as much doubt as its wisdom, because Napster-like free swapping services may develop that will make the law largely irrelevant, since it makes Web site operators responsible for ensuring that their patrons are adults. But Herb Lin, a senior scientist at the National Research Council, says: "Right now, the so-called adult online industry is in it for the money. But what happens when a different community starts exchanging pornography on the Net and no money changes hands at all, just like Napster?" The technology already exists for doing just that. (San Jose Mercury News 7 Mar 2001)
http://www.siliconvalley.com/docs/news/svfront/porn030701.htm

---

Category 1B1 *Adult pornography*

2001-08-07 **pornography Internet Service Provider ISP commercial**

NewsScan

EUROPEAN ISPs TURN TO PORN FOR PROFITS
Cash-strapped European ISPs are branding their own adult content, aiming for the tried-and-true profits found in pornography and sex-related products. "What's triggering the move towards (adult content) is the steady revenue streams it generates. Sex sells," says Yankee Group European Internet strategies director Scott Smith. Freenet.de, Germany's No. 2 ISP, is preparing a mid-August launch of Fundorado.de, a site hawking hardcore videos, photos and sex chat rooms for about $8 a month. And on Monday, Freenet.de's biggest domestic rival T-Online announced it was teaming up with Barcelona-based Private Media Group to break into the adult content business, while last month, GMX.de -- a German free e-mail service -- said it would develop a similar venture. Meanwhile in the UK, struggling e-tailer Lastminute.com quietly introduced an auction specializing in sex toys last week. "The old revenue stream was click-throughs and e-commerce. Companies are being urged to develop new business models to convince investors there is value in an ISP or portal business," says Kai Kaufman, an analyst with Dresdner Kleinwort Wasserstein in London. A recent study by Netvalue indicated that 33% of German Internet users regularly access adult sites, and a 1998 Datamonitor report predicted that Internet pornography would represent a $2.8-billion business by 2003. (Reuters 7 Aug 2001)
http://news.zdnet.co.uk/story/0,,t269-s2092680,00.html

Category 1B1 *Adult pornography*

2002-05-06 **online pornography gambling**

NewsScan

INTERNET FINDS NEW WAY TO LOSE MONEY: ONLINE PORNOGRAPHY
Oh, the trials of the pornographer. How do you stand out against all the competition? With so much porn available for free, how do you get people to pay? With broadband connections widely available, how do you prevent customers from downloading everything quickly and then canceling their subscriptions? The days of easy profit on the Web are over, even for pornographers. The marketing and publicity for one well-known sex site says, "I think things are shaking out. The same rules have always applied to this business as any other." Another problem for online pornographers is that credit card companies tend to view them as "slow-pays" or deadbeats, and consider them to be a major source of fraud complaints and illegal activities such as underage sex and bestiality. So what's a poor pornographer to do? Many of them are now turning to online gambling. They're not really interested in sex, they're interested (surprise) in money. (San Jose Mercury News 4 May 2002)
http://www.siliconvalley.com/mld/siliconvalley/3200456.htm

Category 1B1 *Adult pornography*

2002-05-08 **youth children pornography report research sexual predators online**

RISKS, http://bob.nap.edu/html/youth_internet/ 22 06

[T]he National Academies' report entitled "Youth, Pornography and the Internet" was released on May 2. The report examines approaches to protecting children and teens from Internet pornography, threats from sexual predators operating on-line, and other inappropriate material on the Internet. It discusses social and educational strategies, technological tools, and policy options for how to teach children to make safe and appropriate decisions about what they see and experience on the Internet. Chaired by former Attorney General Dick Thornburgh, it's the most comprehensive study yet on the topic.

More information on the report is available at:
http://www4.nationalacademies.org/onpi/webextra.nsf/web/porn?OpenDocument

The report itself is available online at:
http://bob.nap.edu/html/youth_internet/

Category 1B1 *Adult pornography*

2002-08-16 **online pornography mainstream providers**

NewsScan

REALNETWORKS MULLING ADULT PAY-PER-VIEW
RealNetworks has made no secret of its desire to emulate the cable industry, with its core business strategy focused on delivering name-brand content and software services to paying customers. The company is currently in discussions with several audio and video producers to expand the lineup on its RealOne SuperPass service, and VP Dave Richards says that although there are no immediate plans to offer adult-only fare, the possibility of a future venture cannot be ruled out. "We expect we will have different tiers" of service. "Maybe even an adult tier." And while some analysts say getting into porn distribution is the kiss of death for mainstream publishers, others point out that the cable industry has dabbled in adult content for years without sparking a major backlash. Still, several Internet companies have tested the waters in the booming online pornography industry and decided to pull back. In April 2001, Yahoo yanked all pornographic ads, auction items and merchandise from its site in response to consumer complaints, and in January 2000, Ask Jeeves shelved plans to launch a separate search engine for pornography in order to preserve its family-friendly image. (CNet News.com 15 Aug 2002)
http://news.com.com/2100-1023-950053.html?tag=fd_top

Category 1B1 *Adult pornography*

2002-08-29 **online pornography national archives**

NewsScan

AUSTRALIA'S NATIONAL LIBRARY TO ARCHIVE INTERNET PORN
Australia's National Library is breaking new ground in digital archiving -- as part of its six-year-old project to record a selection of Web sites for historical purposes, the Library now says it will include a smattering of Internet pornography. "Whether we like it or not, pornographic sites are part of the Australian Web and we feel it is necessary to collect a sample, a small sample, of sites that reflect the use of some Australians of that kind of site," said Margaret Phillips, manager of the Library's online collection, in an interview with the Australian Broadcasting Corp. When asked whether she anticipates a backlash from those who feel such images have no place in the National Library, Phillips replied: "There may be a backlash, we haven't been expecting it. From time to time there is criticism of the kind of material the Library collects, both in print and online. But it is not the role of the National Library to act as the role of the censor." (ABC Online 27 Aug 2002)
http://www.abc.net.au/am/s659750.htm

Category 1B1 *Adult pornography*

2002-09-13 **pornography online commercial e-commerce auction bids**

NewsScan

SPANISH PORN COMPANY BIDS ON NAPSTER TRADEMARK
Private Media Group, a Spanish adult-entertainment company, has made an all-stock offer worth $2.4 million in a bid to acquire the trademark and Web address of the now-defunct Napster. Last week, a bankruptcy judge rejected a $9 million bid by Bertelsmann, saying the deal wasn't negotiated at arm's length, as required by law. Private Media said it plans to use the Napster trademark to promote its collection of "top quality" adult-oriented fare at a reasonable price, and to offer adults the ability to swap adult content for free. Private Media owns the global copyrights to what it claims is the largest library of adult-oriented content in the world. "Acquiring Napster is our way of entering the peer-to-peer marketplace for adult content in a closed environment," says Private Media CEO Charles Prast. "Along with Hollywood and the recording industry, we have become increasingly concerned about the level of copyright infringement inherent in the peer-to-peer file swapping services." (Reuters/CNet 12 Sep 2002)
http://news.com.com/2100-1023-957784.html?tag=fd_top

ROXIO WINS BID FOR NAPSTER
Roxio, the top seller of CD-burning software, has successfully bid to acquire Napster's technology, the Napster.com domain name, and the Napster brand for $5 million in cash and warrants to buy 100,000 shares of Roxio stock. The move took some music execs by surprise, but Roxio CEO Chris Gorog hastened to reassure the record labels that he planned to promote legitimate use of Napster. "Based on my relationships and general discussions with the labels, I think they will be excited at this announcement. They know that anything that Roxio will do in this space will be respectful of artist rights and will be working toward a commercial solution." (Los Angeles Times 15 Nov 2002)

Category 1B1 *Adult pornography*

2002-10-16 **video games pornography children adolescents teens parents**

NewsScan

HOLIDAY VIDEO GAMES ARE RISQUÉ BUSINESS
This holiday season will serve up some of the raciest footage yet on the upcoming releases of new computer and video console games. The offerings range from "Dead or Alive Xtreme Beach Volleyball," which offers buxom, scantily-clad volleyball players who "jiggle" realistically, to "BMX XXX," in which players rack up cash on the circuit and then get to spend it at a local strip joint, watching live-action footage of topless dancers. The BMX game also allows players to design their own topless biker characters, starting with chest measurements. "Consumers seem to be getting a little bored of a guy on a bike on a ramp," says Ben Fischbach, brand manager for Acclaim. "This product is a true comedic entertainment property. We really look at this game as 'American Pie' meets 'Airplane' meets 'Howard Stern.'" And while BMX XXX is rated "M" for players 17 and up, there are a number of other BMX games on the market now aimed at younger players, and the Parents Television Council worries that parents might grab it off the shelf without noticing the rating. In an effort to alert parents to the mature content, PTC has issued a warning about the game: "This may look like an ordinary biking game but it is the first sports game to carry an M rating and feature strippers, public urination, and yes? dog humping," reads the notice. (CNN/Money 17 Sep 2002)

VIDEO SEXXX GAMES
Video games are getting sexier and sexier. Industry analyst Michael Pachter says that sales of M-rated games (so-called "Mature" games) in the U.S. are expected to double this year from 7% overall to 14%, thanks to titles such as "BMX XXX," "The Getaway," and "Grand Teft Auto: Vice City," the last of which features interactive prostitutes whose services players can buy to boost their "health points." (Los Angeles Times 10 Oct 2002)
http://makeashorterlink.com/?U23112112

MAJOR RETAILERS WON'T SELL "ADULT" VIDEO GAMES
National retailers Wal-Mart, Toys R Us, and KB Toys have decided not to carry a new video game — BMX XXX — that features full-action nudity, prostitutes, and pimps, and is described by its creators as "a game of cultural sophistication and artistic aspiration." Wal-Mart executive Tom Williams says, "We're not going to carry any software with any vulgarity or nudity — we're just not going to do it." The chief executive of Acclaim Entertainment, the company that distributes the game, defends it as a spoof and says: "What we're doing here is funny." (Reuters/USA Today 16 Oct 2002)

Category 1B1 *Adult pornography*

2003-04-30 **P2P peer-to-peer file swapping music piracy**

NewsScan

FILE-SWAPPERS' DIRTY LITTLE SECRET
Despite the best efforts of the music industry, file-swapping services like Kazaa and Morpheus just keep getting bigger. But that doesn't mean music piracy is burgeoning out of control; instead, file-swappers increasingly are trading in smut. A February survey showed that 42% of all Gnutella users were seeking blue images and movies, a phenomenon that Greg Bildson, COO of LimeWire, a leading maker of Gnutella software, refers to delicately: "We're about all different kinds of content sharing." Wayne Rosso, president of Grokster, is a little more blunt: "P*rn — there's a ton of it being traded around." The surge in p*rn-trading has some smut-peddlers considering RIAA-type retaliations against the Gnutellas and Kazaas of the world. Like the movie executives, they blame the free services for their falling revenues. "The explosion of free p*rnography, fueled by file sharing, has diminished interest in pay sites," warns one veteran p*rn industry observer. Meanwhile, some businesses have taken a more collaborative approach. "We love file trading. Why? It's called greed. We've found a way to monetize that sharing," says the sales director for Triple X Cash. His company embeds hidden links in video clips and sends them out on file-sharing networks. When a file-swapper downloads a clip and clicks somewhere in the video's frame, he's taken to one of Triple X's sites. The company gets 25 to 40 "joins" — $30 monthly subscriptions — per day from this technique. "The record industry should have taken a cue from the p*ornographers," says Grokster's Rosso. (Wired.com 30 Apr 2003)

Category 1B1 *Adult pornography*

2003-05-29 **broadband internet pornography music consumer demand**

NewsScan

EUROPEAN BROADBAND GROWTH FUELED BY P*RN, MUSIC
High-speed Internet access growth is booming in Europe, boosted by consumer demand for music and p*rnography downloads, according to a new study by Nielsen/NetRatings. "The adult entertainment sector has increased its reach year-on-year in all European markets except Italy, where, not coincidentally, broadband access is the relative lowest in Europe," says the report. The biggest gains were in the UK, where broadband penetration has more than tripled to 3.7 million users. With only one in five Internet users opting for a broadband connection, however, the UK still remains second from the bottom in terms of percentages. France, Spain and the Netherlands head the top of the list, with 39%, 37% and 36% broadband penetration rates. In comparison, 35% of U.S. users connect via broadband, but the total number — 38 million — makes it No. 1 in the world in terms of sheer volume. (Reuters 29 May 2003)

Category 1B1 *Adult pornography*

2003-07-11 **pornography PC hijacking spread**

NewsScan

HAS YOUR PC BEEN HIJACKED TO SPREAD PORNOGRAPHY?
Computer security expert Richard M. Smith says that in the last month network vandals (possibly linked to Russian organized crime) have found ways to take over PCs with high-speed connections to the Internet and use them, without their owners' knowledge, to send Web pages advertising pornographic sites. Smith says that "people are sort of involved in the porno business and don't even know it." Most PC owners don't know when their computers have been hijacked and the hijacking apparently doesn't damage the computer or disrupt its operation. Because so many different machines are hijacked to perpetrate this scheme, there's no single computer that be shut down to end the problem. Smith adds: "We're dealing with somebody here who is very clever." (New York Times 11 Jul 2003)

Category 1B1 *Adult pornography*

2003-09-24 **MSN Microsoft misuse internet forums chat room pornography sexual predator activities**

NewsScan

MSN MUZZLES CHAT ROOMS
Microsoft MSN is closing down Internet chat services in most of its 34 markets in Europe, Latin America and Asia, and is limiting service in the U.S., citing concerns over use of the online forums for pornography scams and pedophile and sexual predator activities. "We recognize that it's a common industry-wide problem," says an MSN spokeswoman. "We've taken a look at our service and how can we make efforts to step up our efforts to provide a safe environment." In the U.S., MSN will now require chat room users to subscribe to at least one other paid MSN service, so that it will have credit card numbers that it can use to track down those who violate MSN's terms of use. In Canada, Brazil, New Zealand and Japan, MSN will offer some moderated chat rooms and discussions. The move to restrict chat use will probably turn out to be a good thing for the company, says one Microsoft watcher, by allowing it to shed a number of freeloaders. "I think this change will have welcome side effects, like keeping spammers out of the chat rooms. But fundamentally I believe this is a move to make MSN more profitable. It will allow the company to get rid of some infrastructure that was supporting chat, and to make money on what it leaves in place." (AP 24 Sep 2003)

Category 1B1 *Adult pornography*

2003-12-30 **net nudity pornography naked Nebraska Melissa J. Harrington public**

NewsScan

STOPPING NET NUDITY AT ITS SOURCE — IN LINCOLN, NEBRASKA
Since it's unlawful to be naked in public in Lincoln, Nebraska, that city's police chief ticketed 21-year-old Melissa J. Harrington for posting on her Web site photos "showing her naked at one of our downtown bars and in several other locations around the city." Harrington works as a Web designer at a local Bank and says that she likes "being naked in public... even more when there's a lot of people there to watch." The objectionable photos of the lady were taken inside the Marz Intergalactic Shrimp and Martini Bar, and the owner of the bar is the one who called the police to complain about the nude pictures. If convicted, Harrington faces a maximum penalty of six months in jail and a $500 fine. (AP/Los Angeles Times 30 Dec 2003)

Category 1B1 *Adult pornography*

2004-01-10 **pornography DVD HD-DVD Blu-ray high-resolution**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A62546-2005Jan10.html?nav=headlines

PORN DRIVES DVD TECHNOLOGY

Just as it has with other home entertainment technologies, pornography is proving a driving force in the future of high-definition DVDs. The multi-billion-dollar industry releases about 11,000 DVD titles a year, giving it a strong position in the debate over which technical standard -- Blu-ray or HD-DVD -- will dominate in next-generation DVDs. Analysts say currently, the smaller outfits are leaning toward HD-DVD because of its lower cost, while larger operations like Blu-ray's bigger storage capacity, which could be used for "creative expression" -- like giving viewers a choice of camera angles. Hollywood is also lining up on both sides of the battle, with Fox and Disney declaring their preference for Blu-ray and Warner Home Video siding with HD-DVD. But for now, everyone's kind of waiting around to see which format takes the lead. "We're kind of riding it out a little further to see where the trend goes," says an executive with leading porn producer Wicked Pictures. (Reuters/Washington Post 10 Jan 2004)

Category 1B1 *Adult pornography*

2004-02-08 **pornography porn digital piracy unworried intellectual property rights copyright**

NewsScan

PORN INDUSTRY VIEWS PIRACY AS 'DIRECT MARKETING'

The pornography industry takes a very different view of digital piracy than their counterparts in Hollywood and the music business — they're all in favor of it. "It's direct marketing at its finest," says Randy Nicolau, president of Playboy.com, who doesn't mind one bit that his magazine's pictures appear on thousands of other Web sites. When asked whether he thinks the entertainment industry is on the wrong track with their prosecution of online freeloaders, Nicolau says, "I haven't spent much time thinking about it. It's like asking Henry Ford, 'What were the buggy-whip guys doing wrong?'" And while the folks peddling porn may have a live-and-let-live attitude when their content gets ripped off, they show a different face when someone else is making money off of it. "We haven't gone after Joe Citizen who's sharing something he printed off something from the Hustler Web site with another guy," says a lawyer who represents Hustler on copyright issues — but he does send out about 20 letters a week to fee-based Web sites who are charging for his client's content. Meanwhile, another group, Titan Media, tracks down copyright violators and then offers them amnesty if they will become subscribers, an approach that may work for other content owners, says Wendy Seltzer, a staff attorney for the Electronic Frontier Foundation who calls it "a much more sensible approach" than the music industry's litigation strategy. "People always want this stuff. Seeing some of it just whets their appetite for more. Once they get through what's available for free, they'll move into the paid services." (New York Times 8 Feb 2004)

Category 1B1 *Adult pornography*

2004-03-09 **pornogrpahy porn industry business model innovative profitable Internet**

NewsScan

PORN: TRASH INTO CASH

It could be called high-tech's dirty little secret. Some of the Web's most innovative and profitable entrepreneurs are online pornographers, who for more than a decade have been among the first to exploit such new technology as video-streaming, fee-based subscriptions, pop-up ads, and electronic billing. In fact, porn is one of the most profitable online industries, and it's venturing into such new fields as wireless services and digital-rights management. One Internet porn entrepreneur started her business by posting to the Internet some photos she'd retrieved from a trash bin: "Technology turned trash into cash. That's a lesson other industries can learn." (USA Today 9 Mar 2004)

Category 1B1 *Adult pornography*

2004-05-14 **australia mobile porn Daryl Williams telecommunications watchdog adult content**

NewsScan

AUSTRALIAN CRACKDOWN ON MOBILE PORN

Risqué adult material will no longer be accessible to children using mobile phones in Australia, under new regulatory changes. Australian Communications Minister Daryl Williams said he had ordered the telecommunications watchdog to put in place new measures to protect hi-tech mobile phone users from offensive content. As part of the new measures, the Australian Communication Authority (ACA) will regulate access to content provided on new premium mobile phone services. "These new measures will help make access to the Internet and mobile communications services safer and more enjoyable for all Australians, particularly children," says Williams. "These controls will restrict access by children to adult content." (The Australian 14 May 2004) rec'd from John Lamp, Deakin University

---

Category 1B1 *Adult pornography*

2004-05-25 **porn offshore australian users phone bills dial-up services overseas lines providers**

NewsScan

PORN DUMPERS MOVE OFFSHORE

Some Australian Internet users are getting huge bills for phone calls to exotic overseas locations, as providers of Internet pornography move Internet dialing services offshore. Dial-up Internet users are disconnected from their Internet service provider and then reconnected without their knowledge to a premium overseas line. Charges are then split between the telcos and the content provider. Many embarrassed users claim to have been "dumped" — i.e., connected to a premium-rate call without being fully informed of the cost of the call. (The Australian 25 May 2004) Rec'd from John Lamp, Deakin U

Category 1B1 *Adult pornography*

2004-06-29 **online pornography law unconstitutional Supreme Court wary First Amendment**

NewsScan

SUPREME COURT WARY OF ONLINE PORNOGRAPHY LAW

The Supreme Court has ruled in a 5-4 decision that a law meant to protect children from exposure to online pornography is probably an unconstitutional restriction on free speech guaranties of the Constitution's First Amendment. The law, which passed in 1998 and was signed by then-President Clinton, is now backed by the Bush administration. Known as the Child Online Protection Act, the law would have authorized fines up to $50,000 for the crime of placing material that is "harmful to minors" within the easy reach of children on the Internet. The majority opinion, written by Justice Anthony M. Kennedy, said that "there is a potential for extraordinary harm and a serious chill upon protected speech" if the law were to take effect. The case has been sent back to a lower
court for a trial that would allow a discussion of what technology, if any, might allow children to be shielded from online pornography but at the same time would allow adults to see and buy any material that is not illegal. (AP/Washington Post 29 Jun 2004)

Category 1B1 *Adult pornography*

2004-08-17 **pornography study Australia sexuality children protection hard core**

NewsScan

NET-PORN IS GOOD FOR YOU, SAY ACADEMICS

Pornography is good for people, says the academic leading an Australian taxpayer-funded study of the subject. Alan McKee and his colleagues Catharine Lumby and Kath Albury are conducting the Understanding Pornography in Australia study. The Labor party is considering forcing Internet service providers to filter hardcore porn in order to protect children using home computers. McKee says: "The surprising finding was that pornography is actually good for you in many ways. When you look at people who are using it in everyday life, over 90% report it has had a very positive effect" because it had taught them to be "more relaxed about their sexuality," made them think about another person's pleasure, and made them less judgmental about body shapes. (The Australian 17 Aug 2004) Rec'd from John Lamp, Deakin U.

Category 1B1 *Adult pornography*

2004-08-25 **Geman police swap pornography e-mail law enforcement**

NewsScan

GERMAN POLICE ACCUSED OF E-MAIL PORN-SWAPPING

Two dozen German police officers suspected of using office computers to exchange pornographic messages. These activities were discovered by a maintenance technician who then reported them to his superiors. The police officers being investigated face possible disciplinary sanctions and could
be brought before a judge. (The Age 25 Aug 2004) Rec'd from J. Lamp

---

Category 1B1 *Adult pornography*

2004-10-25 **pornography wireless profit bandwidth**

NewsScan;
http://www.reuters.com/newsArticle.jhtml;jsessionid=TPZD2EKVY5JQSCRBAE
OCFEY?type=technologyNews&storyID=6600488

ADULT CONTENT TO BOOST WIRELESS WEB SERVICES

Analysts say porn purveyors will do the same thing for the wireless sector that they did for the fixed-line Internet, fueling major growth while raking in the bucks. In the U.S., consumers will shell out some $90 million for adult entertainment in four years' time, according to a report by Yankee Group, which estimates that excluding portals of U.S.- based wireless operators, half of all wireless data traffic consists of pornography. Meanwhile, the only thing holding back the U.S. carriers is the worry over a backlash if adult content falls into the hands of children: "Fear is trumping greed for the moment, but the two can work together if carriers can develop a solid mechanism for protecting minors and safely profit from the opportunity," says Yankee. (Reuters 25 Oct 2004)

Category 1B1 Adult pornography

2004-11-22 **pornography Google copyright images piracy search engine lawsuit**

NewsScan; http://www.wsj.com/

ADULT-ENTERTAINMENT GROUP SUES GOOGLE

In a federal lawsuit filed against Google, the adult-entertainment firm Perfect 10 Inc. is charging that Google's search engine has been displaying copyrighted images from Perfect 10's magazine and Web site, along with passwords to its subscription Web site, in response to user queries. The company says that Google's computers retrieve the passwords and images (mainly photos of female models) not from Perfect 10's own site but from other sites that have pirated them; charging that it would be "virtually impossible" for consumers to locate the stolen content if Google didn't direct them to it, its complaint accuses Google of "putting them on their servers knowing in most cases these pictures are unauthorized." Google has not yet responded to the complaint. (Wall Street Journal 22 Nov 2004)

Category 1B1 Adult pornography

2006-02-01 **spam anti-spam conviction unsolicited pornographic e-mail CAN-SPAM**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/story/0 23 ,10801,108267,00.html?SKC=security−108267

CONVICTION SECOND-EVER FOR TRANSMISSION OF OBSCENE E-MAIL MESSAGES.

A California man accused of managing the computer system to send hundreds of thousands of pornography-related e-mail messages has pleaded guilty to violating a U.S. antispam law. Kirk F. Rogers of Manhattan Beach, CA, pleaded guilty in U.S. federal court in Arizona Tuesday, January 31, to violating the U.S. CAN-SPAM Act, according to the U.S. Department of Justice (DOJ). Rogers' plea is the second-ever U.S. conviction related to the transmission of obscene e-mail messages, the DOJ said. Rogers agreed to forfeit money obtained in his spamming operation and faces a maximum sentence of five years in prison for a one-count violation of CAN-SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing Act). Sentencing is scheduled for June 5.

1B2 Child pornography

Category 1B2 *Child pornography*

1997-01-14 **child pornography arrests police investigation privacy**

EDUPAGE

EDUPAGE reports: >Ontario police have charged several people with downloading child pornography off the Internet. The police refuse to reveal the techniques they use to build cases against people caught with huge stockpiles of child porn, and defense lawyers and legal experts say constitutional issues surrounding the state's right to monitor a person's private computer will surface as the cases come to court. Defense lawyer Marie Henein finds it "a little frightening" that you could be sitting at your computer at home while the police are assessing what you're doing. She and another lawyer represent an Ontario man charged with distributing child pornography on the Internet after police seized 20,000 computer files containing photos and video clips. (Montreal Gazette 13 Jan 97 A5)<

Category 1B2 *Child pornography*

2000-01-17 **child pornography kiddie porn vigilante legal action criminal hacker vandalism destruction evidence law enforcement**

Computerworld

In mid-December 1999, a group of activists and technology experts formed Condemned.org, dedicated to eradicating child pornography, pedophile sites and child exploitation on the Internet. The group uses legal means such as notifying law enforcement and system administrators of the presence of child porn on their servers; most immediately terminate the accounts responsible. However, the group warns, if there is no action taken, some of the members turn to illegal tactics. In such cases, members will hack into vulnerable sites and wipe entire hard drives. Some opponents of child pornography protest that these illegal methods destroy the evidence needed by law enforcement to locate and prosecute malefactors.

Category 1B2 *Child pornography*

2000-11-16 **pornography fraud children trickery metatags**

NewsScan, Financial Times http://news.ft.com/news/industries/media

[In November, an article in the Financial Times reported that pornographers were] using "metatags," the labels attached to Web pages that identify their contents, to draw visitors seeking information on the holiday season's most popular toys, with the result that children surfing the Web for My Little Pony, Barbie or Muppets could find among their choices not only toy retailers but such sites as www.picturesofanalsex.com. Envisional, a UK company that specializes in searching the Net for trademark violations, said it has found nearly 12,000 examples of toy names being used this way. A British attorney noted that using registered trademarks in this way is illegal, as is using metatags to drive children toward obscene material, but that such laws were difficult to enforce, given the worldwide reach of the Internet. (Financial Times 16 Nov 2000)

Category 1B2 *Child pornography*

2001-03-27 **child pornography international investigation arrests**

NewsScan

ARRESTS FOLLOW RAID ON RUSSIAN CHILD PORN SITE
Operation Blue Orchid, a joint criminal investigation by Moscow city police and the U.S. Customs Service, has shut down a Russian child pornography Web site and brought about the arrest of nine people, with more under investigation. Four people have been arrested in the U.S. and 15 search warrants have been issued. The site sold videotapes of children participating in sexual acts. (AP/USA Today 26 Mar 2001)
http://www.usatoday.com/life/cyber/tech/2001-03-26-net-porn.htm

---

Category 1B2 *Child pornography*

2001-08-08 **child pornography investigation Web international indictment**

NewsScan

CRACKDOWN ON INTERNET CHILD PORNOGRAPHY [8 Aug 2001]
More news about the world of netporn: A two-year investigation by the U.S. Postal Inspection Service and other federal agencies has resulted in the indictment of subscribers to a child porn site operated by a Texas couple charged with running the largest commercial child pornography business ever uncovered. The couple provided a credit card verification service that, for $29.95 a month, let customers visit sites that offered graphic pictures and videos of children engaging in sex acts with adults and with each other. The sites were operated by webmasters in Russia and Indonesia. (AP/USA Today 8 Aug 2001)
http://www.usatoday.com/life/cyber/tech/2001-08-08-child-porn.htm

---

Category 1B2 *Child pornography*

2002-07-10 **child pornography investigation arrests**

NewsScan

FBI ARRESTS 10 IN INTERNET CHILD PORN INVESTIGATION
Among those in Manhattan and Brooklyn arrested by the FBI yesterday in its ongoing "Operation Candyman" investigation of Internet child pornography were a U.S. Army sergeant, two former NYC police officers, a subway conductor, a construction company owner, and a retired firefighter. If convicted, they will face up to five years in a federal prison. A government official said: "As you can see, those who collect and receive images of sexual abuse of children are not nameless faces lurking in cyberspace, nor are they shadowy figures leering in a dark alley. But they come from every cross-section of our society and both our urban and suburban neighborhoods." The porn site made available to its members images of real children 12 and under having sex with adults. (New York Times 10 Jul 2002)
http://partners.nytimes.com/2002/07/10/nyregion/10PORN

Category 1B2 *Child pornography*

2003-03-14 **child pornography arrests international**

NewsScan

INTERNET CHILD PORN ARRESTS CONTINUE IN BRITAIN
British law enforcement officials have arrested 43 more men on suspicion of having downloaded child pornography from U.S. porn sites. The officials are working their way through a list (obtained some months ago from U.S. postal investigators) of 7000 British subjects who used their credit cards to enter the sites. Out of the 1,600 individuals arrested in London, 46 have allegedly been directly involved in the abuse of children. A British police official says: "We are sending out a strong warning to those who think they can remain anonymous and escape the law by using the Internet to access abusive images of children." (The Inquirer (UK) 13 Mar 2003
http://www.theinquirer.net/?article=8299

Category 1B2 *Child pornography*

2003-06-13 **spammers target users' pc hijacking microsoft vulnerability MessageLabs windows**

NewsScan

SPAMMERS TARGET USERS' PCs
Security experts at UK firm MessageLabs say that a "trojan virus" mailed to up to 1 million computer users last week was designed to exploit a vulnerability on Windows PCs that would enable the perpetrator to use the recipients' PCs to distribute ads for Web sites carrying incest pornography. Internet security experts have suspected for some time that spammers would use viruses to access third-party computers, but MessageLabs says their investigation offers the first conclusive proof. "This is a massive discovery. It completely undermines the spammers' claim that they are legitimate marketers and shows that they are nasty insidious hijackers who drive me and the vast majority of computer users nuts," says MessageLabs senior technologist Matt Sergeant. The virus targeted a feature known as open proxy, which is often installed by software companies as the default setting on home PCs. Proxy servers are designed to allow the machine to link to the Internet through a local network, but if left open, they provide a back door for computer crackers to hijack the machine. The incident last week targeted customers of Outblaze, a Hong Kong-based webmail company that has about 30 million customers worldwide and owns domain names such as usa.com. "Open proxies are becoming the spammers' lifeline so they are always looking for more. Now we know how they are going about it," says Sergeant. (The Guardian 13 Jun 2003)

Category 1B2 *Child pornography*

2003-09-03 **mousetrapping website disney children porn sites thousand inernet addresses**

NewsScan

MAN ARRESTED FOR 'MOUSETRAPPING' CHILDREN
Federal agents have arrested a Florida man they say runs Web sites that exploit misspellings by computer users to redirect children looking for Disneyland or the Teletubbies to explicit porn sites instead. The government say it is the first prosecution under a provision of the new Amber Alert legislation that makes it a crime to use a misleading Web address to draw children to pornography. The man registered thousands of Internet addresses and was earning up to $1 million per year off them — much of it from sites that paid him when he sent Web users their way. The redirection technique is called "mousetrapping." U.S. Attorney James Comey said: "Few of us could imagine there was someone out there in cyberspace, essentially reaching out by hand to take children to the seediest corners of the Internet." (San Jose Mercury News 3 Sep 2003)

Category 1B2 *Child pornography*

2003-09-04 **ICANN lawmakers pornography scammers stolen credit cards registering**

NewsScan

ICANN TAKES HITS FROM LAWMAKERS
Rep. Howard Berman (D-Calif.) is critical of ICANN (the Internet Corporation for Assigned Names and Numbers) for not doing enough to stop scammers and child pornographers from registering under false names with stolen credit cards: "I'm disappointed with the failure of the marketplace and regulators to deal with this problem. A legislative solution seems necessary." And Rep. Lamar Smith (R-Texas) agrees: "There's not a real seriousness of intent either by ICANN or the Department of Commerce to have an accurate whois database." Commerce Department General Counsel Theodore Kassinger says that ICANN is busy working on solving the problem. (Reuters/USA Today 4 Sep 2003)

Category 1B2 *Child pornography*

2004-01-05 **Child pornography John B Martin sex offender internet**

NewsBits;
http://www.zwire.com/site/news.cfm?BRD=1302&dept_id=181981&newsid=10738256&PAG=461&rfi=9

Supreme Court upholds convictions for child pornography

John B. Martin, 64, of Belle Fourche, South Dakota, was convicted in 2002 of having child pornography on his office and home computers; he claimed that his three-year project of collecting pornography was an attempt to provide evidence for new anti-porn laws. Records showed no attempts to contact government or law enforcement on this subject. He was sentenced to 90 days in local prisons in lieu of several years in federal prison. In his appeal against this sentence, his attorneys argued that the child pornography laws were unconstitutional because their overly-broad language could forbid ownership of digitally-created or modified images that did not in fact involve real children. In a decision on his appeal, the Supreme Court of the United States (SCOTUS) ruled unanimously that "the laws did not violate the U.S. Constitution, did not improperly restrict free speech and gave Martin adequate notice of what activities were illegal."

Category 1B2 *Child pornography*

2004-01-05 **Child pornography Roger Jacobs internet prostitution**

NewsBits;
http://rockymountainnews.com/drmn/local/article/0,1299,DRMN_15_2547407,00.html

Appeals court rules child-porn term unjustified

The state Court of Appeals vacated the sentence of a man convicted in an Internet child-porn case, ruling his term of 25 years to life was not warranted. The court said Wednesday there wasn't enough evidence to justify an indeterminate sentence for Roger Jacobs, convicted of two counts of soliciting for child prostitution. Jacobs was convicted after a California detective set up an Internet site offering "very young, very attractive escorts," and Jacobs, who lived in Westminster, responded. The detective sent Jacobs a picture of a girl and told Jacobs she was 12 years old. Jacobs sent the detective a picture of himself and the type of girl with whom he would like to have sex.

Category 1B2 *Child pornography*

2004-01-05 **child pornography Alfred Wayne Velasquez sexual assault internet**

NewsBits;
http://www.wfaa.com/localnews/stories/010104dnmetvelasquez.4b50f.html

Fort Worth man makes plea deal in sex case

A 36-year-old Fort Worth man suspected of having sex with underage girls he met through the Internet has struck a deal with Tarrant County prosecutors that includes an eight-year prison sentence. Alfred Wayne Velasquez pleaded guilty last month to sexual assault of a child for having sex with a 14-year-old Arlington girl in September 2001 at her house while her parentsere away. Mr. Velasquez has been indicted on similar charges in Johnson and Collin counties. Plea agreements are likely in those jurisdictions, but nothing has been finalized, officials said. Mr. Velasquez was being held in the Tarrant County jail in lieu of $225,000 bail.

Category 1B2 *Child pornography*

2004-01-13 **child sex case nude photogragpy pornography Stephen Wilson**

NewsBits;
http://www.fayettevillenc.com/story.php?Template=local&Story=6115863

Suspect in child-sex case arrested on new charges

A Fayetteville, NC man faces a second round of charges that he possessed nude photographs of girls as young as 12. Stephen Wilson, 28, was charged in early January with first-degree sexual exploitation of a minor. According to an arrest warrant, girls posed for Wilson "in a sexual manner" as he photographed them with a digital camera. Sheriff's Detective J. Stallings said in a magistrate's document that Wilson downloaded the photos onto his computer. Stallings said a forensic pediatrician examined the images and estimated the unknown girls to be 12 or 13. "Mr. Wilson also admitted to downloading pictures from the Internet of teenage girls for his own curiosity," Stallings said.

Category 1B2 *Child pornography*

2004-01-16 **child pornography pedophilia**

NewsBits; http://wildcat.arizona.edu/papers/97/75/01_1.html

Student charged in child porn case

A UA student has pled guilty to charges of downloading child pornography and sharing the material over the Internet while he lived in a campus residence hall last fall, officials said. Donilo Phillip Colich, 20, was charged with one count of attempted sexual exploitation of a minor under 15, a class 2 felony, according to UAPD Sgt. Eugene Mejia. Colich, originally indicted on 11 counts, received 10 years of probation last week, which includes no access to children and the Internet. He will also have to register as a sex offender, said Assistant County attorney Kathleen Mayer. On Nov. 12, 2002, an unknown person from Switzerland notified the UA webmaster that Colich had been using the KaZaA file-sharing program to download child pornography in his room in the Manzanita-Mohave Residence Hall, 1010 NewsBits; . Park Ave. The webmaster notified the computer management division on campus, which was able to trace the files back to an IP address that corresponded to Colich's computer.

Category 1B2 *Child pornography*

2004-01-20 **internet pornography probe charges child**

NewsScan

PORN PROBE

Officers investigating child porn have identified nearly 250 residents across the region who have accessed indecent websites. The figures are being discussed by Hampshire Police Authority at a meeting today. Panel members will be told that Operation Danforth is still a major commitment to the force, with 238 residents of Hampshire and the Isle of Wight identified as accessing websites containing indecent images of children. There's also a warning that on-line storage, encryption and file sharing are making the police's investigations more difficult.

Category 1B2 *Child pornography*

2004-01-21 **child pornography sentence Clifford James Robinson**

NewsBits; http://www.nzherald.co.nz/latestnewsstory.cfm?storyID=3544951

Jail term for child porn trader pleases investigators

Child pornography investigators are pleased with the jail term handed down to a Christchurch New Zealand, man yesterday for copying and possessing images of adults sexually abusing children, incest and bestiality. The Internal Affairs Department polices illicit publications, including images traded on the internet. Clifford James Robinsin, 38, was jailed in January for seven months for trading a three-minute movie of a baby girl being sexually abused and 22 other charges relating to objectionable images, transcripts, and movies.

Category 1B2 *Child pornography*

2004-01-21 **Christopher Wade Ooms child pornography plead**

NewsBits;
http://www.swtimes.com/archive/2004/January/21/news/child_porn.html

Van Buren Man Gets Probation In Child Porn Case

A Van Buren man accused of using his neighbor's computer to surf the Internet in search of child pornography has been sentenced to probation. Christopher Wade Ooms, 20, pleaded no contest Tuesday to one count of pandering or possessing visual or print medium depicting sexually explicit conduct involving a child. Ooms was arrested in April after a neighbor contacted police and said that she found sexually explicit material on her computer after Ooms used it.

Category 1B2 *Child pornography*

2004-01-22 **child pornography distribution**

NewsBits; http://www.southbendtribune.com/stories/2004/01/15/local.20040115-sbt-MARS-A2-Prosecutor_s_staff_g.sto

Indiana Prosecutor's staff goes after child pornography on Net

An undercover investigation by the St. Joseph County, IN prosecutor's office has identified 26 people around the world suspected of possessing or distributing child pornography on the Internet. The monthlong investigation resulted in the seizure of more than 10,000 images and movies portraying child pornography, officials reported. During the operation, Mitch Kajzer, an investigator in the prosecutor's office, posed on the Internet as someone who wanted to trade child pornography files, said Prosecutor Michael Dvorak. In just one month, more than 100 people approached Kajzer wanting to download child pornography and Kajzer traded with 39 of them. Twenty-six of those people now face criminal charges such as child exploitation, possession of child pornography and distribution of child pornography.

Category 1B2 *Child pornography*

2004-01-30 **child pornography Boy Scout volunteer teacher Maxwell**

NewsBits

NJ Substitute Teacher Accused Of Possessing Child Porn

A 53-year-old substitute teacher and Boy Scout volunteer was arrested and charged with possession of child pornography, federal authorities said. John Maxwell of Clifton was released Thursday after posting $100,000 in unsecured bonds, said Brett Dreyer, a spokesman for the U.S. Immigration and Customs Enforcement agency. The criminal complaint, filed in U.S. District Court in Newark, alleged that Maxwell downloaded more than 100 pornographic images onto his personal computer from the Internet. Federal authorities seized the computer and other evidence during a search of Maxwell's home in January, authorities said in a statement.

Category 1B2 *Child pornography*

2004-01-30 **Child Pornography county sherrif Gary Penrod Vertican**

NewsBits;
http://www.dailybulletin.com/Stories/0,1413,203%7E21481%7E1921248,00.html

Suit against sheriff cost county $50,000

The federal lawsuit filed against San Bernardino County Sheriff Gary Penrod and two others cost taxpayers $50,000 to defend only to be dropped by the plaintiff under a settlement before it went to trial. Gary Vertican's $60 million lawsuit filed in U.S. District Court in Riverside against Penrod, sheriff's Detective Michael DiMatteo and Probation Officer Melinda Carpenter on Feb. 24 disintegrated for lack of evidence, attorneys for both sides said Tuesday. In the lawsuit, the former Twin Peaks resident accused DiMatteo of planting evidence of child pornography on computer disks seized with a warrant from Vertican's home in February 2002.

Category 1B2 *Child pornography*

2004-01-30 **Kelly child pornography trial evidence search seizure**

NewsBits;
http://www.theledger.com/apps/pbcs.dll/article?AID=/20040130/NEWS/401300
393/

Judge to Rule On Evidence in Illinois Child Porn Case

Lawyers for R&B star R. Kelly, who is facing child pornography charges in Polk County and Chicago, have asked a judge to throw out key evidence in the singer's local case, arguing it was seized during an illegal search. In a motion filed last week, Bartow lawyer Ron Toward argued that prosecutors should not be allowed to use the evidence, including a digital camera that investigators said contained 12 nude pictures of an underage girl. The evidence was seized during what Toward described as an illegal search of one of two houses Kelly was renting in the Ridgewood Lakes subdivision near Davenport in June 2002.

Category 1B2 *Child pornography*

2004-02-27 **child pornography Europe raids arrests Internet**

NewsScan

CHILD PORN RAIDS IN TEN EUROPEAN COUNTRIES

Interpol, the European Union police agency, says that coordinated police raids in 10 countries have broken a number of Internet child pornography networks and arrested people in more than 40 locations. The main focus of the raids were in Wiesbaden, Germany, but other countries where raids took place were Australia, Belgium, Canada, the Netherlands, Norway, Peru, Spain, Sweden and Britain. (Los Angeles Times 27 Feb 2004)

Category 1B2 *Child pornography*

2004-09-20 **child pornography Switzerland police arrest**

NewsScan

SWISS POLICE ARREST TEN OVER CHILD PORN

Swiss police have arrested 10 people and carried out about 400 searches in a massive nationwide operation against international child pornography networks operating in Switzerland. Swiss Federal Police say they seized large quantities of material including computers during the ten-day swoop,
which was prompted by investigations into child porn websites in the United States. Another 120 countries are concerned by the probe, which follows on from a similar international operation in 2002. (The Age 20 Sep 2004) Rec'd from J. Lamp

---

Category 1B2 *Child pornography*

2004-09-30 **child pornography Australia international global warrants credit cards**

NewsScan; http://theage.com.au/articles/2004/09/29/1096401645228.html

CHILD INTERNET PORN RING SMASHED

Australian police and U.S. FBI agents have smashed a global Internet child pornography ring, with hundreds of search warrants issued on properties throughout Australia. Though it's often difficult to catch Internet child porn users, some of the perpetrators used their own credit cards to gain access to illegal images.

1B3 Pedophilia, kidnapping, Net-adoption fraud

Category 1B3 *Pedophilia, kidnapping, Net-adoption fraud*

1997-01-09 **child pornography rape arrest**

DPA

In Solothurn, Switzerland, police arrested a 37-year-old child molestor who had spread tens of thousands of pictures on the Internet with pornographic representations involving children. The paedophile computer-expert confessed, the authorities said in Solothurn. According to police statements, the 37-year-old abused numerous girls in Cambodia in a massive misuse and recorded this on video. The police found more than 100 corresponding photos in the Internet.

Category 1B3 *Pedophilia, kidnapping, Net-adoption fraud*

2000-06-09 **children pedophiles attacks kidnap parental responsibility abduction infants**

NewsScan

Child safety experts warned the U.S. congressional committee on child online protection . . . [on 8 June] that with the average of age of online users declining, children increasingly are put at risk by their careless or ignorant online activities. Parry Aftab, a children's advocate, told committee members that 3,000 children were kidnapped in the U.S. last year after responding to online messages posted by their abductors. A recent survey of teenage girls found 12% had agreed to meet strangers who'd contacted them online. Children between the ages of two and seven are among the fastest growing user cohorts. (Financial Times 9 Jun 2000)

Category 1B3 *Pedophilia, kidnapping, Net-adoption fraud*

2000-08-03 **pedophile statutory rape conviction sentencing**

San Jose Mercury News

Patrick Naughton, a former executive of the INFOSEEK online company, pled guilty in March 2000 to having crossed state lines to commit statutory rape of a child. Since then, said FBI officials, he has been providing help in law enforcement investigations of pedophilia on the Net. In return for his cooperation, prosecutors asked the court for five years of probation (instead of a possible 15 years in prison), counseling, a $20,000 fine (instead of the maximum $250,000) and an agreement not to have "unapproved" contact with children and to stay out of sex-chatrooms online.

Category 1B3 *Pedophilia, kidnapping, Net-adoption fraud*

2002-10-31 **Web logs blogs children hysteria evidence**

NewsScan

CHILD SAFETY ON THE WEB
The Internet personal diaries known as Blogs (or, more formally, Web logs) are providing the latest source of concern to parents and educators worried about the safety of children on the Net; author Jean Amour Polly says: "The Internet has moved on into new territory. Strangers can comment on the diaries and even e-mail kids advice and comfort." But criminologist David Finkelhor, who studies Internet crime and teaches at the University of New Hampshire, warns against hysteria on the subject: "There are new perils for kids, but no evidence that kids are on the whole more endangered today as a result of the Internet. There's no sign of an incredible tidal wave of mayhem and danger that's washed onto our shores." (New York Times 31 Oct 2002)

Category 1B3 *Pedophilia, kidnapping, Net-adoption fraud*

2003-01-07 **pedophiles Internet chat rooms children victims confidence tricksters warning education advertising**

NewsScan

U.K. EFFORT TO CONTROL CHAT-ROOM PEDOPHILES
The British Home Security Office has launched a major advertising campaign to alert children and parents to the dangers of pedophiles who use the Internet to "groom" a young victim by spending many months gaining the child's confidence in chat rooms and e-mail. Home Office minister Hilary Benn said: "Parents can play a role in making their children aware that strangers on the Internet may not always be who they say they are. The messages to children are clear: do not give out personal contact details online and never meet up with someone you have met online unless accompanied by an adult." (The Enquirer, UK, 6 Jan 2003)
http://www.theinquirer.net/?article=7048

Category 1B3 *Pedophilia, kidnapping, Net-adoption fraud*

2003-11-25 **spam unsolicited junk e-mail message Amber Alert Rebecca Mercuri**

RISKS 23 4

Amber Alert, Coming to the Inbox Nearest You

Rebecca Mercuri warns about a new kind of spam--Amber Alert. She writes, "[T]his one promises to clog your email box with photos of children who may or may not have vanished, probably for years even after they've (hopefully) been found." Because of the possibility of emotional involvement with the message in the spam, Mercuri says the best way to combat Amber Alerts is to "immediately redirect all messages with the subject phrase "Amber Alert" into your trashbin…"

Category 1B3 *Pedophilia, kidnapping, Net-adoption fraud*

2004-01-05 **child exploitation sexual contact pedophilia David Gipson Jr.**

NewsBits; http://www.cincypost.com/2004/01/03/briefs01-03-2004.html

Man held on sex charge

A North College Hill man has been arrested and charged with unlawful sexual contact after authorities said he tried to solicit sex from a 14-year-old female on the Internet. The minor was in fact a detective with the Regional Electronic and Computer Investigations, which is made up of deputies, officers and detectives from the Cincinnati police department and Hamilton County Sheriff's Department. David Gipson Jr., 32, was arrested in Sycamore Township on Monday and charged with one count of attempted unlawful sexual contact with a minor and one count of importuning. Authorities arrested Gipson at the location he designated to meet the girl.

Category 1B3 *Pedophilia, kidnapping, Net-adoption fraud*

2004-01-13 **underage sexual assault internet pedophile Nicholas Ardent cyber sting exploited child**

NewsBits;
http://www.greenbaypressgazette.com/news/archive/local_14141664.shtml

Green Bay, Wisconsin Area man charged in child-sex sting

A 22-year-old De Pere man was arrested Saturday after he allegedly arranged to have sex with 10- and 12-year- old girls while their father watched. However, hat father turned out to be special agent Eric Szatkowski of the state Department of Justice Division of Criminal Investigation. Nicholas Arendt now faces two counts of attempted sexual assault of a child under 13. Szatkowski zeroed in on Arendt after a complaint was filed with the cyber-tip line of the National Center for Missing and Exploited Children. According to the criminal complaint filed Monday in Brown County Circuit Court, Szatkowski first posed as the father of two young girls, ages 10 and 12, in an Internet chat room and agreed to bring his children to Arendt's Morning Glory Road apartment for sex.

Category 1B3 *Pedophilia, kidnapping, Net-adoption fraud*

2004-01-14 **pedophile internet stalking police investigation prosecution sentencing**

NewsBits; http://www.smh.com.au/articles/2004/01/15/1073877933063.html

University student first to be sentenced over internet porn

An Australian university graduate is facing jail under tough new Queensland laws aimed at catching pedophiles preying on children in internet chat rooms. Matthew William Ross Kennings will be the first person sentenced under the laws next month after pleading guilty in the District Court in Brisbane yesterday. The 26-year-old refugee centre volunteer was charged in July last year with intending to procure a person he believed to be under 16 years old to engage in a sexual act. The new laws were introduced two months beforehand, with police and the state's Crime and Misconduct Commission setting up a joint operation to target offenders. Kennings was caught after making contact with one of the officers who was posing as a 13-year-old girl using the name BeckyBoo13 in internet chatroom MSN Whisper.

Category 1B3 *Pedophilia, kidnapping, Net-adoption fraud*

2004-01-14 **net prowler laws legislation Jeff Denham**

NewsBits; http://www.modbee.com/local/story/8003223p-8870893c.html

California Legislation to fight Net prowlers halted

An effort by Sen. Jef f Denham, R-Merced, to better nab Internet child-sex prowlers died in a committee hearing Tuesday when not enough senators showed up to vote. California Senate Bill 882 failed on a 2-0 vote in the Senate Public Safety Committee. The bill needed a majority, or four votes, to move out of the six- member panel. Denham expressed disappointment that his bill died because of procedural rules. A similar effort passed out of the same committee two years ago but later stalled.

Category 1B3 *Pedophilia, kidnapping, Net-adoption fraud*

2004-01-20 **child molester pedophilia internet**

NewsScan

CONVICTED CHILD MOLESTER ACCUSED OF SECOND CRIME

A former Fort Hood soldier has been convicted in Montague for stalking a 14 year old Bowie girl after meeting her on the Internet. While out on bond on that charge, he was arrested for allegedly trying to solicit sex with a 15 year old girl in Bastrop county. That girl turned out to be an attorney general cyber crime unit investigator.

Category 1B3 *Pedophilia, kidnapping, Net-adoption fraud*

2004-01-21 **internet child stalking sex offender pedophilia**

NewsBits; http://www.thestate.com/mld/thestate/news/local/7762250.htm

SC Attorney General pushes to outlaw Internet child stalking

A bill that would make enticing children using the Internet illegal in South Carolina was unanimously approved Wednesday by a SC House subcommittee. If passed by legislators, it would be the first law in the state barring adults from luring children to have sex or commit crimes. The bill makes it easier to prosecute these crimes by expanding the state grand jury's authority to investigate them, state Attorney General Henry McMaster said. Sexual cybercrimes often cross state lines because the Internet enables predators to contact children in practically any part of the world.

Category 1B3 *Pedophilia, kidnapping, Net-adoption fraud*

2004-01-21 **sex abuse internet solicitation pedophilia child pornography John McPartland**

NewsBits; http://www.katu.com/news/story.asp?ID=63779

Oregon teacher investigated on sex abuse charges

A teacher and coach at a middle schol in Gresham, OR is on administrative leave after his arrest by the FBI and local police on charges of trying to use the Internet to solicit a boy for sex. The "boy" was actually an undercover federal agent. Agents arrested 42-year-old John McPartland Friday at his apartment. He is a math teacher and basketball coach at Clear Creek Middle School. The investigation was done by the FBI's Innocent Images Task Force, which focuses on child pornography and people who use the Internet to prey on children. District plans sexual predator training.

Category 1B3 *Pedophilia, kidnapping, Net-adoption fraud*

2004-01-21 **pedophile sting Gudzyk**

NewsBits; http://www.mcall.com/news/local/all-b3_1cyberpervjan10,0,4631594,print.story

Pennsylvania man busted in online pedophile sting, police say

A 49-year-old Carbon County, PA man who used the Internet to arrange a sexual tryst with what he believed was 12-year-old girl sped off from a store when he saw he was about to be arrested, and was stopped only after a detective fired bullets into the car, according to court documents. No one was injured. Ernest R. Gudzyk of 3 Spring Valley Farms, Weatherly, was arrested when he drove up to a King of Prussia grocery store where he had arranged to meet the girl, actually a Montgomery County detective posing as a child to catch online pedophiles, the documents said.

Category 1B3 *Pedophilia, kidnapping, Net-adoption fraud*

2004-01-23 **sex offender registration California**

NewsBits; http://www.mercurynews.com/mld/mercurynews/news/local/7778004.htm

Sex offender data posting gains support

Prospects for Californians to get better information about registered sex offenders living among them are the strongest they have ever been, after sharp scrutiny of the state's Megan's Law. After years of failed efforts, state leaders say they are optimistic about passing legislation to put the names, photographs and exact addresses of high-risk sex offenders on the Internet. A Mercury News investigation last month showed that most states already provide that information online, while California clings to a system that is one of the most restrictive and error-riddled in the country.

Category 1B3 *Pedophilia, kidnapping, Net-adoption fraud*

2004-01-30 **sexual abusers sentencing Salazar pedophilia criminal record seduction Internet**

NewsBits; http://www.tecrime.com/llartL06.htm

Sexual abusers of children often get deals, no convictions

Manny Garcia and Jason Grotto wrote a report for the Miami Herald about the variable prosecutions of men caught seducing minors into sexual relations. In one case, 20-year-old Alan Salazar was arrested in Houston after arranging for a 14-year-old Dania Beach, FL teenager to fly to Texas. The perpetrator "pleaded no contest to interfering with the custody of a minor, [but] a Broward County judge withheld adjudication, meaning Salazar can say he has never been convicted of a crime." According to research by the newspaper staff, most of the Internet seduction cases end up without convictions even though the criminals plead guilty or no contest; about 80% of the child pornographers arrested in the state have their convictions erased from their criminal records. "Investigators blame the Florida Criminal Punishment Code, which scores some Internet sex crimes no worse than writing a bad check at the grocery store." Defense attorneys claim that their clients did not know that their victims were minor; some accuse police of entrapment when the officers impersonate children online.

Category 1B3 *Pedophilia, kidnapping, Net-adoption fraud*

2004-06-09 **Internet chat room pedophiles monitor joint efforts**

NewsScan

PATROLLING INTERNET CHAT ROOMS

Law enforcement agencies in Britain, Australia, Canada and the U.S. are planning joint patrols of Internet chat rooms in search of pedophiles. Their hope is to establish a "24/7 police presence on the Internet." Jim Gamble of the UK's National Crime Squad says: "We're looking to put a police presence on the Internet in an overt way that reassures people." The four countries plan to develop a "simple visible logo" to indicate police presence in a chat room, and Gamble explains: "I don't think we're talking about devoting massive numbers to this… People feel safer when police are present, it's as simple as that. There is no Big Brother initiative here, this is about reassurance through visibility." (AP/Los Angeles Times 9 Jun 2004)

Category 1B3 *Pedophilia, kidnapping, Net-adoption fraud*

2004-07-19 **Web alert system Amber child abduction kidnapping monitor thwart**

NewsScan

AMBER ALERT COMES TO THE WEB

The nation's Amber Alert system will be connected to the Web starting today, making it easier for that system to thwart child abductions by transmitting messages about child abductions. An executive of the company that designed the Amber Alert portal says: "The tag line on all this is, 'We'll all be looking for you.' This unbelievable technology is going to make that possible." Speed is considered vital in recovering an abducted child. The Justice Department estimates that three of every four victims are killed within three hours of being taken. (USA Today 19 Jul 2004)

Category 1B3 *Pedophilia, kidnapping, Net-adoption fraud*

2005-05-22 **pedophiles police children parents Internet chat guidance warnings assault rape**

http://www.news-journalonline.com/NewsJournalOnline/News/Headlines/03NewsHEAD03052205.htm

INTERNET PEDOPHILE PREDATORS OFTEN UNPUNISHED

A report in the Daytona Beach News Journal Online summarizes police experience with pedophile predators. These adults prey on pre-teens and early teens, especially young girls. The number of predators is so high that police officers in training who pose as thirteen-year-old girls cannot keep up with the number of instant-messaging solicitations they receive within minutes to hours of going online. Police urge parents to get involved in their children's online experience and not to be punitive if children report inappropriate behavior by someone they have met online.

Http://www.news-journalonline.com/NewsJournalOnline/News/Headlines/03NewsHEAD03052205.htm

[MK adds: see the booklet "Cyber-safety for All" available free at
http://www2.norwich.edu/mkabay/cyberwatch/cybersafety.pdf
Anyone may make copies of this guide for free distribution.]

1B4 Stalking & harassment

Category 1B4 *Stalking & harassment*

1997-04-01 **anonymity stalking harassment threats free speech law**

AP

John Hendren,writing for AP, reported in April on several cases of cyber-harassment. An Annapolis, MD woman was mail bombed after she warned other writers about extortionate fees from an author's agency; her name, phone number and address were posted on alt.sex groups on the USENET and resulted in floods of offensive phone calls. A woman in Atlanta was appalled when someone posted a photograph of an unknown anonymous woman with the victim's name and contact information; she received calls from men who told her the announcement claimed she was offering free sex. A victim of such anonymous harassment founded WHOA — Women Halting Online Abuse — to help victims fight this oppression. The CyberAngels, an offshoot of the Guardian Angels vigilante group, claim to be willing and able to help victims; another vigilante is Peter Hampton, who can marshall thousands of people to saturate Web servers and who claims to take unspecified measures to damage harassers.

Category 1B4 *Stalking & harassment*

1997-04-15 **eavesdropping harassment cyberstalking**

RISKS, Reuters 19 8 ff

Around April 1997, police resolved a case of what had appeared at first to be spectacularly successful and mysterious technical attack on a suburban family in Emeryville, Ontario. Starting at the beginning of 1997 and dubbed "The Emeryville Horror" by a credulous press, the case involved heavy breathing on the phone, vague threats, boasts and inexplicable control of household electrical appliances. Counter-surveillance experts swept the house and found it "clean." Police suggested that the couple's adolescent boy might be responsible. After much denial by the family, they brought their son into the local police station for a polygraph exam to prove his innocence; he promptly confessed to the whole thing, which turned out to be a prank gone 'way too far. The 15-year old was recommended for psychiatric evaluation. As Ron Pfeifle implied in a subsequent issue of RISKS, the moral for all of us techno-nerds who speculated about wiring, HERF guns, and the whole bit: use Occam's Razor liberally when something seems too weird to be true.

Category 1B4 *Stalking & harassment*

2001-06-14 **data consolidation Web publication privacy public records tracking tracing stalking real estate taxes addresses location**

RISKS 21 49

The Washington Post Web site consolidated records from tax records and property tax appraisals and posted the resulting detailed database for the Washington DC metropolitan area. Nick Laflamme commented in RISKS that the unprecedented level of detail, comprehensive coverage and ease of access raise concerns over privacy issues. The situation also makes it easier than ever before for stalkers to locate victims' addresses.

Category 1B4 *Stalking & harassment*

2001-08-27 **privacy database automobile registration license plate stalking electronic access directory commercial telephone**

RISKS 21 63

Ulf Lindqvist summarized a report frm the Swedish newspaper *Aftonbladet* of Aug 27, 2001 < http://www.aftonbladet.se/vss/nyheter/story/0,2789,84644,00.html > that described "a new type of directory service" allowing one to supply "the license plate number of a car" for immediate access to "the name, address and phone number of the person registered as owner of that car." Lindqvist pointed out that rapid access to such a service (e.g., using a mobile phone) might exacerbate the consequences of road rage.

[MK: the potential dangers of increasing temptation for stalkers is another source for concern.]

Category 1B4 *Stalking & harassment*

2002-03-12 **online culture pornography children chat spam cybersex relations parental supervision**

NewsScan

30% OF TEENAGE GIRLS SUFFER ONLINE HARASSMENT
Thirty percent of teenage girls have been sexually harassed in a chat room, according to a poll conducted by the Girl Scout Research Institute. Only 7% had reported the harassment to their parents, however, because they feared being banned from online activities. Most of the girls said they tried to avoid pornographic sites, but that they sometimes ended up there by accident. They also reported receiving a lot of pornographic spam. And while the GSRI said parents should pay more attention to their daughters' online activities, 87% of the girls polled said they could chat online without their parents knowledge and 54% said they could conduct a clandestine cyber relationship. (NUA Internet Surveys 11 Mar 2002)
http://www.nua.com/surveys/?f=VS&art_id=905357736&rel=true

Category 1B4 *Stalking & harassment*

2002-04-15 **Internet harassment bullying stalking threats e-mail chat text instant message culture children violence intimidation**

NewsScan

BULLYING GOES ONLINE
Schoolyard bullies are harnessing technology to pursue their victims around the clock, warned UK children's charity NCH, which reports that one in four school children suffer from bullying via text-message, e-mail or in Internet chat-rooms. "The crucial difference from traditional bullying is that in the past kids who are being bullied could go home and find a safe haven," says NCH associate director John Carr. "But if they're bullied on their mobile (phone) or on the Internet, then it's ever-present." Carr said a survey conducted last month showed that one in six children aged 11 to 19 had received bullying text messages and about one in ten had been bullied over the Internet. (Reuters 15 Apr 2002)
http://story.news.yahoo.com/news?tmpl=story&cid=581&ncid=581&e=1&u=/nm/20020415/tc_nm/britain_bullying_dc_1

Category 1B4 *Stalking & harassment*

2003-04-18 **cyberstalking Internet rising privacy personal safety**

NewsScan

CYBERSTALKING ON THE RISE
Cyberstalking — stalking people over the Net — is increasing across the U.S., according to a new study by Wired Safety. And while women remain the most likely targets, they're getting into the act as perpetrators, too. In addition, growing numbers of children are cyberstalking children. "We didn't find much good news," said Wired Safety executive director Parry Aftab. "Identity theft is increasing. And because more people are cyber dating they become victims of cyberstalking when things don't work out." Aftab expressed concern over a recent court ruling that compelled Verizon to turn over the name of an ISP subscriber under the subpoena power of the Digital Millennium Copyright Act. "This is an outrageous and dangerous ruling. It was supposedly about music piracy, but the result of the case is that anyone can obtain personal information about any Internet user by simply filling out a one-page form and submitting it to a court clerk. There is absolutely nothing you can do to protect yourself, even if you are a police officer doing undercover work against s*xual predators. The future safety and privacy of all Americans engaged in online communications now rests with Verizon winning this case on appeal." [Asterisk inserted so that NewsScan Daily doesn't get caught in the software filters meant to ward off pornography.] (Internet News 18 Apr 2003)

Category 1B4 *Stalking & harassment*

2004-03-10 **Internet stalker victim compensated Docusearch private information revelation**

NewsScan

MOTHER OF INTERNET STALKER'S VICTIM GETS $85,000 FROM DOCUSEARCH

Docusearch, an Internet information broker which provided information used to stalk and murder a young woman with whom he was obsessed, has agreed to pay $85,000 to the victim's mother. Although Docusearch insists that none of the information it provided was private, the victim's mother says the company invaded her daughter's privacy and broke other laws in helping the obsessed stalker to find her. The woman's lawyer warned that information brokers such as Docusearch "will have to pay attention to whom they are providing people's private information," and he accused Docusearch of having "laid a red carpet" for the stalker which led him to the victim's place of employment. (AP/USA Today 10 Mar 2004)

Category 1B4 *Stalking & harassment*

2004-04-26 **Internet stalking lawsuit annoyance abuse threat lawsuit prosecution**

NewsScan

'FACELESS ENTITY' SAYS HE ISN'T A STALKER

In a South Carolina federal courtroom, a 38-year-old man named Robert James Murphy has pleaded innocent of Internet stalking charges and now remains free on $50,000 bond. Murphy was charged with 26 counts of using his computer "to annoy, abuse, threaten and harass" a Seattle woman who had never seen him until the day of his court appearance. The woman says: "He didn't give me any eye contact. He has been a faceless entity to me. I wanted to see him, and I wanted him to know that I was looking at him." If convicted, Murphy faces as many as 52 years in prison. He is accused of sending obscene messages and pictures to the woman and her co-workers beginning in 1998 — tracking her from his computer as she moved from state to state and job to job. For several years she had been simply deleting and ignoring the man's messages, but then began saving them as evidence and eventually approaching the police. (AP/USA Today)

Category 1B4 *Stalking & harassment*

2004-11-02 **Internet stalking South Carolina sentencing probation commuty service restitution e-mail fax authenticity forgery**

NewsScan; http://apnews.excite.com/article/20041102/D863O0TO0.html

INTERNET STALKER IN ANOTHER 'BAD PATCH' OF HIS LIFE

A South Carolina man has been sentenced to five years of probation, 500 hours of community service, and more than $12,000 in restitution for breaking a federal Internet stalking law by sending dozens of e-mails and faxes to a woman who broke up with him more than a decade ago. He also made it appear that the woman was sending pornographic material to her colleagues. The man now acknowledges that he was "stupid, hurtful and just plain wrong" to torment the woman, and says: "I was going through a bad patch in my life. I want to take my lumps and get on with life." He could have faced two years in prison and a fine of $250,000, but prosecutors agreed to recommend a sentence of three to five years on probation. (AP 2 Nov 2004)

1B5 Gambling

Category 1B5 Gambling

2000-02-14 **gambling stupidity gullibility consumer cheating fraud law**

NewsScan, New York Times
http://partners.nytimes.com/library/tech/00/08/biztech/articles/11gambling.html

The future of online gambling could be decided in a trial . . . [that started in February and pitted] the U.S. Justice Department against the World Sports Exchange (www.wsex.com), an online betting operation based in Antigua. The importance of the case goes beyond gambling, however, says one Internet attorney: "This is an interesting case of asserting jurisdiction over overseas Web sites in a criminal context. It will be closely followed by companies doing business on the Internet, both in the U.S. and abroad." The attorney prosecuting the case maintains that where the bet is placed physically doesn't matter; the crime occurs when an "interstate wire communication facility" like the Internet is used to transmit the wager. But Internet legal experts disagree, pointing out that legislation aimed at banning Internet gambling has not yet been passed in the House of Representatives. "This pushes the concept of jurisdiction to its limits," warns Henry Judy, a member of the American Bar Association's committee on cyberspace law. (Financial Times 14 Feb 2000)

[In August,] A co-owner of an online offshore gambling business based on the Caribbean island of Antigua . . . [was] sentenced to 21 months in a U.S. prison for violating . . . [that] country's federal Wire Wager Act, which makes it illegal to use telephone lines in interstate or foreign commerce to place sports bets. The prosecutor noted: "An Internet communication is no different than a telephone call for purpose of liability under the Wire Wager Act." (Reuters/New York Times 11 Aug 2000)

Category 1B5 Gambling

2000-02-28 **online gambling fraud**

NewsScan, Los Angeles Times
http://www.latimes.com/wires/wbusiness/20000228/tCB00V0457.html

The number of cybercasinos has ballooned from 15 in 1996 to more than 700 today, with revenue estimated to reach $1.5 billion this year, and $3 billion by 2002, according to an analyst for the online gambling industry. And despite government moves to criminalize online gambling, U.S. citizens account for about 50% of the industry's revenues. Using the Internet for sports-wagering is already banned, and the Senate passed the Internet Gambling Prohibition Act last year [in 1999], which would make it illegal to bet on casino-style games online. A companion bill [was] pending in the House and [would] be the subject of a subcommittee hearing on March 9. (AP/Los Angeles Times 28 Feb 2000)

Category 1B5 Gambling

2000-02-29 **online gambling fraud prosecution conviction lawsuit international**

NewsScan, Los Angeles Times
http://www.latimes.com/business/20000229/t000019506.html

The first defendant to stand trial in New York for online gambling via offshore locations has been convicted. Jay Cohen, a U.S. citizen, ran an Antigua-based sports betting parlor called the World Sports Exchange. He was found guilty under a federal law against using telephone lines to place illegal wagers. Cohen faces up to five years in prison on a conspiracy charge and two years for each of seven sports betting counts. (Bloomberg/Los Angeles Times 29 Feb 2000)

Category 1B5 Gambling

2000-07-14 **online gambling fraud legislation proposal law**

NewsScan, New York Times
http://partners.nytimes.com/library/tech/00/07/biztech/articles/14gamble.html,
San Jose Mercury News
http://www.sjmercury.com/svtech/news/breaking/ap/docs/206358l.htm

Legislation was introduced in July in the US House of Representatives to ban Internet gambling. [However,] The U.S. House of Representatives gave the Internet gambling industry a victory by failing to muster the two-thirds majority set as a requirement by House leaders in its 245 to 159 vote on a bill to ban online casinos. The votes in favor of the ban fell 25 short of the requirement. Sue Schneider of the Interactive Gaming Council said: "It appears that cooler heads have prevailed here. We have a brand new medium we're dealing with. We don't have the same kind of borders we had before." But Rep. Robert Goodlatte (R-Va.), who sponsored the bill, scoffed at the notion that it was anti-Internet: "One way to promote the Internet is to make sure that the seamy side of life is dealt with on the Internet. Just like child pornography has to be dealt with on the Internet, so does unregulated, out-of-control, illegal gambling." (AP/San Jose Mercury News 17 Jul 2000)

Category 1B5 Gambling

2000-10-13 **online gambling legislation jurisdiction**

NewsScan, Wall Street Journal
http://interactive.wsj.com/articles/SB971401767656792229.htm

For the first time, an online-gambling site has received approval to operate in the U.S. The Nevada Gaming Control Board has okayed Virtgame.com's plan to run an online betting parlor for football games, horse races and other sports. "Twenty-four hours is one of the beauties of the Internet," says a book manager for Coast Resorts, which owns four Las Vegas casinos, "but it could be a monster to manage." Virtgame has a contract with Coast to provide the computer system for Coast's online sports-betting sites, and is now marketing its system to others in the gambling business, including state lotteries. States have jurisdiction over all types of gambling within their state lines, but federal laws still prohibit transmitting bets over state lines. (Wall Street Journal 13 Oct 2000)

Category 1B5 Gambling

2000-12-06 **lottery ticket purchase online gambling**

NewsScan, Wall Street Journal http://interactive.wsj.com

Lottery players in Maryland will soon be able to buy their tickets online, making Maryland the first in the U.S. to offer online ticket sales. The new service is "just the beginning in gaining access to this large and demographically desirable market niche," said the Maryland Lottery director. "The Internet will be a big factor in the future of lotteries." Maryland players will need to file an online application, and can then choose their games, numbers and the number of weeks to participate. Charges for the tickets will still have to be paid by check or money order because it's illegal in Maryland to pay for lottery subscriptions by credit or debit cards. (Wall Street Journal 6 Dec 2000)

Category 1B5 Gambling

2001-05-30 **online gambling state law legislation prohibition international jurisdiction**

RISKS 21 45

On May 30, 2001 the California legislature passed a bill making it illegal to play illegal games online. According to a summary in RISKS, "The bill would fine first-time transgressors $25 per transaction (not conviction) and $100 per transaction thereafter. Companies (anywhere) convicted of catering to Californians could be liable for $1000 per transaction and 90 days in jail. The bill supposedly specifically allows prosecutors to go after offshore corporations."
http://www0.mercurycenter.com/breaking/docs/064216.htm

Category 1B5 Gambling

2001-07-25 **online gambling legislation proposal casinos betting gaming fraud**

NewsScan

NEW EFFORT TO CURB ONLINE GAMBLING
After three unsuccessful attempts at reining in the $1.6-billion Internet gambling industry, members of Congress are trying again, this time with a package bill that attempts both to ban online gambling completely and to block the ability of online casinos to collect bets through credit cards, checks or electronic fund transfers. In the past, gambling companies have evaded credit card restrictions by passing off gambling transactions as non-gambling purchases. The congressmen introducing the current legislation are Representatives Bob Goodlatte, Jim Leach, John LaFalce and Senator Jon Kyl. Goodlatte says that Internet gambling "is sucking billions of dollars out of the country. It's unregulated, untaxed, illegal and offshore, and we need legislation to address that problem." (AP/Salon 25 Jul 2001)
http://www.salon.com/tech/wire/2001/07/25/gambling/index.html

---

Category 1B5 Gambling

2001-07-26 **online gambling betting gaming marketing video games**

NewsScan

ADVERTISERS TURN TO ONLINE GAMING TO BOOST BRANDING
Traditional corporations, including General Motors, Honda and PepsiCo, are turning to online videogames to get their message out, targeting the 145 million consumers who are active computer and videogame players, according to a study by the Interactive Digital Software Association. "Forget your image of a gamer being a teenage punk with a skateboard and loud music," says the president of an advertising agency that specializes in targeting the 18-34 age group. IDSA's survey found that 42% of frequent game players are older than 35, while 30% are in the 18-34 range. The online games cost advertisers between $150,000 and $500,000 to create, depending on the graphics, says one game developer, who predicts the next wave will include other media, including cell phones and pagers. One scenario under discussion involves a player receiving pages during the day instructing him or her to log on to the game because the player's character is in danger. (Wall Street Journal 26 Jul 2001)
http://interactive.wsj.com/articles/SB996102206258182085.htm (sub req'd)

Category 1B5 *Gambling*

2001-08-02 **privacy personal information geographical location surveillance online gambling gaming taxation law enforcement police investigation**

NewsScan

GEO-LOCATION SOFTWARE FINDS PEOPLE ON THE NET
"Geo-location software" is the next wave in collecting information from online users, tracing the connection route to locate the city where a user is logging on. The software is raising new questions among privacy advocates, who worry that geo-location capabilities infringe on both a user's anonymity and his or her access to information. "Right now oppressive governments around the world are not able to keep information away from their citizens as they had (before the Internet)," says David Sobel, general counsel for the Electronic Privacy Information Center. One industry likely to benefit from the technology is online gambling, which is expected to generate $6 billion worldwide by 2003. Legitimate gambling sites could restrict access to only residents of states and countries where such activities are legal. In June, the state of Nevada moved forward on legislation to consider making online gambling legal within state borders. (Financial Times 2 Aug 2001)
http://news.ft.com/news/industries/infotechnology

Category 1B5 *Gambling*

2001-09-10 **online gambling penetration hacking data diddling code modification algorithms corrupted illegal winnings**

RISKS 21 67

Peter G. Neumann summarized an article about a hacked online-gambling site:

"The article is on risks in on-line gambling, and particularly CryptoLogic, Inc., a Canadian on-line casino games developer that has been hacked. One of their sites had been "fixed" so that craps and video slot players could not lose, with winnings totalling $1.9 million. Every dice throw turned up doubles, and every slot spin generated a perfect match. Whether it was an insider attack or a penetration is not clear from the article. (We noted the likelihood of hacking of Internet gambling sites in RISKS-19.27, 1 Aug 1997, not to mention my 1995 April Fool's piece in RISKS-17.02.) Interesting question: which laws against hacking will apply to subversions of illegal Internet gambling parlors? Who gets to prosecute remote attacks on off-shore operations?

http://news.excite.com/news/r/010910/11/net-tech-gambling-hacking-dc

---

Category 1B5 *Gambling*

2001-09-10 **online gambling international**

NewsScan

BRITISH TV TO OFFER REAL-TIME GAMBLING
Two British digital television platforms are planning to launch real-time interactive gambling services in an effort to boost revenues and attract the loyalty of couch-potato bettors. Both Telewest and ITV Digital will use SportXction software developed by U.S. software maker Interactive Systems Worldwide. SportXction allows bets to be placed at key points in television programming -- in particular during sports events where, for example, a player is about to take a penalty shot in soccer or serve in tennis. The UK's interactive TV industry is betting on gambling to help it win back some of the billions of pounds spent on subsidizing and selling digital TV to British consumers. "Many broadcasters now realize that their future success will be based upon incremental revenues generated from new, compelling and distinctive services," says Global Interactive Gambling CEO Cees Zwaard, whose company is partnering with Telewest on its interactive gambling venture. (Reuters 10 Sep 2001)
http://news.excite.com/news/r/010910/12/net-media-britain-tvbetting-dc

---

Category 1B5 *Gambling*

2002-01-14 **online gambling legalization interactive TV handheld**

NewsScan

COMPANIES GAMBLE ON ONLINE WAGERING
A growing number of companies are developing online gambling technologies, betting that cyberwagering will be legalized in the U.S. in the not-too-distant future. Interactive Systems Worldwide has designed interactive-television gambling software for German media firm Kirch Group that will enable European sports fans to bet from their own living rooms, and Interactive chairman Barry Mindes expects it will be available for this year's soccer World Cup. Interactive Systems is now working on a handheld gambling device and is hoping to introduce an online "contest" concept in the U.S. based on the gambling software. Under current U.S. law, online gambling is prohibited but TV viewers can enter contests to win prizes such as a car. Mindes envisions users answering a list of questions posed by an advertiser to rack up credits that could then be used for playing the game. (Wall Street Journal 14 Jan 2002)
http://interactive.wsj.com/articles/SB1010960972280769280.htm (sub req'd)

Category 1B5 Gambling

2002-01-31 **online gambling gaming mobile telephone Internet**

NewsScan

MOBILE GAMING SET TO BOOM
Almost half of all European mobile phone customers will be using their handsets to play games by 2005, according to a recent Forrester Research report, as users take advantage of snazzy new handsets and upgraded wireless networks. "The increase in wireless bandwidth and better phones will attract more firms to offer mobile games. Just as an increase in Internet-ready PCs pushed more companies to offer Web services, a bigger audience for mobile games will make firms like Eidos Interactive and Electronic Arts follow in the footsteps of Riot Entertainment and Picofun," says the report. As more games become available, the number of mobile game users is anticipated to rise from 5 million currently to 130 million by 2005. And while most of these players will be young, older gamers are expected to join the fun next year as classic 1970s- and '80s-era games, such as Pong, Frogger and Space Invaders, are revamped for the mobile platform. However, in order to capitalize on this new source of revenue, "operators must curb their greed," warns the report, saying that to ensure developers to continue to produce the games, operators must share their revenues with them. Forrester predicts that over the next five years, ad agencies will begin to acquire their own game development groups to create games for advertising and branding purposes. Television and film studios will also jump into the mix, with mobile games based on shows such as "Who Wants to Be a Millionaire?" (ElectricNews 31 Jan 2002)
http://www.electricnews.net/news.html?code=5909714

Category 1B5 Gambling

2002-06-18 **credit card online gambling bank block abuse fraud**

NewsScan; http://www.nytimes.com/2002/06/15/business/15GAMB.html 90

CREDIT CARDS BANNED FOR INTERNET GAMBLING
Citibank has agreed to block use of its credit cards for Internet gambling after New York State regulators said the bank could face criminal prosecution for aiding in the promotion of online gambling, which is illegal in New York. Citibank, with 33 million Visa and MasterCard holders, is the largest credit card issuer in the United States. Citibank also agreed to pay $400,000 to nonprofit agencies that provide gambling counseling. Other major credit card issuers, including Providian Bank, have already said they will try to block use of their cards for Internet gambling. Like other credit card issuers, Citibank is motivated to block the transactions for additional reasons, such as the "increased potential for fraud loss" and higher "delinquency rates" on the online gambling charges. New York Times, 15 June 2002 (registration req'd)

Category 1B5 Gambling

2002-09-11 **online gambling law ruling international Greece casino Internet café**

NewsScan

GREEK COURT REVERSES BAN ON VIDEO GAMES
The first case to test the new Greek law banning people from playing video games in public places has been thrown out of court, setting the country's legal establishment on a collision course with the state. Legislation passed in July forbade the games as part of a drive to stamp out illegal gambling, but it has been harshly criticized by the Internet community for not making a distinction between gaming and interactive gambling. Under Greek law, gambling is permitted only in licensed casinos, and the draconian legislation was enacted in response to an unlicensed slot-machine scandal that had embarrassed the government. The two Internet café owners charged with violating the ban could have faced jail sentences of up to three months and fines of $4,950 each, as well as the loss of their business licenses. Greece's Internet Café Owners Union welcomed the ruling, but say that their business has dropped precipitously since the law was passed. Computer usage in Greece is one of the lowest in the European Union, and Internet cafés have been credited with helping to expand access. (BBC News 10 Sep 2002)
http://news.bbc.co.uk/1/hi/technology/2249656.stm

Category 1B5 Gambling

2002-10-02 **online gambling law bill proposed legislation**

NewsScan

HOUSE ATTACKS INTERNET GAMBLING
The U.S. House of Representatives has passed a bill that would make it illegal to use credit cards or other forms of electronic payment for gambling on the Internet. Supporters of the legislation see a distinction between casino gambling and offshore gambling. Rep. Joseph Pitt (R-Penn.) says: "It may be impossible to keep illegal gambling sites off the World Wide Web, but it is entirely possible to prevent American credit card companies from completing these transactions that these crooks need to make their money, and that's what this bill does." James Leach (R-Iowa) adds: "Internet gambling serves no legitimate purpose in our society — it is a danger to the family, it is a danger to society at large." (Austin American Statesman 2 Oct 2002)

Category 1B5 *Gambling*

2002-10-04 **online gambling offshore jurisdiction e-commerce law legislation**

NewsScan

MGM LAUNCHES ONLINE CASINO
Las Vegas resort operator MGM Mirage has quietly launched an online casino, becoming the first major U.S. gambling company to do so. Its site is open to all for free play, but only residents of the UK, Portugal, Spain, Ireland, South Africa and New Zealand are allowed to open accounts and bet real money. The online casino office is located on the Isle of Man, an island-nation off the coast of Great Britain that has licensed four other Web casinos. The MGM Mirage site uses layers of database-searching software designed to verify that gamblers are who — and where — they say they are, and regulators and auditors on the Isle of Man and in London also monitor the network of systems. MGM is hoping that its move will encourage other large casinos to go online, but at the same time, online gambling is running into stiff opposition in Congress, where a bill passed on Tuesday would make it a crime for a gambling business to accept credit cards, checks or fund transfers in connection with unlawful Internet gambling. Gambling industry analysts predict that online casinos are likely to become an established niche in the market, where approximately 1,800 largely offshore Internet gambling sites already generate $3.5 billion in annual revenues, according to Bear Stearns. (AP/Wall Street Journal 3 Oct 2002)

Category 1B5 *Gambling*

2003-03-31 **eBay illegal gambling Paypal**

NewsScan

EBAY REACTS TO CHARGES AGAINST ITS PAYPAL OPERATION
Federal prosecutors in Maryland have accused PayPal, the Internet payments company acquired by eBay, of violating the [U.S.A.P.A.T.R.I.O.T.] Act by facilitating illegal gambling. The company disclosed the accusation in its annual report filed with the Securities and Exchange Commission; it says that prosecutors have offered a complete settlement of all possible claims and notes that the amount of its earnings from online gambling was less than what prosecutors asserted. (AP/San Jose Mercury News 31 Mar 2003)

Category 1B5 *Gambling*

2003-05-06 **internet gambling restricted house committee prohibit credit card checks electronic transfer funds**

NewsScan

HOUSE COMMITTEE APPROVES RESTRICTIONS ON INTERNET GAMBLING
The House Judiciary subcommittee approved legislation that would prohibit the use of credit cards, checks and electronic fund transfers as means to pay for online wagering. The bill, which is sponsored by Rep. Jim Leach (R-Iowa), has already been approved by the House Financial Services Committee. The House approved a similar bill last year in Congress, but it died in the Senate. Meanwhile, Rep. Jim Conyers (D-Mich.) and a small group of bipartisan lawmakers are taking a different approach to the issue: they have proposed creating a commission to explore legalizing Internet gambling in states interested in licensing, overseeing and collecting taxes on Internet gambling transactions. A report by the General Accounting Office last year called Internet gambling "a fast-growing industry" with estimated 2003 revenues of more than $4 billion. (AP 6 May 2003)

Category 1B5 *Gambling*

2003-09-02 **gaming gambling cheap players gaming for money profit by playing**

NewsScan

GAMING FOR MONEY
The game Ultimate Arena allows players to wager small sums to play a match against a single challenger or group of opponents at a similar skill level. At the end of a 10-minute match, the winner of a $2 bet would take home $1.70 home (with Ultimate Arena keeping 30 cents). The maximum bet for a single game is $20 and the most someone can lose in a month is $100, while there is no upper limit on how much players can win. (San Jose Mercury News 2 Sep 2003)

Category 1B5 *Gambling*

2004-03-01 **Internet online gambling gaming security dishonest manipulation prevention software**

NewsScan

KEEPING ONLINE GAMES HONEST

IT GlobalSecure sells software that prevents network vandals and dishonest players from manipulating online gambling. The company's chief executive says: "If you look online, there are whole Web sites either complaining about cheating or sharing ways to cheat. We've had people who are even just playing gin rummy online saying, 'We think we're being cheated, but we don't know what to do.'" The firm's software is based on encryption technology that can be applied to any network gaming system to validate the randomness of events in games of chance, verify player identities and create audits of each game. (Washington Post 1 Mar 2004)

Category 1B5 *Gambling*

2004-05-31 **offshore online gambling prosecution domestic support services international law first amendment rights litigation**

http://www.nytimes.com/2004/05/31/technology/31gambling.html?th=&pagewanted=print&position=

In early April 2004, United States Marshals seized $3.2M in advertising fees paid to the Discovery Communications Corporation for TV ads promoting the online gambling service ParadisePoker.com. Online gambling is illegal in the United States, but offshore gambling facilities cannot be attacked because the countries where they reside do not consider them illegal. Under international law, the doctrine of dual criminality requires equivalent crime laws in order to extradite people accused of a crime in one jurisdiction from the jurisdiction where they reside. Therefore, federal law enforcement authorities are cracking down on online gambling by attacking American companies who provide services to those offshore organizations. Critics of the new campaign argue that US law is inconsistent with respect to online gambling because not all states make it illegal. In addition, some analysts raised First Amendment rights arguments. Others complain that seizing foreign funds is a violation of international law.

Category 1B5 *Gambling*

2006-04-12 **gambling electronic slot machines wireless reprogramming manipulation vulnerability corruption theft cheating**

RISKS; NYT; http://tinyurl.com/ou6jf 24 24

CASINO CAN REPROGRAM SLOT MACHINES IN SECONDS

As an enormous operational improvement, the 1,790 slot machines in Las Vegas's Treasure Island Casino can now be reprogrammed in about 20 seconds from the back-office computer. Previously this was an expensive manual operation that required replacing the chip and the glass display in each machine. Now it is even possible to have different displays for different customers, e.g., changing between "older players and regulars" during the day and a different crowd at night ("younger tourists and people with bigger budgets". (Slot machines generate more than $7B revenue annually in Nevada.) Casinos are also experimenting with chips having digital tags that can be used to profile bettors, and wireless devices that would enable players to gamble while gamboling (e.g., in swimming pools!). . . .

There are various risks of interest to RISKS. Regulators are concerned that machines might be "invaded by outsiders", while bettors are concerned that casinos could be intentionally manipulating the odds -- for example, giving preferential treatment to high rollers. Internal and external manipulation are clearly potential issues, which of course could be exacerbated by compromisible wireless security. By Nevada law, odds cannot be manipulated while someone is playing, although with four-minute timeouts before and afterward, machines may be reprogrammed on the fly.

If it were still April Fools' Day, I might suggest that the slot machines could be reprogrammable for use as voting machines on election day. That way you could have instant payoff if you vote the right way.

[Abstract and commentary by Peter G. Neumann]

1B6 Auctions

Category 1B6 Auctions

1999-02-15 **online auctions theft fraud misrepresentation court case law**

USA Today

The online eBay auction house was embarrassed when someone offered computers for sale via its services, collected money for the items and then defaulted on delivery. The malefactor was convicted of fraud in federal court in mid-February.

Category 1B6 Auctions

1999-04-08 **fraud Internet auction eBay FBI investigation**

CNET news.com, Reuters

The integrity of Web-based auctions has been questioned before, but in February the eBay auction-house admitted that the FBI and the New York State Department of consumer affairs were investigating the practices of some of its sellers. Problems included sales of guns to unauthorized buyers and sales of illegally copied software. The company was also accused of failing to make it clear to buyers that it takes no responsibility for completion of the transactions initiated through its service nor for quality or deliver of goods sold online. In April, the firm settled with the NY regulators on a plan for cracking down on fake sports memorabilia sold through its service.

Category 1B6 Auctions

1999-07-15 **fraud online auction eBay investigation court case prosecution guilty**

CNET news.com http://news.cnet.com/category/0-1007-200-344903.html

Robert Guest of Los Angeles admitted in court in July that he defrauded victims of around $37,000 by offering goods for auction via eBay but failing to deliver anything.

Category 1B6 Auctions

1999-09-03 **fraud online auction e-commerce hoax kidney organs**

CNET news.com http://news.cnet.com/category/0-1007-200-346765.html

In September, someone put up a human kidney for sale through the online auction-house eBay and received bids of up to $5.8M. The auction service canceled the sale because selling human organs is a Federal felony with up to $250,000 in fines and at least 5 years in jail.

Category 1B6 Auctions

1999-09-07 **online auction traffic human baby unborn fetus eBay**

CNET news.com nhttp://news.cnet.com/news/0-1007-200-346836.html

A week after someone claimed to want to sell a human kidney online, eBay had to shut down an auction for an unborn human baby. Prices for the supposed baby had risen into the $100K range before eBay pulled the plug.

Category 1B6 Auctions

1999-09-23 **fraud online auction drug marijuana dope traffic**

CNET news.com http://news.cnet.com/category/0-1007-200-123002.html

Someone tried to sell 500 pounds of fresh marijuana via online auction-house eBay. The auction was shut down after 21 hours, during which prices offered had reached $10M.

Category 1B6 Auctions

2000-01-25 **credit card fraud theft online auction**

ZDNet http://www.zdnet.com/zdnn/stories/news/0,4586,2427490,00.html

A new scam involving online auctions and an offshore bank was reported in January. Steps in the fraud:
* Scam artist advertises expensive electronics on auction site and posts specific price as well for direct sale.
* Buyer agrees to purchase equipment.
* Thief proposes to send equipment directly to buyer's address in return for pledge to wire price to bank if product is OK.
* Using the buyer's detailed information (name, address, phone number), thief opens account with Web retailer.
* Arranges to ship equipment to buyer but pays for product using a stolen credit-card number.
Results:
* Buyer now has stolen equipment in possession.
* Owner of stolen credit-card has expensive charge for product never received.
* Thief has money in offshore bank.

Category 1B6 Auctions

2000-02-15 **online auction fraud investigation suspicion gullibility naive consumers cheating**

NewsScan, Financial Times

The Federal Trade Commission is launching an assault on online auction fraud, a problem that prompted 10,000 complaints last year, up from 107 in 1997. The agency plans to train law enforcement officers, educate the public and prosecute more offenders, but notes it lacks the jurisdiction to protect the rights of U.S. citizens who purchase items from overseas Web sites. Many online auction companies have responded by saying they will cooperate with FTC efforts: eBay, for example, will begin routing complaints about its vendors directly to the FTC this week. (Financial Times 15 Feb 2000)

Category 1B6 Auctions

2000-05-04 **online auction fraud tax international law jurisdiction**

NewsScan

A Paris court . . . barred French consumers from participating in online auctions unless they use a state-approved auctioneer and pay the French value-added tax. The ruling came in response to a lawsuit filed by the association of Paris auctioneers (commissaires priseurs) against online upstart Nart.com, the first company to auction off high-priced art work on the Net. Nart does not require its buyers to pay the tax, because its auctions are handled by a subsidiary incorporated in New York, with sales paid in U.S. dollars to a U.S. bank. The French court ruled the sales were illegal, because the activities were tantamount to the "organization of auctions of objects located in France." Nart says it will appeal the ruling: "This is almost like saying that French people should not be allowed to walk into Christie's or Sotheby's in New York and bid for something on sale there," says Nart co-founder Antoine Beaussant. (Financial Times 4 May 2000)

Category 1B6 Auctions

2000-06-07 **online auction fraud shill misrepresentation investigation**

NewsScan, New York Times
http://partners.nytimes.com/library/tech/00/06/biztech/articles/07ebay-fraud.htm

The Federal Bureau of Investigation . . . launched an investigation of several sellers in eBay auctions suspected of "shilling" (the practice of running up a bidding price through fraudulent bids by the seller or the seller's friends). The inquiry was prompted by a . . . New York Times article about a California lawyer who almost sold an abstract painting for $135,805, after starting the bid at 25 cents. Shilling is forbidden by eBay rules, and eBay is using its proprietary "shill hunter" software to review bidding by users. (New York Times 7 Jun 2000)

Category 1B6 Auctions

2000-08-29 **online auctions fraud law enforcement investigation complaints government agency industry**

NewsScan, USA Today http://www.usatoday.com/life/cyber/tech/cti455.htm

The Internet Fraud Complaint Center, a project of the FBI and the Department of Justice, . . . [said] that online auctions are the No. 1 source of complaints about fraud on the Internet, and expects to receive more than 1,000 complaints a day starting in November when the center is fully automated. The online auction industry denies that fraud is a serious problem, and eBay says that only one of every 40,000 listings has resulted in a confirmed case of fraudulent activity. Complaints about Internet fraud can be reported to http://www.ifccbi.gov. (USA Today 29 Aug 2000)

Category 1B6 *Auctions*

2000-10-16 **online auction purchase e-commerce fraud insurance guarantee confidence**

NewsScan, Los Angeles Times
http://www.latimes.com/business/20001016/t000098573.html

Yahoo is launching a new program to protect consumers who make purchases made on its auction and shopping sites from fraud. The initiative, which is backed by insurance from Lloyd's of London, is designed to "add another layer of confidence for consumers during the shopping season," says Brian Fitzgerald, producer for Yahoo auctions, who adds that fraudulent transactions account for less than 1% of all purchases on the Yahoo commerce site. (AP/Los Angeles Times 16 Oct 2000)

Category 1B6 *Auctions*

2000-11-13 **online auction law lawsuit judgement copyright infringement**

NewsScan, New York Times
http://partners.nytimes.com/2000/11/13/technology/13EBAY.html

A provision of the federal 1996 Communications Decency Act that had been written to protect Internet service providers. . . [was] extended by a California state judge in San Francisco to apply as well to eBay, the online auction company. A lawsuit against eBay charged it was liable for customer sales of bootlegged music sold through its Web site, but Judge Stuart R. Pollak rejected that contention, noting that eBay did not select the items to be sold, determine their minimum price, inspect them ... nor did it ever have them in its possession. (New York Times 13 Nov 2000)

Category 1B6 *Auctions*

2002-06-11 **online auction fraud deception cheat stolen property law enforcement**

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/3443962.htm

ONLINE AUCTIONS THE NEWEST WAY TO FENCE STOLEN GOODS
Online auctions such as eBay are the newest way to fence stolen property, because they're so anonymous and so simple. A Santa Clara prosecutor says: "There's no need for the pawnbroker. Internet auctions have suddenly become a really easy way to fence stuff." But law enforcement officials agree that eBay is extremely diligent in helping authorities track down criminals, by running sophisticated anti-fraud operations and by helping prosecutors build legal cases. An executive of the National Consumer League reminds us: "As we always say, if the deal is too good to be true, it usually isn't." (San Jose Mercury-News 10 Jun 2002)

Category 1B6 *Auctions*

2002-12-05 **Internet online auction scam fraud indictment**

NewsScan

INTERNET AUCTION SCAM
A 27-year-old Los Angeles man, Chris Chong Kim, has been charged with defrauding eBay buyers on six continents who had purchased computer equipment from him but never received delivery of the products they had purchased. The criminal complaint against Kim details losses of $453,000 to 26 U.S. customers and to eBay and Bank of America. If convicted, Kim will face a penalty of up to 24 years in prison. (Reuters/USA Today 4 Dec 2002)
http://www.usatoday.com/tech/news/2002-12-04-ebay-scam_x.htm

Category 1B6 *Auctions*

2003-02-03 **online auction illegal materials drugs arrest**

NewsScan

MAN ARRESTED FOR SELLING OPIUM POPPY ON E-BAY
The federal Drug Enforcement Administration (DEA) has arrested a Sacramento CA man for selling opium poppy pods on Internet auction site eBay, where he advertised them as "decorations"; each pod is the size of a golf ball and is at the end of a two-foot high stalk. An eBay executive said, "We check the site frequently for any illegal or illicit items and we remove them as fast as we find them," and he said that trying to use eBay to sell illicit drugs online "might be one of the dumbest things you can do." (AP/San Francisco Chronicle 31 Jan 2003)

Category 1B6 *Auctions*

2003-05-01 **internet auction fraud Federal Trade Commission FTC criminal failure deliver**

NewsScan

INTERNET AUCTION FRAUD
The Federal Trade Commission, together with 33 state and local law enforcement agencies, has announced the filing of 51 criminal and civil cases charging Internet auction fraud, most of them involving failure of the seller to deliver an item (usually items such as computers, plasma TVs, or diamond jewelry). Online auctions accounted for 46% of all complaints lodged with the Internet Fraud Complaint Center last year. (New York Times 1 May 2003)

Category 1B6 *Auctions*

2004-05-09 **eBay guarantee auctions marketing future prediction**

http://www.nytimes.com/2004/05/09/business/yourmoney/09digi.html?th=&pagewanted=print&position=

Randall Stross wrote about eBay's lack of guarantees. He observed that transactions are changing from low-cost, used products being exchanged under auction to high-cost, new products sold under a fixed price. He predicted that the company would eventually have to start providing moneyback guarantees to remain competitive.

Category 1B6 *Auctions*

2004-11-07 **eBay price inflation New York crime shills fraud bidding overpayments**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A32944-2004Nov7.html

BIDDING UP PRICES ON ONLINE AUCTIONS

Eight eBay sellers who bid up products online to inflate their prices have been ordered by the New York Attorney General's office to pay almost $90,000 in restitution and fines. More than 120 people will receive money from the settlement of the three cases. One man will receive a check for $3,089 after overpaying for a 1999 Jeep Cherokee sport-utility vehicle he bought from an eBay seller in 2002.(Washington Post 7 Nov 2004)

Category 1B6 *Auctions*

2004-11-17 **eBay Virgin Mary cheese sandwich auction joke**

NewsScan; http://theage.com.au/articles/2004/11/16/1100574471142.html

BIDS FOR VIRGIN MARY CHEESE SANDWICH CANCELED

The folks at eBay were no believers in this cheesy miracle: half of a 10-year-old grilled cheese sandwich whose owner claimed it bore the image of the Virgin Mary. Diana Duyser put the sandwich up for sale last week, drawing bids as high as $22,000 before eBay pulled the item on Sunday night. The page was viewed nearly 100,000 times before being taken down. An e-mail Duyser received from eBay said the sandwich broke its policy, which "does not allow listings that are intended as jokes." (The Age 17 Nov 2004)

1B7 Hate groups, speech

Category 1B7 *Hate groups, speech*

1997-07-31 **hoax rumor fabrication Internet infowar**

Reuter

The notorious fabrication, the "Franklin Diary" first surfaced in 1934 in a US pro-Nazi publication; it purports to quote Ben Franklin as an anti-Semite. Despite repeated debunking, the fraudulent document continues to circulate in the neo-Nazi underground, including KKK networks. It has recently been quoted in Hamas materials and seems to be kept alive today by repeated postings on the Internet. The Franklin Institute in Philadelphia has been swamped with phone calls about this document, which is described as being kept there.

Category 1B7 *Hate groups, speech*

2000-02-18 **hate speech Web Internet censorship government law regulation restriction international**

Inter Press Service

In February, an international seminar in Geneva ("Expert Seminar on Remedies Available to the Victims of Acts of Racism, Racial Discrimination, Xenophobia and Related Intolerance and on Good National Practices in this Field,") examined how national governments can fight racism without infringing on freedom of speech. Participants pointed out that censorship of hate speech is not far removed from the anti-democratic censorship practiced by totalitarian regimes worldwide. Self-regulation doesn't seem to work very well, especially with radically different levels of tolerance for expression of unpopular ideas. The conference concluded that as long as the US First Amendment protects racist and hate-spewing sites based in that country, international efforts at control are doomed.

Category 1B7 *Hate groups, speech*

2000-02-24 **hate groups terms of service acceptable use ISP lawsuit**

Benton Project; USA Today

The Jewish Anti-Defamation League protested to Yahoo for allowing several hate-speech groups on its service.

Category 1B7 *Hate groups, speech*

2000-10-17 **hate groups online identification recognizing law enforcement**

NewsScan, New York Times http://partners.nytimes.com/aponline/nyregion/AP-Hate-Internet.html

The Anti-Defamation League, www.adl.org, has created an online guide to hate symbols, logos, and tattoos to help people become aware of warning signs of the development of "hate" groups in their communities. A police official friendly to the ADL project says, "There are new symbols out there all the time. Unless you're affiliated with these groups, these are symbols you wouldn't have any idea about." (AP/New York Times 17 Oct 2000)

Category 1B7 *Hate groups, speech*

2001-01-03 **hate speech auction censorship filtering**

NewsScan

YAHOO TO BE PROACTIVE IN POLICING COMMERCIAL POSTINGS

Yahoo has adopted a new "proactive" monitoring program that will use software to accomplish an initial review of all commercial postings on its auctions, classified sections, and shopping areas. If the software detects any postings that appears to violate the site's policies hateful or violent material, it will give the senders the opportunity to revise their submissions or appeal the rejection to a human reviewer. Yahoo has been under pressure from human rights groups to take a more proactive stance against auctions of Nazi memorabilia and similar kinds of activities, and believes its new monitoring process will show that it has "thought about these issues in good faith." The monitoring will apply only to the commercial side of Yahoo and not to its discussion groups or home pages: "There we want to promote inclusiveness. We don't want Yahoo deciding who can or cannot speak in public debates." (New York Times 3 Jan 2001)
http://partners.nytimes.com/2001/01/03/technology/03YAHO.htm

Category 1B7 *Hate groups, speech*

2002-07-10 **terrorist Internet communictions Web**

NewsScan

TERRORIST LIFE, INTERNET-STYLE

In recent months sites like azzam.com, almuhajiroun.com, and qassam.net have been set up for terrorists to "make the Internet our tool," and although service providers frequently shut them down they usually reappear someplace else: al-Qaeda's Arabic site alneda.com has reemerged in the past five weeks on different servers in Malaysia, Texas, and Michigan. Most suspected terrorist sites are written in Arabic, proclaim hatred for the U.S., and call on militant Muslims to kill Americans and attack U.S. interests. But there are exceptions: the Islamic alsaha.com site has posted comments accusing bin Laden of being "a disgrace to our religion" and accusing him of having made "a mockery of everything we believe." Do these terrorists have day jobs? The site azzam.com offers the following advice to those who want to fight "the Jewish-backed American Crusaders" without disrupting their own employee benefits plans: "If you are working, either resign from your job and take a year off or request unpaid leave from your employer. Many large companies offer unpaid leave to their employees for periods ranging from two months to one year. That way you can fulfill your obligation [of jihad] and not have to give up your job." (USA Today 9 Jul 2002)
http://www.usatoday.com/life/cyber/tech/2002/07/10/terr

Category 1B7 *Hate groups, speech*

2004-03-17 **e-mail racism hate Australia law enforcement police controversy**

NewsScan

AUSTRALIAN POLICE IN RACIST E-MAIL CONTROVERSY

The New South Wales ombudsman will help police decide how to discipline an officer who sent a racist email to his colleagues. The contents of the email, found in the in-boxes of offices in four regional stations including Broken Hill and Dubbo, were described as filthy and disgusting by Deputy Commissioner David Madden at the time of its discovery. Thirty-five officers received the e-mail but the message is thought to have originated from a single source, who has been identified as an officer from Bourke in central northern NSW. The discovery of the e-mail came just two weeks after an alleged riot in the inner-Sydney suburb of Redfern, in which 36 officers were injured. The riot was in response to the death of an Aboriginal teenager. (The Australian 17 Mar 2004)

Category 1B7 *Hate groups, speech*

2004-04-28 **hate group Internet Web counter-terrorism homeland security freedom of speech first amendment violence**

NewsScan

HATE GROUPS ON THE INTERNET

Since the recent conviction in Illinois of a white supremacist who tried to have a judge murdered, the FBI has increased its monitoring of Web sites operated by hate groups. Richard K. Ruminski, the FBI official in charge of counter-terrorism investigations in Chicago, has made it clear that the agency won't tolerate anyone crossing the line from protected free speech to advocating violence. Ruminski says of one site: "It concerns us to the point where we're going to see what legal actions can be taken in order to maybe legally take that Web site down." (AP/Los Angeles Times 28 Apr 2004)

Category 1B7 *Hate groups, speech*

2004-06-17 **hate sites fighting conference Paris free speech censorship**

NewsScan

HATE SITES

An international conference in Paris has been exploring ways to fight anti-Semitic, racist and xenophobic propaganda on the Internet. "Our responsibility is to underline that by its own characteristics -- notably, immediacy and anonymity -- the Internet has seduced the networks of intolerance," French Foreign Minister Michel Barnier told the conference attendees. However, U.S. Asst. Attorney General Dan Bryant urged caution in taking actions that would violate rights of free speech, and suggested that the appropriate test is always whether a particular Web site is or is not engaged in criminal activity: "We believe that government efforts to regulate bias-motivated speech on the Internet are fundamentally mistaken. At the same time, however, the United States has not stood and will not stand idly by, when individuals cross the line from protected speech to criminal conduct." (AP/San Jose Mercury News 16 Jun 2004)

Category 1B7 Hate groups, speech

2006-05-04 **hate groups US Internet server use Islamic militants free speech terrorist recruitment**

DHS IAIP Daily; http://abcnews.go.com/Technology/wireStory?id=1925141 23

REPORT: HATE GROUPS USE U.S. INTERNET SERVERS.

Hate groups around the world, including Islamic militants, often use Internet servers based in the U.S. to send propaganda and instructions to followers, according to a report released Thursday, May 4, by the Simon Wiesenthal Center (SWC). The Center said it had logged some 6,000 Websites in the past year used by racists and bigots to incite violence. Extremist anti-Americans often find it easier and cheaper to use a site hosted in America since the U.S. has free speech and little Internet censorship. Recently, the center also has been intercepting an increased number of online tutorials and how-to manuals aimed at sympathizers who might actually be recruited to carry out attacks. SWC press release: http://www.wiesenthal.com/site/apps/nl/content.asp?c=fwLYKnN 8LzH&b=312458&content_id={433F72C6-2173-4360-8981-0BB7B508C4 87}&notoc=1 SWC's interactive report will be available for purchase May 2006: http://www.wiesenthal.com/site/pp.asp?c=fwLYKnN8LzH&b=242023

1B9 Non-virus hoaxes, urban myths

Category 1B9 *Non-virus hoaxes, urban myths*

1997-10-13 **hoax chain letter availability denial of service**

PA News

Poor little 8-year Craig Shergold was dying of a brain tumor — in 1989. He issued an appeal for get-well cards that began circulating through the Internet ten years ago. In 1997, he was now a healthy, strapping 18-year-old and he said he DOESN'T WANT ANY MORE DAMN GET-WELL CARDS. His family and the Royal Mail issued a world-wide appeal begging people to stop circulating the hoary chain letter and its variants through the Net and via fuzzy photocopies. The family has received over 140 million cards and still gets three to four sacks full daily. At one point it became extremely difficult to find the real mail in the flood of good wishes. This is a real-life case of the Sorcerer's Apprentice. Stop awready!

Category 1B9 *Non-virus hoaxes, urban myths*

2001-08-02 **hoax chain e-mail credit information privacy false news misinformation**

NewsScan

FALSE CREDIT SCARE FROM MESSAGE MAKING THE ROUNDS
The Federal Trade Commission has posted a consumer alert warning against the "half-truths and misinformation" in a widely circulated anonymous e-mail message that's falsely warning consumers that major credit bureaus in the U.S. are now allowed to release people's credit information to anyone who requests it. The head of Associated Credit Bureaus, a trade association, says: "We want to make it perfectly clear that a consumer credit report is provided only to legitimate businesses for the purpose of making a determination on the extension of credit and other consumer benefits... One of the great things about the Internet is the ability to disseminate information at the click of a button. The downside is that things can be picked up and relayed -- and keep going and going." (AP/Washington Post 2 Aug 2001)
http://washingtonpost.com/wp-dyn/articles/A21402-2001Aug2.html

---

Category 1B9 *Non-virus hoaxes, urban myths*

2001-10-10 **securities fraud pump-and-dump scam bogus fraudulent press release ISP liability policy investigation**

NewsScan

YAHOO WON'T CHANGE CHATROOM POLICY [10 Oct 2001]
Trading in shares of Viasource Communications and Extreme Networks was halted Monday after a bogus document resembling a PR Newswire release was posted in a Yahoo Finance chatroom. Yahoo took the release off the message board as soon as it was contacted by PR Newswire. A spokeswoman said, "All of our message boards are considered unmoderated pieces of public forum. We don't proactively monitor the content of our boards." Citing Yahoo's user-privacy policy, she did not comment on whether Yahoo intended to pursue an investigation to determine who posted the press release. (Wall Street Journal 10 Oct 2001)
http://interactive.wsj.com/articles/SB1002654113365462080.htm

---

Category 1B9 *Non-virus hoaxes, urban myths*

2002-01-30 **securities fraud Web marketing gullibility scam SEC government regulators hoax lesson**

NewsScan

SEC PLAYS LITTLE HOAX TO WARN INVESTORS OF WEB SCAMS
The Securities and Exchange Commission is a principal agency behind the hoax site www.mcwhortle.com, which purports to provide testimonials from investment analysts and financial exports for an outfit called McWhortle Enterprises, but which greets visitors with the warning: "If you responded to an investment idea like this... You could get scammed!" (AP/San Jose Mercury News 30 Jan 2002)
http://www.siliconvalley.com/docs/news/svfront/046980.htm

Category 1B9 *Non-virus hoaxes, urban myths*

2003-06-25 **British Airway free tickets e-mail hoax plane valuable bandwidth SARS virus war Iraq encouraging people fly**

NIPC/DHS

June 25, eSecurity Planet — 'Free flight' e-mail hoax serves as security warning.

An e-mail chain letter is tricking people into wasting their own time, cluttering corporate inboxes around the country and hogging up valuable bandwidth. Anti-virus software company Sophos, Inc. is reporting the Free Flight chain e-mail is convincing people that British Airways is giving away free plane tickets to anywhere in the world to anyone who forwards the email to 10 or more people. The e-mail claims that it is encouraging more people to fly, following a downturn in the airlines industry because of concerns about the SARS virus and the war in Iraq. It also contends that the airline is working in conjunction with Microsoft, monitoring the distribution of the message. "There's no malicious content. It won't cause damage to the system," says Chris Belthoff, a senior security analyst with Sophos.

Category 1B9 *Non-virus hoaxes, urban myths*

2003-09-16 **health hazardous internet breast cancer yahoo accuracy information**

NewsScan

INTERNET COULD BE HAZARDOUS TO YOUR HEALTH
A survey conducted by Holly Cardamone, a Melbourne, Australia nurse and communications consultant, indicates that most Web sites that dispense health-related information fail to meet basic standards of impartiality and accuracy. Cardamone evaluated the top 100 Web sites returned in Yahoo searches on breast cancer, diabetes and depression, using the international Health On The Net Foundation's code of conduct. The code's guidelines address issues relating to the authority of the information given, user confidentiality, openness about corporate sponsorship, and emphasis on treating the information as complementary to medical treatment, rather than replacing it. Forty-two of the sites presented useful information: "Such sites contained quality, appropriate information with potentially lifesaving content such as explanations of the symptoms of depression, and healthy recipes for diabetics," says Cardamone. But the other 58 were a disappointment, containing unverified information. Meanwhile, other researchers have cited the growing phenomenon of "cyberchondria" — hypochondriacs who feed their health obsession with information from the Web. Such people are especially drawn to multiple choice quizzes that provide diagnoses based on a list of symptoms. (Sidney Morning Herald 16 Sep 2003)

Category 1B9 *Non-virus hoaxes, urban myths*

2004-08-23 **Sweden king murder online hoax BBC Website impersonation spoof**

NewsScan

KING CARL'S 'MURDER' AN ONLINE HOAX

Hoaxers have faked an announcement of the murder of the King of Sweden on a counterfeit BBC news website carrying a headline "Sweden's King Murdered" over a story saying that "Sweden's King Carl XVI Gustaf was shot in Athens this evening when he was on his way back to his hotel after
watching the Swedish table tennis star Jan-Ove Waldner beat Timo Boll, Germany, in the Olympic games." Swedish newspaper Expressen said the page had been sent by email to an unknown number of Hotmail e-mail addresses. "It's really very bad taste," the newspaper quoted a Royal Palace spokeswoman as saying: "It goes beyond the limit." Apart from the authentic-looking layout closely imitating the BBC, the news page also included genuine items such as the latest from Najaf in Iraq and the Olympics in order to enhance its appearance of credibility. (The Australian 23 Aug 2004) Rec'd fr J Lamp

---

Category 1B9 *Non-virus hoaxes, urban myths*

2005-02-22 **e-mail scam Department Homeland Security DHS exploit war Iraq hoax**

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml?articleID=60402476

E-MAIL SCAMS EXPLOIT HOMELAND SECURITY AND SOLDIERS KILLED IN IRAQ.

Federal authorities are investigating two e-mail scams, including one targeting families of soldiers killed in Iraq, that claim to be connected to the Department of Homeland Security (DHS). Both of the online pleas for help -- and money -- link themselves to the Immigration and Customs Enforcement (ICE) bureau's Website. ICE is one branch of DHS. In one scheme, e-mail sent to families of U.S. soldiers killed in Iraq include a link to the bureau. The e-mail seeks to recover money from a friend of the slain soldier. In the other, the e-mail identifies itself as being sent by a federal agent trying to track down funds looted from the Iraqi Central Bank by Saddam Hussein's son. The e-mail also links to the bureau Website. Both e-mail campaigns are bogus and people are urged to ignore and delete them.

Category 1B9 *Non-virus hoaxes, urban myths*

2005-11-22 **FBI warning e-mail scam fraud Internet Crime Complaint Center**

DHS IAIP Daily;
http://www.cnn.com/2005/TECH/internet/11/22/email.scam.ap/index.html

FEDERAL BUREAU OF INVESTIGATION WARNS OF E-MAIL SCAM

The Federal Bureau of Investigation (FBI) issued an alert Monday, November 21, about a scam involving unsolicited e-mails, purportedly sent by the FBI, that tell computer users that their Internet surfing is being monitored by the agency. The users are told they have visited illegal Websites and are instructed to open an attachment to answer questions. The FBI did not send these e-mails and does not send any other unsolicited e-mails to the public. The FBI is investigating the scam. Recipients of these e-mails are asked to report them by visiting the Internet Crime Complaint Center. Internet Crime Complaint Center: http://www1.ifccfbi.gov/strategy/051122.pdf

1C Identity, impersonation, spoofing

Category 1C *Identity, impersonation, spoofing*

1997-01-20 **pornography appropriate-use policy**

Reuters

A young Polish man was arrested by police in Katwice province for allegedly distributing child pornography via the Internet from his workplace computer. The porn was discovered and reported by a discussion group in Sweden.

Category 1C *Identity, impersonation, spoofing*

1997-01-21 **pornography**

EDUPAGE

From EDUPAGE: "A feature article on pornography on the Internet said the abundance of sex on the Internet is the result of a century of obscenity battles won in the courts. It mentions that Industry Canada has recently released a background paper on illegal and offensive material on Internet, which points out that many Web images are taken from magazines that are freely available in Canada. (Ottawa Citizen 21 Jan 97 A4) <http://info.ic.gc.ca/ic-data/info-highway/general/offensive/offens_e.html>"

Category 1C *Identity, impersonation, spoofing*

1997-01-23 **pornography**

EDUPAGE

EDUPAGE: "An Albany, New York, college business major was arrested yesterday in a cyberporn sting operation, on a charge of using America Online to transmit three dozen sexually explicit photos of children. (Vancouver Province 23 Jan 97 A37)"

Category 1C *Identity, impersonation, spoofing*

1997-01-24 **pornography**

Reuters

Two Bavarians were arrested by German federal police for offering to sell children for sadistic sex and murder. The accused were denounced by users of Deutsche Telekom's T-Online Internet Access Service.

Category 1C *Identity, impersonation, spoofing*

1997-01-24 **AOL pornography lawsuit**

AP, Reuters

In Miami, FL, the mother of a pedophile's victim sued AOL for allowing pedophiles to set up chat rooms for trading in child pornography. Her son was raped and photographed by Richard Russell, a middle-school teacher; he is serving a 22-year sentence in state prison for his crimes. The mother argues that AOL should have monitored activities on its service and prevented the abuse. Because of AOL's lack of policing, she says, "AOL service became known to the pedophile community as a place for open discussion, trading, and marketing of child pornography. In essence, AOL Inc. has created a home shopping network for pedophiles."

Category 1C *Identity, impersonation, spoofing*

1997-02-12 **pornography filter**

Reuters, UPI

In Boston, parents kicked up a ruckus when they discovered that the Boston Public Library has nothing in place to prevent children from Net-surfing into pornographic sites. The librarians pointed out that recent jurisprudence indicated that censoring materials in public libraries infringes on children's First Amendment rights. Within a day of the mayor's order to install CyberPatrol Web filtering software on 200 computers at Public Libraries across the city, the American Civil Liberties Union and the Office for International Freedom at the American Library Association protested the censorship.

Category 1C *Identity, impersonation, spoofing*

1997-02-12 **pornography seducation e-mail**

AP

Paul Brown, Jr, a 47-year-old, 400-pound man, misrepresented himself as a 15 year-old boy in e-mail to a 12-year old girl in New Jersey. He was arrested in February and police found correspondence with at least ten other teenaged girls across the country. Brown convinced his young victims, some as young as 12, to perform various sexual acts in front of cameras and send him pictures and videotapes. He pleaded guilty in June to enticing a minor into making pornography. He faced fines of up to $250K and 5 years in prison. In August, one of his many victims told the court that she had suffered ridicule and humiliation as a result of her entrapment and had left her school to escape the trauma. She accused Brown of emotional rape. Displaying an astonishing interpretation of his own behavior, Brown said at his sentencing hearing, "It was just bad judgment on my part." Using good judgment, the court sentenced him to five years incarceration.

Category 1C *Identity, impersonation, spoofing*

1997-04-08 **child pornography FBI sting Net chat**

AP

FBI Director Louis Freeh, speaking before a Senate panel, described the Bureau's attempts to protect children in cyberspace. The "Crimes Against Children" initiative includes a program in which undercover agents monitor chat lines where pedophiles have taken to impersonating children; the agents turn the tables on the victimizers and have been responsible for 91 arrests and 83 felony convictions since 1993.

Category 1C *Identity, impersonation, spoofing*

1997-05-27 **child pornography international law treaties**

Reuters

The 29 nations of the OECD agreed to harmonize national laws covering the distribution of child pornography through the Internet. The doctrine of dual criminality requires an act to be a crime in both jurisdictions for extradition to be legal, so this move could herald a more effective international response to the problem of child sexual abuse inherent in child pornography.

Category 1C *Identity, impersonation, spoofing*

1997-06-09 **Internet pedophiles**

UPI

Richard Romero went to trial in June, accused of tricking a 13-year-old boy into leaving his Chicago home for a tryst in Florida. The events allegedly took place in 1996, when Romero is accused of having befriended the child through the Net by pretending to be a 15-year-old boy. The abducted boy's mother luckily found details of the meeting place after the child had left home and police were able to track the pair with the help of a taxi driver who remembered them.

Category 1C *Identity, impersonation, spoofing*

1997-06-30 **child pornography library censorship**

AP

A library user was arrested for downloading images of nude boys onto floppy disks at the Lakewood Public Library in Ohio. Library staff reported James R. Thomas of Strongsville, OH to police and undercover agents watched him as he viewed and copied similar images. Thomas was banned from the library; however, library staff will continue to allow patrons to access the Internet from public terminals. In some libraries, Internet terminals have been placed in highly public areas where librarians can keep an eye on the screens.

Category 1C *Identity, impersonation, spoofing*

1997-07-02 **child pornography chat rape AOL**

UPI

Several police operations successfully captured pedophiles after hundreds of creeps sent sexual innuendos to a virtual girl. One was caught in Concord, CA as he prepared to enter a motel armed with condoms and a bag of Nordstrom lingerie. In another sting, police captured a homosexual pedophile in Washington, DC when he attempted to meet a virtual 13-year-old boy he had attempted to seduce via chat line.

Category 1C *Identity, impersonation, spoofing*

1997-07-11 **child pornography Internet**

AP

Fox Meadow School students and staff in Scarsdale, NY were shocked to find their well-liked teacher, Robert M. Nebens, charged with interstate transportation of child pornography and interstate travel with the purpose of engaging in sex with a person under 18. FBI Special Agent Anne Figueiras posed as a thirteen-year-old boy to trap the accused pedophile into arranging a meeting in Florida via the AOL online chatroom "Barely Legal: Male-for-Male." Other children may also have been abused by Nebens, according to the FBI.

Category 1C *Identity, impersonation, spoofing*

1997-07-17 **hackers child pornography infowar**

Computer Weekly

Hacker Christian Valor declared infowar on child pornographers in mid-July. His manifesto explained that he had scoffed at claims that the Net is being used by pornographers until he was made physically ill by anonymous child porn sent to him by e-mail. He appealed to hackers to join him in a cyber-vendetta against makers and purveyors of such images and claimed that law enforcement authorities would ignore the violations of law that such a campaign would entail.

Category 1C *Identity, impersonation, spoofing*

1997-07-18 **Internet seduction child abuse**

AP

A 22-year-old Senior Airman from Offutt AFB (NE), Brooker Maltais, pleaded guilty to statutory rape and sodomy of a 14-year-old Rochester NY girl he met via Internet chat and who ran away from home to be with him while he was absent without leave. He was sentenced to four years in military prison and a bad-conduct discharge.

Category 1C *Identity, impersonation, spoofing*

1997-07-25 **Internet seduction**

UPI

Two 15-year-old Bronx (NY) girls ran away in July with a 19-year-old man they met over the Internet. The three were captured by police in Orlando, FL; information the children left on their computers helped police track them down.

Category 1C *Identity, impersonation, spoofing*

1997-07-25 **child pornography Internet**

PA News

Graham Fitchie, a computer system manager in Merstham, Surrey, was convicted of trafficking in child pornography and was sentenced to three years in prison. He was a member of a ring of about 20 pedophiles around the world who traded such material; police found 20,000 obscene pictures in his home — the largest seizure of child porn in Britain to date. The evidence is being shared with other police forces in Britain and internationally.

Category 1C *Identity, impersonation, spoofing*

1997-07-28 **pornography filtering censorship children hackers passwords**

Newsbytes

Reports surfaced in late July that Web sites catering to seekers of pornography include thousands of user IDs and passwords for entering restricted porn catalogues. Some sites include instructions for bypassing Net-filtering software. Details of how to reach these filter-busting sites are widely circulated on IRC channels. Ironically, the people fighting hardest to shut down the password sites are the pornographers themselves, upset because they are losing potential revenue.

Category 1C *Identity, impersonation, spoofing*

1997-07-30 **child pornography**

Reuters

Spanish police in Barcelona arrested 12 people accused of participating in a network of pedophiles. They seized a large mass of child pornography, some of it distributed through the Internet, and found evidence that the adults were also involved in prostituting children.

Category 1C *Identity, impersonation, spoofing*

1997-08-01 **Internet gambling**

RISKS 19 27

Peter G. Neumann commented cogently on the RISKS of Internet-based gambling: "The risks include bogus virtual casinos whose payoffs turn out to be more virtual than real, semi-legitimate casinos working credit-card scams on the side, glorious opportunities for money laundering, serious gambling debts accumulated in your name by a masquerader, spawning of serious undetected addictive behavior that might otherwise be observed (on the Internet no one knows you are a gambler, except for the casino), your 9-year-old gambling with your credit card — especially if your browser automagically inserts your credit information — and so on into the night. As a second-order effect, massive illegal activities could also lead to attempted restrictions on the good system security and cryptography necessary to conduct legitimate Internet commerce. In any event, whether or not you bet on the Net, don't bet on the Net being adequately secure! You are already gambling with the weaknesses in our computer-communication infrastructures, but NetBet could raise the ante considerably. Caveat aleator."

Category 1C *Identity, impersonation, spoofing*

1997-08-07 **pedophiles Internet**

Reuters

In Munich, two Internet users were put on trial for offering to sell young Czech girls as slaves for sadism and murder. The accused claim that they were just joking. However, police found a torture chamber in the couple's home.

Category 1C *Identity, impersonation, spoofing*

1997-08-09 **Internet bomb children**

UPI

Two Long Island teenagers blew themselves up by following an Internet recipe and running with a bottle full of explosives. The blame, no doubt, would rest on the Internet and not on their own stupidity.

Category 1C *Identity, impersonation, spoofing*

1997-08-14 **child pornography ISP privacy**

AP

A 21-year-old man in Loveland, CO was arrested after his ISP reported him to local police when staff members discovered child pornography downloads through his account. The case raised questions of privacy and the role and responsibilities of ISP's. Dave Banisar of the Electronic Privacy Information Center pointed out that most ISPs prefer to take a hands-off approach to what their customers are doing.

Category 1C *Identity, impersonation, spoofing*

1997-08-15 **Internet addiction**

EDUPAGE, AP

Kimberly S. Young, a clinical pyschologist at U. Pittsuburgh, reported that those at risk for "Internet addiction" are likely to gravitate to chat rooms and MUDs. She has been called into cases of divorce caused by Net addiction.

Category 1C *Identity, impersonation, spoofing*

1997-08-17 **child pornography ISP privacy**

EDUPAGE

When ISP staff investigating a Colorado customer's account ran across evidence of traffic in child pornography, they informed police and the man was arrested. Possession of child pornography is a misdemeanor; creation and distribution is a felony. The incident created a stir in privacy circles because ISPs normally avoid prying into customers' activities, much as common carriers take no responsibility for the content of phone calls and fax transmissions.

Category 1C *Identity, impersonation, spoofing*

1997-08-26 **child porn FBI sting Internet**

AP

Swiss residents John and Buntham Grabenstetter were arrested in Buffalo, NY after allegedly trying to sell child pornography to FBI agents posing as pornography mercants. The accused apparently offered the smut for sale via the Internet.

Category 1C *Identity, impersonation, spoofing*

1997-09-05 **pornography Internet child**

Reuters

A 24-year-old Polish man was convicted for spreading pornography via the Internet in Poland's first such case. He received a nine-month prison term suspended for three years contingent on good behavior.

Category 1C *Identity, impersonation, spoofing*

1997-09-22 **pornography**

Reuters

A poorly-designed survey in Britain sponsored by Novell revealed that one male worker in four among the respondents (the Reuters story failed to mention sample size, but everybody knows that size doesn't matter. . .) knew someone at work who used the Internet to access pornography or other anti-social materials during working hours. Unfortunately, since several people may be aware of the same person's behavior, this provides only an upper bound on the number of pornophiles at work.

Category 1C *Identity, impersonation, spoofing*

1997-09-30 **child pornography law enforcement sting**

AP, EDUPAGE

A joint federal and New York State initiative captured more than 1,500 people involved in child pornography through the Internet. AOL cooperated in the sting operations, called Rip Cord because some of the images so enraged investigators that one yanked a computer cord out of the wall socket. The operation may have caught some big fish in Buffalo, NY — John and Buntham Grabbenstetter of Switzerland, accused of being the masterminds of a international child pornography ring.

Category 1C *Identity, impersonation, spoofing*

1997-10-01 **police cybercrime Internet fraud criminal**

OTC

New York State set up a cybercrime tip line for sending information directly to the NY Internet Unit established to fight fraud, pedophilia, and any other illegal activities involving the Net. See <http://www.cnn.com/US/9709/30/cybersting/> for details of the operation. Try <http://www.oag.state.ny.us> to supply information on electronic wrong-doing in the Empire State.

Category 1C *Identity, impersonation, spoofing*

1997-11-06 **censorship appropriate use library civil liberties**

EDUPAGE, NY Times

In Loudoun, VA, the Library Board decided that adults would have to request permission to the uncensored Internet from a librarian. Youngsters less than 17 years old would not be permitted to surf the unfiltered Net without a parent or guardian physically present. The ACLU immediately protested the policy. Defenders of the filtering/censorship policy argued that allowing unfettered access to the filth-drenched Net would constitute a hostile work environment for employees.

Category 1C *Identity, impersonation, spoofing*

1998-01-06 **Internet gambling**

EDUPAGE

Federal attorneys for Oklahoma seized a gaming computer at Multimedia Games Inc. claiming that its online bingo is in fact an illegal slot machine. The company protested its innocence.

Category 1C *Identity, impersonation, spoofing*

1998-02-05 **child pornography Web**

EDUPAGE

According to Professor Michael Mehta of Queen's University in Kingston, Ontario, online pornography may ironically be a factor in the growing market for better monitors and faster access to the Internet.

Category 1C *Identity, impersonation, spoofing*

1998-02-10 **online Internet gambling lawsuits states**

EDUPAGE

The attorneys general of Missouri and Wisconsin sued the Coeur d'Alene Indian tribe to block their new Internet- and phone-based parimutuel betting activity, the "U.S. Lottery." Senator Jon Kyl (R., AZ) introduced a bill to ban Internet gambling throughout the U.S.

Category 1C *Identity, impersonation, spoofing*

1998-02-17 **hacker threatening e-mail harassment**

UPI, EDUPAGE, New York Times

Richard Machado, a 19-year former college student, was charged with ten counts of threatening Asian Americans via e-mail. In a brilliant display of logic, his attorney argued that he should be charged with only one count of hate e-mail because the multiple hate messages were sent out in a single operation. By this logic, someone who kills several people in one incident using a machine gun ought to be charged with a single count of murder because the trigger was held down only once. In November, the jury deadlocked 9:3 in favor of acquittal and the judge declared a mistrial. The key argument of the defense was that because the defendant was bored and not actively involved in hate groups, his hate messages should be ignored. Machado was finally convicted in February 1998, setting an important precedent for governing behavior in cyberspace.

Category 1C *Identity, impersonation, spoofing*

1998-03-29 **Internet gambling prosecution wire fraud**

EDUPAGE

US federal prosecutors charged several cybergambling joints with violation of laws prohibiting interstate wire communications of bets. The International Internet Gaming Association announced that it was working on recommendations for complying with national laws on this issue. [Comment from MK: There was no explanation of how a gambler can determine if a game of chance being run via the internet involves any chance at all; for example, a program giving the appearance of a card game of chance could easily evaluate all bets made during one round and rig the results so that no bettor would win. "Mechanical" games such as roulette wheels that are in fact simply programs could easily be manipulated to provide fraudulent probabilities that would translate into higher earnings for the house. If, as Garrison Keilor of Minnesota Public Radio's _Prairie Home Companion_ says, "Lotteries are a tax on those people who were never good at arithmetic," then online gambling is a tax on people who never stopped believing in Santa Claus.] In July, the huge international gambling company GTECH announced plans for Internet lotteries supposedly structured to exclude participation by US residents. At the end of July, the Senate passed Sen. J. Kyl (R-AZ)'s anti-online-gambling bill 90-10.

Category 1C *Identity, impersonation, spoofing*

1998-04-26 **pornography first amendment free speech journalism chat room**

EDUPAGE

Larry Matthews, a National Public radio and public TV journalist in Maryland, was arrested and indicted on charges of a felony violation of anti-child-pornography laws. Matthews agreed that he pretended to be a child pornographer in chat rooms and actually exchanged lewd pictures of and with children, but he explained that he was doing research for an article. The prosecutor dismissed his explanation, stating, "The defendant is seeking what amounts to an absolute immunity to violate valid criminal statutes when he decides to do so in the name of gathering news." In July Mr Matthews pleaded guilty after giving up the case as hopeless once the judge opined that "a press pass is not a license to break the law." He and his legal team planned an immediate appeal.

Category 1C *Identity, impersonation, spoofing*

1998-05-31 **video games violence school shootings**

EDUPAGE

Speakers for the video-game industry in the US vigorously denied any connection between their blood-spattered, mindless games of death and destruction and the recent spate of schoolboy massacres. Showing admirable objectivity and balance, Nintendo chairman Howard Lincoln said, "I don't think there's any connection with video games and violence."

Category 1C *Identity, impersonation, spoofing*

1998-07-21 **child pornography Internet Germany Europe**

EDUPAGE

Horrified by finding German members of an international child pornography ring, the German government announced an intensification of their war against such materials.

Category 1C *Identity, impersonation, spoofing*

1998-07-28 **acceptable use filtering Internet Web employee policy porn**

EDUPAGE

A civil servant in the Ministry of Justice in Netherlands was fired for downloading child pornography to his office computer. He faced a possible term of up to six years imprisonment.

Category 1C *Identity, impersonation, spoofing*

1998-09-03 **child pornography international police ring Internet arrests**

EDUPAGE

Two hundred people around the world were arrested in a massive coordinated raid on the Internet child-pornography ring. US suspects belonged to the "Wonderland Club," which required possession and trading of illegal materials including pictures of the rape of infants.

Category 1C *Identity, impersonation, spoofing*

1999-01-06 **child pornography pedophiles Internet Web site prosecution**

Belfast Newsletter

Focus on Children, a Dublin-based charity, discovered a nasty nest of pedophiles operating a child-pornography exchange service on Web sites they found in mid-1996. In a 30-month investigation, the agency cooperated with the European Commission in Brussels and with police forces (including the FBI and Europol) to close in on the perpetrators.

Category 1C *Identity, impersonation, spoofing*

1999-02-23 **hate speech Web report**

Reuters

According to a study by the Southern Poverty Law Center issued in February 1999, hate groups such as the KKK were using the Web as a cheap and effective way to twist the minds of victims, many of which were in colleges and universities. The spread of hateful speech through the Internet vastly increased the potential audience, said the SPLC.

Category 1C *Identity, impersonation, spoofing*

1999-02-24 **gambling international regulation legislation supervision**

AAP

In Australia, a conference on casinos and gambling heard from the chair of the US Interactive Gaming Council, Sue Schneider, that an international interactive gaming council should be established to supervise online gambling. Chris Herde, writing for Australian Associated Press on 1999-02-24, wrote that the 1998 value of online gambling worldwide was several billion dollars a year and that the number of online gambling sites had risen from 15 in 1997 to more than 280 in 1999. [Of course, the entire online gambling industry is an IQ test: people who gamble online are willing to allow someone to take their money to allow them to bet on random processes simulated by computer programs. The victims of these potential or actual scams must be unaware that computer programs can generate non-random results as easily as pseudo-random sequences. In June 1998, for example, it was discovered that the Arizona state computer-based lottery had never in its history generated a number 9 in winning numbers. It is presumed that the error was due to quality assurance failures, but the same kind of problem could just as easily be deliberate.]

Category 1C *Identity, impersonation, spoofing*

1999-03-05 **child pornography Internet pedophiles journalist law**

AP, USA Today via EDUPAGE

In 1998, freelance journalist Larry Matthews of Maryland was arrested for trolling through child pornography sites on the Internet in violation of federal laws. Although Matthews pleaded guilty to the felony, he argued that he was merely trying to investigate the problem of child pornography. The judge dismissed his argument and sentenced him to 18 months in a halfway house. Matthews planned an appeal.

Category 1C *Identity, impersonation, spoofing*

1999-11-15 **child pornography police law enforcement crackdown investigation interdiction Internet**

The Times (London)

The British Home Office announced a feasibility study for the formation of a top-level unit dedicated to investigating and interdicting crime on the Internet. A particular focus of the team would be stopping the traffic in child pornography.

Category 1C *Identity, impersonation, spoofing*

1999-11-24 **Web pornography libel nude picture pornography victim policy international**

The Nation (Bangkok), AP

Angkana Timdee and two other famous Thai actresses were furious when fake pictures appeared on an Internet Web site purporting to show them in the nude — a serious matter in Thailand but not in the USA, where the Web hosting company was presumed to be unaware of the fraud.

Category 1C *Identity, impersonation, spoofing*

1999-11-29 **stalking harassment law enforcement Internet police investigation prosecution**

The Guardian

Duncan Campbell, writing in The Guardian (1999-11-29, p. 13), reported on the increasing threat of cyber-stalking. A new report by the Attorney General of the United States warned that obsessive stalkers are increasingly turning to the Internet as a tool in their campaigns of harassment. A couple of high-profile cases:

* Gary Delapenta was jailed for six years in July for having posted a young woman's address as that of a fictional sado-masochistic woman; at least six men tried to break into his victim's house. Delapenta was tricked into communicating with the victim's father, who trolled the Net looking for him and turned over enough evidence to the FBI to allow an arrest.

* Duwayne Comfort, a post-graduate student at the Catholic University of San Diego, CA was arrested after police set up a camera in the university computer lab to trace the sender of threatening e-mail messages to five women students. Comfort also hacked into the university records and lowered his victims' grades. Due to Comfort's need for a serious heart operation, he was given only a year's suspended sentence.

The US Department of Justice published a report in August on cyber-stalking; it was posted online at <http://www.usdoj.gov/ag/cyberstalkingreport.htm>.

1C1 Impersonation

Category 1C1 Impersonation

1997-01-08 **fraud impersonation**

AP

In New York, local police arrested 51 stockbrokers who allegedly paid to have two other stockbrokers take their qualifying exams in their place. The ringers charged up to $5,000 per exam. Luckily, an alert exam monitor noticed the same person showing up under different names. The National Association of Securities Dealers now requires fingerprinting and videotaping of all candidates. Samuel Maul, AP Writer, reports that the 53 people "were charged with forgery and criminal possession of forged instruments, which each carry a maximum penalty of seven years in prison, and falsifying business records and filing a false instrument, with penalties of up to four years in prison."

Category 1C1 Impersonation

2000-02-16 **impersonation penetration bad password guessing online chat**

NewsScan, CBC News http://cbc.ca/cgi-bin/templates/NWview.cgi?/news/2000/02/15/online000215

In what was billed as the first live online interview with a sitting U.S. president, CNN's chat with President Clinton turned kinky when a computer security consultant [Christopher Petro of Lorcom Technologies, an Internet company in New York] assumed Clinton's identity and changed his response to: "Personally, I would like to see more porn on the Internet." The consultant said guessing the president's nickname was an "easy trick," and that "I hope this harmless prank has served to let CNN know that this system is insecure and needs to be overhauled before someone does actual harm to them or one of their guests." Such security flaws can easily sabotage New Media journalism if not fixed, he added. (CBC News 16 Feb 2000)

Category 1C1 Impersonation

2000-06-01 **trademark domain name system hijacking theft forgery fraud authentication e-mail quality assurance QA**

NewsScan

At least two Internet companies recently suffered a dot-com's worst nightmare — their domain names were reregistered without their knowledge, and all traces of their legal ownership were erased. Web.net, based in Toronto, and Bali.com of Hong Kong both have suffered crippling losses from the hijacking, which occurred last weekend. Sleuthing by Web.net's owners found that someone in Jakarta, Indonesia had sent a forged e-mail to Network Solutions, asking them to redirect all the site's e-mail and Web site information to a new location. He then requested that the registration, which had been recorded with Network Solutions in 1993, be transferred to a Toronto registrar, and asked them to switch the ownership to someone living in Hong Kong. In Bali.com's case, an investigation shows that the name now belongs to someone living in Madrid, Spain. "These are what I call A-class domain names," says Toronto Star columnist K.K. Campbell. "If the person collected 50 of these, they'd have $5 million in assets they could afford to sit on for a little while until they're laundered and then resold." (Toronto Star 1 Jun 2000)

Category 1C1 Impersonation

2000-08-17 **identity theft SSN social security number impersonation credit-card fraud forgery**

RISKS 21 02

A Professor at Central Washington University allegedly obtained the names and social security numbers of students and presented these people as the parents of imaginary children born in Massachusetts. He forged these cyberinfants' birth certificates and then applied for identification and ultimately 40 sets of credit cards. As a result of this criminal activity, the University has revised its software to exclude use of the SSNs in class listings.

Category 1C1 Impersonation

2000-08-29 **impersonation air traffic control radio communications spoofing**

RISKS, Yahoo 21 04
http://dailynews.yahoo.com/h/ap/20000827/wl/britain_fake_air_controllers_1.html

Joe McCauley reported in RISKS, "Britain's Civil Aviation Authority has noted various cases in which `radio hackers' have commandeered air-traffic control communications, giving false instructions or fake distress calls. The number has risen from 3 in 1988 to 18 in 1999, and 20 thus far in 2000. A case at Washington's Reagan International in April 1999 was also noted."

Category 1C1 *Impersonation*

2001-05-11 **jamming emergency radio broadcasts impersonation intrusion penetration law enforcement police investigation arrest**

RISKS 21 39

The _Rocky Mountain News_ for 11 May 2001 reported on a case of dangerous hacking:

>A 16-year-old boy using a handheld radio and a computer allegedly sent Denver police cruisers and a helicopter to fake emergencies and called officers off legitimate 911 calls for more than a month before getting caught.

Police said Thursday that the teen managed to hack into the department's computer-controlled radio system, program his radio to transmit on the department's frequency from his Southwest Denver home and then took on the alias of Jerry Martinez, a fictitious Denver police officer.

The teen enjoyed chatting with police helicopters flying overhead as well as reporting non-existent emergencies and accidents.

Eventually, police dispatchers caught on. When he called requesting license-plate information, they kept him talking for an hour and a half while the FCC physically located him using "special equipment". The final straw came a couple days later when an informant talked him into modifying another radio to transmit on police frequencies. The teen was charged with a dozen misdemeanors and a dozen felonies.<

Category 1C1 *Impersonation*

2001-06-27 **e-mail SMTP headers IP address reverse lookup electoral fraud forgery impersonation criminal prosecution charges no contest nolo contendere plea Internet MS-Word properties sheet GUID globally-unique identifier**

RISKS 21 50

A report from a RISKS correspondent (name not supplied) told a story of technobumbling in the political fray of Minnesota:

Christine Gunhus, wife of former U.S. Senator Rod Gram (R-MN) pled "no contest" to charges of criminal violations of Minnesota election code. She used a pseudonymous Hotmail e-mail account to send disparaging propaganda about her husband's rival -- but failed to notice that the "X-Originating-IP:" header shows the IP address of the sender. A simple reverse IP lookup identified "the AT&T WorldNet user who repeatedly used the 'Katie Stevens" Hotmail account by connecting from Gunhus' home number. In addition to the compromising headers, the e-mail included MS-Word documents as attachments, and those documents listed Christine Gunhus as an author. The Globally Unique Identifiers (GUIDs) in the attached Word documents; "[the] GUID includes the Ethernet MAC address. Prosecutors last August obtained a search warrant to seize Gunhus' computer, from which they could extract the MAC address if the Ethernet card was still the same."

The correspondent adds an interesting comment about the effects of such stupid dirty tricks on anonymous or pseudonmous speech: "The Minnesota Civil Liberties Union reasonably argues that a criminal law that bans sending pseudonymous messages is unconstitutional. A Supreme Court decision, McIntyre v. Ohio Elections Commission < http://www.epic.org/free_speech/mcintyre.html >, says that a prohibition on the distribution of anonymous campaign literature violates the First Amendment. The state law seems to be ecumenical in its application: A Republican has used it to attack the Sierra Club < http://www.fcregister.com/ziegler11_6_00.htm >.

Cluebot story (with links):
http://www.cluebot.com/article.pl?sid=01/06/15/0135212&mode=nocomment

Minnesota Public Radio story on original affidavit:
http://news.mpr.org/features/200009/08_radila_grams/index.shtml

---

Category 1C1 *Impersonation*

2001-08-07 **bank credit card fraud countermeasures identification authentication I&A mutual protocol failure design spoofing impersonation**

RISKS 21 59

Michael Bacon identified a problem in the credit-card fraud countermeasures used by his bank. Called by someone claiming to be the bank's fraud department to check on unusual buying patterns, he requested a method of verifying _their_ identity before revealing his authentication information. Apparently no one had ever thought of checking to see if the caller were legitimate bank employees. He settled the problem in an imaginative way: "After much discussion and calling two supervisors, we agreed that they would tell me the last two purchases I had made on that card (approximately 1 hour and 20 minutes beforehand respectively from two different stores). If they could, then they were probably from the bank, and I would authenticate myself to them." He added, "The RISKS are clear. You supply some 'secret' data to the bank so that they can authenticate you when you call them. But there is no simple way to authenticate the bank when it calls you. You can't ask for the number and call them back, because you have no way of authenticating the number given. They're ex-directory, so you can't confirm it through Enquiries, and they withhold the number so the CLI doesn't show! If you blindly supply the data (as clearly many people do), then you may be divulging to a crook the 'secrets' necessary to authenticate yourself to the bank. The bank has not thought to provide any means of authenticating themselves. I suspect this to be endemic."

Category 1C1 *Impersonation*

2002-01-24 **spoofing forgery impersonation voting information warfare**

RISKS 21 89

Nick Brown wrote about a case of e-mail spoofing that backfired because of a spelling mistake. As he reported in RISKS, "An e-mail was sent from the account of the mayor, telling members of a city commission to vote in favour of a plan to extend a local hypermarket. The official, public policy of the city council and the mayor is to oppose this extension. The mail to one member of the commission bounced, because the recipient's name was incorrectly spelled. An assistant to mayor Fabienne Keller, who has access to her mailbox, noticed the "undeliverable" reply and determined that the mail had been sent at a time when the mayor could not have sent it. The general manager of the hypermarket is under police investigation for illegal entry into a computer system, forgery, use of forged documents, and attempted fraud."

[French references:]
http://www.dna.fr/cgi/dna/motk/idxlist_light?a=art&aaaammjj=200201&num=18041610&m1=keller&m2=mairie&m3=
http://www.dna.fr/cgi/dna/motk/idxlist_light?a=art&aaaammjj=200201&num=19049910&m1=keller&m2=mairie&m3=

Category 1C1 *Impersonation*

2002-10-03 **social engineering psychology deceit impersonation trickery penetration**

NewsScan

DECEIT, NOT TECHNOLOGY, IS THE REAL MENACE TO SECURITY
Reviewing Kevin Mitnick's new book "The Art of Deception: Controlling the Human Elements of Secrecy," Simson Garfinkel writes in the Christian Science Monitor: "Although some will accuse Mitnick of creating a handbook that teaches crooks how to break into organizations, the truth is that we all need to understand these con games to protect against them. To stress this point, his last two chapters contain policies, procedures and training that companies can implement to further protect themselves. In keeping with his premise that the most damaging security penetrations are the result of deceit - not technical penetration - almost none of Mitnick's suggestions is technical in nature. The most important recommendation is that when somebody contacts you claiming to be from your organization, you need to verify that they are working for your organization no matter whether they are asking for your help, offering to help you, or just trying to be friendly." (Christian Science Monitor 3 Oct 2002)
http://www.csmonitor.com/2002/1003/p15s02-bogn.html

Category 1C1 *Impersonation*

2003-02-07 **impersonation fraud misrepresentation lies journalist worm**

NewsScan

REPORTER PERPETRATES WEB HOAX ON FELLOW JOURNALIST
Although it violates journalistic ethics for a reporter to misrepresent his identity, freelance journalist Brian McWilliams (whose work has appeared Salon and Wired News) used a fake Web site and phony to deceive Computerworld's Dan Verton into believing that he was a Pakistan-based terrorist who unleashed the recent Slammer network worm on the world. Computerworld published, then quickly retracted, Verton's story. McWilliams says he wanted to teach reporters "to be more skeptical of people who claim they're involved in cyber-terrorism." Computerworld editor-in-chief Maryfran Johnson says, "I couldn't believe a journalist could do this to another journalist," and Verton says, "I feel like I've been had, and that's never an easy thing to swallow. So, I'm left here scratching fleas as the price you sometimes pay for sleeping with dogs." (AP/San Jose Mercury News 7 Feb2003)

Category 1C1 *Impersonation*

2004-02-26 **e-mail spoofing stop solutions Microsoft Yahoo**

NewsScan

PUTTING AN END TO SPOOFING

To stop Internet "spoofing"— the sending of mail from someone who pretends to be someone else — Microsoft and Yahoo are each developing systems aimed at authenticating senders of e-mail, as are companies such as America Online, Sendmail, Brightmail, and Amazon. Microsoft's proposal (Caller ID for E-mail) would require Internet service providers to submit lists of unique numeric addresses for their mail servers so that, on the message receiving end, software could check a database to verify that a message actually originated from one of its registered machines. Yahoo's proposal (DomainKeys) would use encryption to digitally sign messages, and if the sender or message content were altered the signature would get rejected. Experts predict that some combination of the techniques will be ready for use later this year. Margaret Olson of the Email Service Provider Coalition's technology committee says that once enough service and software providers adopt the technology, "getting unauthenticated mail delivered will be extremely difficult." (AP/USA Today 26 Feb 2004)

Category 1C1 *Impersonation*

2004-03-01 **electronic mail e-mail security privacy authentication identity spoofing**

NIPC/DHS

February 26, Associated Press — Companies work on E-mail identity system.

With a simple adjustment in your e-mail software, you can pretend to be anyone. This is known as spoofing. To close that loophole, Microsoft and Yahoo! Inc. are each developing systems aimed at authenticating senders of E-mail. America Online is testing a third. "Having E-mail come in, and not really being able to identify where it comes from, this is a huge security hole," Bill Gates, of Microsoft, said this week in announcing specifications for his proposal. Microsoft's proposal, known as Caller ID for E-mail, calls for Internet service providers to submit lists of unique numeric addresses for their mail servers. On the receiving end, software would check a database to verify that a message said to come from an e-mail provider actually originated at one of its registered machines. In January, AOL began testing a similar system called Sender Policy Framework (SPF), which checks a different part of the message. Yahoo's proposed solution would use encryption to digitally sign messages. If the sender or message content is altered, the signature gets rejected. Issues to be worked out for all three systems include how to properly send E-mail from cybercafes, hotels, and public Wi-Fi hotspots and how to preserve privacy when using anonymous re-mailers, which are used by whistleblowers and others to intentionally mask the origin of messages.

Category 1C1 *Impersonation*

2004-09-04 **spoofing telephony caller-ID criminal hackers threats entrepreneur**

NYT http://www.nytimes.com/2004/09/04/technology/04caller.html

Jason Jepson, an entrepreneur who tried to offer a commercial service that would have allowed callers such as debt collectors to fool callerID systems by feeding them incorrect identifying information -- spoofing the callerID system -- received a death threat along with harassing e-mail and phone calls and decided to abandon the idea only three days after his announcement. The company, Star38, would have charged a fee to trick call recipients into answering the phone and could have helped criminals trick victims into revealing confidential information under the mistaken belief that they were speaking to trustworthy callers based on the forged originating phone numbers.

Category 1C1 *Impersonation*

2004-10-27 **caller ID spoofing impersonation Website open security privacy implication White House call origination spoof**

DHS IAIP Daily; http://www.securityfocus.com/news/9822

October 27, SecurityFocus — New Caller ID spoofing site opens.

A new Website offers subscribers a simple Web interface to a caller ID spoofing system that lets them appear to be calling from any number they choose. Called "Camophone," (www.camophone.com) the service functions much like the Star38.com (www.star38.com) site that struggled with an abortive launch last month: a user types in their phone number, the number they wish to call, and the number they'd like to wear as a disguise. The system instantly dials back and patches the call through with the properly-forged caller ID. The Star38.com site relaunched this week as a tool offered exclusively to law enforcement officials and "intelligence agencies." In contrast to Star38, Camophone is open to anyone with a PayPal account, at a rate of five cents per minute, pre-paid. The Camophone site performed as advertised in a test by SecurityFocus, in which a reporter made phone calls appear to originate from the White House switchboard.

1C2 Identity theft

Category 1C2 Identity theft

2000-01-16 **identity theft case studies prevention**

Los Angeles Times

Caitlin Liu of the Los Angeles Times published a thorough report on identity theft on January 16 (front page). In one case, 22-year-old San Diego college student Jessica Smith had her car stolen — with her handbag inside. Although the car and bag were recovered, someone stole her identity. She nearly got fired from her new job when a background check showed that "she" had outstanding warrants for prostitution. She was unable to obtain credit, phone service or even to rent an apartment. With the help of a sympathetic police investigator, Smith was able to prove her innocence of the charges — a reversal of the usual burden under criminal law, where usually the state has to prove guilt. She obtained judicial documents explaining that her identity had been stolen; nevertheless, she has been hauled into police stations to be fingerprinted to prove that she is indeed the person authorized to carry those documents.

Image Data LLC, an identity-fraud prevention service based in Nashua, NH, commissioned a study in September 1999 that suggested that one out of five Americans or a member of their family have been victimized by identity fraud. [Readers should always be wary of statistics that report how many "members of your family" or "people you know" have particular characteristics: it is possible that a single person can be reported by multiple people. The over-counting bias increases as a function of sample size and of social relationships among the sample population.]

Category 1C2 Identity theft

2000-07-13 **identity theft impersonation credit-card fraud legislation law proposal**

NewsScan, Washington Post http://www.washingtonpost.com/wp-dyn/articles/A31663-2000Jul12.html

U.S. Senators Jon Kyl (R-Ariz.) and Diane Feinstein (D-Calif.) have introduced a bill to reduce the chances of identity theft, which Feinstein says "any thief with a computer can do anonymously," because "the Internet is making it very easy." The bill would require credit-card issuers to confirm any change of address with a cardholder within ten days, and would require "fraud alerts" to be conspicuously placed on credit reports once a consumer notifies a credit bureau of identity theft. The FTC site on identity theft is www.consumer.gov/idtheft/. (Washington Post 13 Jul 2000)

Category 1C2 Identity theft

2000-07-18 **identify theft privacy social security number SSN database disclosure Web**

RISKS 20 95

Given the foolish reliance of many credit-card companies and financial institutions on one's mother's maiden name as an authentication mechanism, the State of Texas has recently taken a giant step in increasing identity theft: they put birth records on the Web. Bill Tolle reported to RISKS, "Go to < http://userdb.rootsweb.com/tx/birth/general/search.cgi > .Enter `Smith' as Surname. Leave all other fields blank. The search engine will return 35,072 names (first, last, and middle) with birth dates and the Mothers Maiden name (first, last, and middle) and Father's name (first, last, and middle)."

Category 1C2 Identity theft

2000-09-25 **identity theft fraud government**

RISKS 21 07

Peter G. Neumann reported a shocking case of irresponsibility at a government service: "An AP item (seen by me on the front page of the *Palo Alto Daily News*, 25 Sep 2000) says that the California Department of Motor Vehicles issued over 100,000 fraudulent drivers' licenses in 1999, and typically makes little or no effort to check the validity of the 900,000 duplicate license requests it receives each year. Examples include duplicate licenses issued to people of the wrong race or the wrong gender, and in one case bogus duplicates of a particular individual's license to 18 different people. The driver's license is called a ``breeding document'' for identity thieves, leading to financial fraud, ruined credit, purchases of firearms by felons, and other misuses. DMV officials claim that implementing an on-line photo-retrieval system would cost $3 million over the next two years. This seems like a useful system — especially if it were used pervasively."

Category *1C2* *Identity theft*

2000-12-12 **automobile drivers identity license forgery theft counterfeit break-in**

RISKS 21 15

In Gresham, OR, thieves broke into the state Department of Motor Vehicles office and, in less than two minutes, stole equipment for forging drivers' licenses plus computerized information about 3,215 recent holders of valid licenses. Such information and equipment is ideal for creating bogus identification documents and contributes to, among other crimes, theft of identity.

Category *1C2* *Identity theft*

2001-01-17 **identity theft bogus accounts fact-checking background quality assurance design**

NewsScan

IDENTITY THIEVES MAY HAVE OPENED AN ACCOUNT FOR YOU
Fraud investigators are reporting that one of the common strategies used by identity thieves is to open a new account with a utility company under the name of the person whose identity they are trying to assume. The address on the account could be anywhere, because utility companies typically check only names and credit worthiness. Another trick used by scam artists is to generate bogus credit card numbers and then attach the real names and addresses of the people whose identity they plan to steal. By doing this they are relying on the fact that the verification process of online merchants is usually restricted to name, address, and phone number, and doesn't reveal until later the fact that the credit card number is a work of fiction. (USA Today 16 Jan 2001)
http://www.usatoday.com/life/cyber/tech/ctj001.htm

Category *1C2* *Identity theft*

2001-02-28 **identity theft personal information confidentiality impersonation fraud international**

RISKS 21

Keith A Rhodes wrote in RISKS about a system penetration at Indiana University that raised fears of identity theft: "A user browsing from Sweden stored music and video files on a server at Indiana University that had apparently been left unprotected after a crash. IU realized it had a problem when huge increases were noted in network traffic. In the process, they also noted that a file of over 3,100 student names and SSNs had been copied from the server. Associate Vice President Perry Metz contacted the Social Security Administration about what might be an appropriate reaction, and said that they told him ``it's unlikely and unusual for someone who has your Social Security number to be able to do anything with it. Normally, financial institutions require additional information." [Is that reassuring to RISKS readers? Sources: Swedish hacker breaches IU server; Culprit stored music, video files on system and also downloaded private student data, AP item 28 Feb 2001, and article by John Meunier, *Herald-Times*, 28 Feb 2001; PGN-ed]"

Category *1C2* *Identity theft*

2001-03-20 **identity theft impersonation fraud public records confidentiality Web**

RISKS 21 29

RISKS moderator Peter G. Neumann wrote a brief summary of a recent arrest with implications for theft of identity; his item started with the punning title, "Identity theft: Forbes-ing a head?" His comments were as follows:

>In RISKS, we have for many years been warning about the burgeoning increase in identity theft. The following case could foster a broader awareness of the depth of the problem, but then again most folks still seem to have their heads in the sand -- unless they have already been burned.

Abraham Abdallah was arrested on 7 Mar 2001, a 32-year-old Brooklyn NY high-school dropout working as a busboy, and already a convicted swindler. Although he was arrested as he was picking up equipment for making bogus credit cards, he is suspected of already having stolen millions of dollars. In his possession were SSNs, addresses, and birthdates of 217 people whose names appeared in a Forbes Magazine itemization of the 400 richest people in the U.S. He reportedly also had over 400 stolen credit-card numbers, and had used computers in his local library to access of the Web for information gathering. He is being held on bail of $1M. His activities were detected after an e-mail request to transfer $10M from a Merrill Lynch account, whereupon authorities found mailboxes he had rented in various names and other evidence. His defense attorney said Abdallah is innocent, and that prosecutors had ``made an unfair leap from possession of this information to an inference that there was an attempt to take money." [PGN-ed from a variety of sources, including an AP item by Tom Hays http://www0.mercurycenter.com/premium/business/docs/forbes21.htm; Thanks to Dave Stringer-Calvert and to Michael Perkins at Red Herring]<

Category 1C2 *Identity theft*

2001-03-21 **identity theft impersonation government documents national identifier driver's license public access confidentiality**

RISKS 21 29

Peter V. Cornell reported in RISKS on the recent declaration of the California driver's license and ID card as the primary identification document for the state. Mr Cornell wrote, "Courtesy of the California legislature, *anyone* who has a fake California drivers license with YOUR correct data, but with *his* picture and *his* version of your signature, can steal your money in many different ways. For example, if he knows your Social Security Number, bank, and account number, (easily obtained online or by mail theft) he can walk into any branch office and receive cash. Tens of thousands have been stolen from my (no longer existent) Wells Fargo accounts. . . . With that fake drivers license, that fraudster becomes YOU. All he need do is write a bad check drawn on another bank's bogus name account set up for that purpose, with the victim (you) as payee. He then walks into (in my case) a Wells Fargo branch and, impersonating the victim, cashes the check. When the check bounces, Wells Fargo (probably others, too) simply debits the victims account."

In addition, writes the correspondent, "The banking industry has arranged the law (California Commercial Code Sections 4401-4407 and 3101-3119) to ensure that the customer takes the hit. So that, among other conveniences, THE LAW allows banks to rely *solely* on the CDL data to confirm the identity of a customer with no risk exposure whatsoever. 'IF THE CUSTOMER PROVES' means you must sue the bank. They have it written so you'd lose anyway, but the amounts, however painful, are not nearly enough to pay a lawyer."

In riposte, attorney John Noble contributed a detailed rebuttal of Cornell's description of the California Commercial Code. He wrote, in part, "Mr. Cornell's description of the CA Commercial Code leaves out the good parts. An account may be debited if the item was 'properly paid,' i.e. 'authorized' in fact. If the item was not authorized, the customer need only notify the bank within a reasonable time after receiving his statement to have the account re-credited -- the burden is on the bank to prove that the endorsement was genuine, which is impossible. Banks typically ask the customer to sign an affidavit; and they pull the video sequence of the transaction at the teller window to confirm that the customer did not cash the check himself (the unlikely exception to the impossibility of proving the endorsement was genuine). Mr. Cornell points to Code provisions that require the victim to "prove" that the bank failed to exercise 'ordinary care.' But the provision only applies to losses caused by the customer's failure to review his bank statement and report an unauthorized debit within a reasonable time. In effect the bank is strictly liable for unauthorized debits during the first 6-8 weeks on little more than the customer's insistence that they were unauthorized. But if the customer doesn't look at his statement and report the unauthorized transactions disclosed on the statement, the bank's liability is cut off and the customer is stuck with the additional losses. The reasons for this are obvious. Only the customer is in a position to know that the debit was unauthorized. If he doesn't look at his statements, and the same guy is cleaning him out month after month, whose fault is that? In addition, the law has to take into account the possibility that the customer is having his own checks cashed by a third party. . . . The moral of the story: review your bank statements -- it's part of the deal."

Category 1C2 *Identity theft*

2001-03-25 **identity theft social security number SSN fraud driver's license theft law enforcement justice system probation**

RISKS 21 31

Tom Goltz described a theft of his identity in some detail in RISKS:

>I am white. I have held a California driver's license in the past, but that license has been inactive for over two years since I established residency in another state.

In October of last year, a black male obtained a fake California driver's license with my name on it and his picture. The driver's license ID # he used belongs to a white female. The address is a Commercial Mail Receiving Agency in Costa Mesa CA, which the state doesn't normally allow. The fake also contained two spelling errors.

This person used this ID and my social security number to open a dozen different credit accounts in my name at various locations around the Los Angeles area. He was using a cell phone with a phone number based in the 603 area code as his residence phone.

If anyone had bothered to look, just about everything about this guy screamed fraud, yet he managed to steal $15,000 worth of merchandise (mostly jewelry).

Out of all these people who were supposed to be checking this information, only TWO found problems. One was a used car dealer who became suspicious when the check this guy gave for the down payment proved to be bogus. They refused to give the guy the car, but didn't bother to pursue the matter with the police. The other was store security at a Costco in Las Vegas, who tracked me down in New Hampshire and informed me that I had a problem. They detained the man, and turned him over to the police.

Sadly, the most he's going do is a couple of years probation - he didn't actually steal anything in Las Vegas, and the identity theft, although a crime in NV is not sufficient to assure jail time by itself. I discussed the matter of extraditing the varmint to California with Las Vegas police, but they told me that it was unlikely that California would bother for something that would only net the offender probation there as well. According to the LV police detective, in California, you have to be charged with stealing over $50,000 before you'll do any jail time.

It's no wonder this crime is exploding...it's low risk, extremely profitable, and trivial to implement.

Oh yes...how did he get my name and social security number? He told the Las Vegas police that he purchased the information on the street for $500.<

Category 1C2 *Identity theft*

2001-05-11 **social security number SSN drivers license permit state federal law identity theft privacy government legislation court ruling judgement**

RISKS 21 39

Brett Glass published a chilling report in RISKS about changes in federal law that _require_ applicants for state drivers' permits to submit their Social Security Numbers. Glass wrote, "What I found out was chilling. Not only does Federal Law -- thanks to the striking of a single word from a huge statute -- require that drivers submit their Social Security numbers when applying for licenses. It also requires that all of the information maintained about a driver by a state -- including that number -- be revealed to virtually all comers. Here are the details of these onerous laws, along with additional information about the laws in my particular state (which are typical of state laws throughout the country). I'll also describe the way in which one state is fighting the Federal laws that would require it to compromise its citizens' privacy and subject them to trivially easy identity theft."

It seems that changes in welfare reform legislation removed the word "commercial" from existing requirements that applicants for commercial drivers' licenses submit their SSN. In addition, amendments to the "Drivers' Privacy Protection Act" now require that "ALL of the information you submit to your state's DMV/DOT [be] available to *anyone* who claims that it's needed for any business purpose. If I wanted your driving records and SSN, all I'd have to do is walk into the courthouse and claim that you owed me a dollar." Athough the amended act "was challenged by the Alabama Attorney General on states' rights grounds and was ruled unconstitutional by a Federal district court" it was upheld by the Supreme Court of the United States.

Mr Glass provides much more extensive documentation and detail in his report.

Category 1C2 *Identity theft*

2001-05-31 **identity theft social security number abuse**

NewsScan

IDENTITY THEFT
Identity theft is an increasing problem in the Information Age, and brokerage companies sometimes unwittingly sell dossiers to people using fake credit card and posing as other people. In one scam, thieves used an e-mail account and a stolen credit card number to purchase reports containing Social Security numbers, employment information and driving records, and were able to use this information to plunder bank accounts. One victim of identity theft said: "What has taken me a lifetime to build -- my trust, my integrity and my identity -- has been tainted. I don't know if I'm dealing with a 14-year-old messing around with a computer or if I'm dealing with organized crime." The Social Security Administration's inspector general says the power of the Social Security number makes it a valuable asset subject to limitless abuse, and calls that misuse has developed into "a national crisis." (Washington Post 31 May 2001)
http://washingtonpost.com/wp-dyn/articles/A77996-2001May25.html

---

Category 1C2 *Identity theft*

2001-08-09 **national identification number cellular phone wireless transmission eavedropping encryption password access code identity theft**

NewsScan

FINLAND MULLS PUTTING NATIONAL IDs ON CELL PHONES
The Finnish government is considering using SIMs -- the subscriber information modules inside every cell phone -- to take the place of its national identity card, and eventually even a passport. Under the plan, the computer chip embedded in every SIM would store personal information, transforming the SIM into a person's legal proof of identity. Of course the drawback would be what would happen if you lost your phone -- about 9,000 cell phones are left on the London Underground alone every year. The solution, according to Roger Needham, manager of Microsoft's British research lab, is to store the information on secure servers accessible via a WAP connection to the Web. The SIM in this case would store only a personal identifier -- an encryption key -- that the owner would have to punch in a PIN to use. The Finnish government is already taking the initiative with a national technical standard called FINEID. Currently FINEID uses a smart card and a card reader attached to a PC, but the plan is to migrate to an SIM, says Vesa Vatka of the Finnish Population Register Center in Helsinki. (New Scientist)
http://www.newscientist.com/hottopics/tech/yourphoneisyou.jsp

---

Category 1C2 *Identity theft*

2001-11-09 **national identity card civil liberties anonymity privacy**

NewsScan

CYBERSECURITY CHIEF NOT INTERESTED IN NATIONAL ID CARD
Bush Administration cybersecurity chief Richard Clarke is showing little interest in a proposal from Oracle's Larry Ellison to create a national identity card as part of the nation's response to the dangers posed by terrorists. Clarke says that no one he's talked to in the administration thinks it's a good idea, and civil liberties groups have uniformly opposed the plan. (ZDNET/USA Today 9 Nov 2001)
http://www.usatoday.com/life/cyber/zd/zd1.htm

Category 1C2 *Identity theft*

2002-04-04 **IRS tax confidentiality penetration security Web encryption plaintext cleartext**

Security Wire Digest 4 26

Sandra Kay Miller reported on the growing identity-theft problem in the US in an article published in the Security Wire Digest. The Federal Trade Commission (FTC) noted that about 400,000 victims experienced identity theft in 2001. Miller pointed out that access to tax forms -- including electronically submitted documents -- is a valuable source of information for identity thieves. She wrote, "Last year, the General Accounting Office reported that during security audits, IRS firewalls on e-filing systems did not effectively restrict external access to network, stored unencrypted e-filed returns on systems, practiced poor password management and had very little intrusion detection capability." In addition, some commercial tax preparers also demonstrate shoddy security, although the leading firms seem to protect their clients' data.

Category 1C2 *Identity theft*

2002-06-27 **identity theft spoofing risk Web design credit card**

RISKS; 22 13
http://www.cnn.com/2002/TECH/internet/06/26/identity.theft.ap/index.html

Conrad Heiney, writing in RISKS, identified a poorly-thought-out design for an anti-fraud site on the Web: > [A] nongovernmental organization called CardCops is providing a service in which consumers can check to see if their credit cards have been abused in some way.

The check is done by visiting the website and entering your credit card number.

The RISKS here are bad enough to be humorous. Although CardCops themselves appear to be a legitimate organization (at least at time of press) , and do not themselves ask for the expiration date required to complete a transaction, there's no protection against copycat websites whose intent is entirely evil, or telephone scams based on the CardCops publicity. The quality of the data is another obvious minefield.<

Category 1C2 *Identity theft*

2002-08-01 **social security number SSN privacy consumer identity theft**

NewsScan

SIMSON SAYS: STOP TOSSING SOCIAL SECURITY NUMBERS AROUND
Privacy advocates have said, and said, and said again, that companies shouldn't use Social Security numbers as identification numbers or passwords -- yet colleges and banks and all kinds of other companies have turned a deaf ear to that plea, because they've been trying to balance security concerns with customer convenience. But Simson Garfinkel, author of Database Nation (and NewsScan Daily contributor), says: "It is the reason we have an epidemic of identity theft right now. The problem here is that people treat the Social Security number as if it is a secret, when in fact it is not." Would new legislation do any good? Garfinkel says no: "We should accept the fact that the Social Security number is a universal identifier, and we should treat it as a public record. Businesses should not use a Social Security number as a password any more than they should use a name." (USA Today 31 Jul 2002)

Category 1C2 *Identity theft*

2003-02-28 **fraud misrepresentation impersonation spoofing privacy confidentiality**

NewsScan; NIPC/DHS

MONSTER.COM WARNS JOB-SEEKERS ABOUT POTENTIAL ID THEFT

Monster.com, a job-seeker's Web service whose database holds a quarter of a million resumes, has issued an e-mail message to its customers warning that "regrettably, from time to time, false job postings are listed online and used to illegally collect personal information from unsuspecting job-seekers." What should job-seekers do to protect themselves? Monster.com advises them not to give out their social security, credit card or bank account numbers, not to disclose marital status or other information not relevant to their job qualifications, and to be especially careful when responding to job-postings from prospective employers outside the country. (AP/San Jose Mercury News 28 Feb 2003)

February 28, Associated Press — Monster.com warns job seekers of ID theft. An e-mail labeled a "critical service message" is being sent from Internet job board Monster.com to all active users of Monster's main site. It cautions that "from time to time, false job postings are listed online and used to illegally collect personal information from unsuspecting job seekers." Pam Dixon, a research fellow with the Denver-based Privacy Foundation, said the e-mail confirms a growing hazard for online job seekers. "It's not just on Monster. I've heard of this on all the major sites." Dixon said most of the cases she's familiar with involve job seekers who have provided credit card numbers, social security numbers or agreed to ship overseas materials that are prohibited from being sold outside U.S. borders. Company spokesman Kevin Mullins said he did not know exactly how many people would receive the e-mail, but that it is "definitely well into the millions." Monster, the nation's largest Internet job board, says it has 24.5 million resumes posted on its main site. Mullins said the warning was not precipitated by any specific incident. Instead, the company is merely trying to protect its users, he said.

Category 1C2 *Identity theft*

2003-09-02 **identity theft microsoft e-commerce coalition ITAA fighting online financial institutions**

NewsScan

COALITION FORMED TO BATTLE IDENTITY THEFT
The Information Technology Association of America has organized a new coalition aimed at fighting identity theft. The Coalition on Online Identity Theft, which includes e-commerce giants Amazon, eBay and Microsoft among its members, plans to launch a public education program and will encourage its members to work more closely with law enforcement officials to fight online crime. According to the Federal Trade Commission, the number of U.S. consumers who complained about some sort of identity theft nearly doubled last year to 162,000, but the Gartner Group says that statistic only scratches the surface of the problem. It estimates that 3.4% of U.S. consumers — some 7 million adults — suffered some form of identity theft in the past year. A report issued by Gartner in July says that while a consumer education campaign may make online users more savvy, there's still a major problem in the way ID theft cases are handled by financial institutions, who tend to treat such fraud as the cost of doing business rather than a crime against their customers: "There is a serious disconnect between the magnitude of identity theft that innocent consumers experience and the industry's proper recognition of the crime. Without external pressure from legislators and industry associations, financial services providers may not have sufficient incentive to stem the flow of identity theft crimes." (CNet News.com 2 Sep 2003)

Category 1C2 *Identity theft*

2004-01-05 **identity theft social security SSN video rental fraud Hollywood Video**

NewsBits; http://www.usatoday.com/tech/news/2004-01-05-ssn-id-theft_x.htm

Identity theft often begins with Social Security number

An article in USA Today for 15 January 2004 by William McCall of the Associated Press reviews excessive use of the Social Security Number. Despite increasing use of the identifier on commercial forms such as video-store rental applications, US residents have no legal obligation to reveal their SSN except for a few government, employment and fanking requirements. Retailers may refuse to grant services if a customer refuses to reveal the SSN, but the customer can take business elsewhere. Some untrained workers with access to SSN have been shown to reveal the information for unauthorized use; a reporter was able to acquire this information for two people with nothing more than providing his own street address.

Category 1C2 *Identity theft*

2004-04-30 **identity theft snail mail**

DHS IAIP Daily; http://www.stamfordadvocate.com/news/local/state/hc−30081128.apds.m0926.bc−ct−brf−papr30,0,4492031.story?coll=hc−headlin es−local−wire

April 30, Associated Press — Postal clerk accused of identity theft.

A postal clerk in the Stamford, CT, police office has been charged with identity theft. Gail Worthington was arrested Wednesday, April 28, in a joint investigation by U.S. Postal Service inspectors and East Haven police. Worthington is accused of using information she obtained while at work to get credit cards in other people's names and use the cards to buy merchandise from high-end stores. The arrest was based on evidence found in a search of Worthington's East Haven apartment on March 10.

Category 1C2 *Identity theft*

2004-05-01 **identity theft phishing Internal Revenue Service IRS**

DHS IAIP Daily;
http://edition.cnn.com/2004/TECH/internet/04/30/identity.the ft.ap/

May 01, Associated Press — IRS warns taxpayers about identity theft e-mails.

TheInternal Revenue Service (IRS) on Friday, April 30, warned consumers about an identity theft operation that tries to elicit personal information from taxpayers by sending e-mails alleging they're the subject of a tax investigation. Neither the Department of Treasury nor theInternal Revenue Service send e-mails to taxpayers about issues related to their accounts. The official-looking e-mail tells recipients they can dispute the tax fraud charge by logging onto a Website and providing detailed personal information like Social Security numbers, credit card numbers and driver's license numbers. Identity thieves use individuals' personal data to create false identification documents, to purchase goods and to apply for loans, credit cards or otherservices in the victim's name. The Internet service provider that hosted the fraudulent web siteshut it down at the request of the Treasury Department's inspector general for taxes. The IRS warns that new versions could surface.

Category 1C2 *Identity theft*

2004-05-08 **hacking identify theft university computer breach**

DHS IAIP Daily;
http://www.fox23news.com/news/national/story.aspx?content_id =5278A633−C320−4F76−B1AB−AA431F5CAB16

May 08, Associated Press — Computer system at University of California, San Diego, hit by hackers.

Hackers broke into the computer system of the University of California, San Diego (UCSD), compromising confidential information on about 380,000 students, teachers, employees, alumni and applicants. Hackers infiltrated four computers that stored Social Security and driver's license numbers in the university's business and financial services department. Investigators are unaware of any illegal use of the data. University officials discovered the security breach April 16 after noticing a spike in traffic on the network. Last month, the San Diego Supercomputer Center, which is on the UCSD campus, was infiltrated by a hacker, although officials said no critical information was lost.

Category 1C2 *Identity theft*

2004-05-10 **identity theft social security numbers cards**

DHS IAIP Daily; http://www.suntimes.com/output/news/cst−nws−identity10.html

May 10, Chicago Sun-Times — State cracks down on identity theft.

In an effort to fight the growing problem of identity theft, the state of Illinois is cracking down on phony Social Security numbers on driver's licenses and ID cards. Secretary of State Jesse White said that Social Security numbers on four percent of Illinois driver's licenses and ID cards don't match records from the Social Security Administration. In many cases, there's no fraud involved. Examples of innocent mix-ups include motorists who use their middle names or change their names after getting married. However, from now on, motorists with suspect Social Security numbers will be required to prove their identity when they renew their licenses. The secretary of state is taking several other steps to combat identity fraud, in which someone steals the identity of someone else, often by assuming their name or other personal information. The office has stopped printing Social Security numbers on driver's licenses and is adopting more stringent document requirements. It also is using facial recognition programs that compare digital photos of motorists.

Category 1C2 *Identity theft*

2004-05-11 **identity theft children fraud popularity increase**

DHS IAIP Daily; http://www.klas−tv.com/Global/story.asp?S=1859775&nav=168XN2 pW

May 11, KLAS-TV.com (NV) — Child identity theft gaining in popularity.

A new variation of identity theft is gaining in popularity, a variation law enforcement says is even tougher to crack. It's child identity theft -- a crime that can go undetected for years. Identity theft expert Roy Michael says over the past five years, about 500,000 cases of child identity theft have been uncovered. However, half of those cases have come in the past two years. Children are targets because thieves can often get a 10 to 15 year head start on law enforcement. In fact, most children who've had their identity stolen don't know it until they someday go to apply for credit, a student loan, or buy a car. That's why identity theft experts say every parent should run a credit check on their child. A child's identity can sometimes get into the wrong hands through unsuspecting sources, for example, clubs or sports in which they participate, because they may require proof of age.

Category 1C2 *Identity theft*

2004-05-11 **identity theft paper trail victims**

DHS IAIP Daily;
http://www1.redding.com/redd/nw_local/article/0,2232,REDD_17533_2876398,00.html

May 11, Record Searchlight (CA) — Identity theft probe follows paper trail.

A former U.S. Bank employee arrested on suspicion of identity theft could be facing more charges in the near future. U.S. Bank's corporate security division is investigating Kenneth David Easley of Redding, CA, on suspicion of providing customer account information and counterfeit checks for others to cash, Redding police Sgt. Paul Grooms said Monday, May 10. "They're looking at victims throughout the West," he said. Easley was arrested April 8 following a month-long probe resulting in allegations that he gave account information and fake checks to three friends in Southern California. Grooms said Easley also is accused of creating counterfeit checks, although he would not say when, where or how he did it. Easley was a teller at the bank's main Redding branch. Approximately $41,000 was stolen from two account holders at that branch and from another branch, Grooms said.

Category 1C2 *Identity theft*

2004-05-13 **identity theft ring gang organized crime Colorado police**

DHS IAIP Daily; http://www.koaa.com/news/view.asp?ID=2236

May 13, KOAA-TV (CO) — Identity theft ring closer to being solved.

Colorado Springs Police are closing in on the last of their organized crime suspects in the widespread identity theft case they've been working since last November. A 29-year-old man turned himself into Denver Police, after a warrant was issued last month for his arrest on Colorado organized crime charges. Three others have already been arrested. Investigators believe they ran a massive identity theft ring that included check forgery, credit card theft, car break-ins and burglaries, with hundreds of victims all across southern Colorado. Police say a number of the crimes are tied back to methanphetamine.

Category 1C2 *Identity theft*

2004-05-13 **identity theft victim assistance program Ohio**

DHS IAIP Daily; http://www.nbc4columbus.com/money/3300186/detail.html

May 13, Nbc4columbus.com (OH) — Ohio gets grant to help identity theft victims.

The federal government gave the Ohio attorney general's office a $250,000 grant to help implement a program aimed at assisting victims of identity theft, Attorney General Jim Petro announced Thursday, May 13. Petro said an Identity Theft Passport will be unveiled this summer that will allow victims to apply for a card when they file police reports with law enforcement agencies. The victims will be issued a card and certificate that can be shown to officers, creditors and others who question them. "The U.S. Department of Justice recognizes that our pilot program has the potential of being replicated nationwide," Petro said.

Category 1C2 *Identity theft*

2004-05-17 **identity theft banking scams phishing Australia bank Westpac**

DHS IAIP Daily;
http://www.smh.com.au/articles/2004/05/17/1084646119834.html

May 17, Sydney Morning Herald (Australia) — Westpac targeted by more scams.

Australian bank Westpac is once again being targeted by e-mail scams which seek to extract usernames and passwords used for online banking. Two e-mails are doing the rounds, purportedly from Westpac Service Center or Westpac Support. Both attempt to lure unsuspecting souls to the same site: 207.150.192.12/temp/artsplos/secur.html. Only users of Internet Explorer are vulnerable to the scam. As soon as one inputs a username and password and clicks on the "sign-in" link, the genuine Westpac home page comes up.

Category 1C2 *Identity theft*

2004-05-19 **identity theft stolen social security numbers Utah**

DHS IAIP Daily; http://www.4utah.com/local_news/local_headlines/story.aspx?content_id=6C104ABD−79C2−4BC4−93FE−ED72A7D84923

May 19, ABC 4 (UT) — Scam using stolen social security numbers in Utah.

An ongoing investigation by federal and state agencies has found that 87 homes in Utah have been purchased using stolen Social Security numbers. So far, 21 individuals, all illegal immigrants, have been charged with felony crimes including identity theft, communications fraud, and forgery for their part in the scam. The scheme combines mortgage fraud with identity theft. Brokers target illegal immigrants in grocery store parking lots, and offer them the opportunity to buy a home despite their lack of credit or jobs. The undocumented workers then buy stolen Social Security numbers, which are used to find employment. The brokers, known as "flippers," then provide free down payments to the buyers, who use the Social Security numbers to qualify for mortgages. A lender then gives the buyer a loan based on an inflated appraisal of the home provided by an appraiser involved in the scheme. Eventually, the home buyer forecloses on the property and taxpayers are forced to cover the losses -- all 87 homes purchased in Utah were federally insured through the U.S. Department of Housing and Urban Development.

Category 1C2 *Identity theft*

2004-05-19 **identity theft home security systems stealing customer data**

http://www.reuters.com/newsArticle.jhtml?type=oddlyEnoughNews&storyID=5193373

May 19, Reuters — Security provider jailed for identity theft.

A Connecticut man who installed home security systems has been sentenced to prison for using a client's personal information to finance a more than $200,000 spending spree, federal prosecutors said. Kenneth Moore, who owned Security Plus Associates in North Haven, CT, was sentenced to 43 months in federal prison and three years probation on Monday, May 17. U.S. District Judge Stefan Underhill also ordered Moore to repay $209,669.25. Moore used a client's name and social security number to secure financing for a $41,420 fishing boat and a $30,211 Mercedes Benz. He also opened credit card accounts with US Bank, First National Bank of Omaha, Shell Oil, Lowe's and Macy's. All of the cards were in the victim's name, but Moore provided his own address so the bills went to him, not the victim. Moore pleaded guilty to identity theft in February.

Category 1C2 *Identity theft*

2004-07-15 **identity theft legislation law George W. Bush President US prison criminals Internet cybercrime**

NewsScan

BUSH SIGNS IDENTITY THEFT BILL

President Bush has signed into law an identity theft bill that will add two years to the prison sentences of criminals convicted of using stolen credit card numbers or other personal data to commit crimes. On top of that, the sentences of identity-theft violators who then commit acts of terrorism will be extended by an additional five years. The Federal Trade Commission estimates that 27.3 million Americans have been victims of identity theft in the last five years. (Washington Post 15 Jul 2004)

Category 1C2 *Identity theft*

2004-07-16 **personal private information theft device Australia ATM PIN**

NewsScan

SMARTER SKIMMING DEVICE FOUND

A device designed to steal the personal details of ATM users was found in Sydney, Australia, by a customer who spotted the device and pulled it from the ATM. It had been in operation for three days, and may have recorded the confidential details of up to 1000 customers. The device, disguised to look like part of the ATM, uses a pin-hole camera to record the personal identification numbers of customers and a high-tech magnetic strip reader to steal the details on the card. Thieves can then use a decoder to burn the information onto any magnetic strip -- even a bus or train ticket -- and access users' bank balances. Police have found other machines used to rip off ATM users but the latest is by far the most hi-tech and devious. (The Australian, 16 Jul 2004) Rec'd from John Lamp

---

Category 1C2 *Identity theft*

2004-08-26 **identity theft I&A global crackdown US Department Justice John Ashcroft Federal Trade Commission FTC**

NewsScan

GLOBAL CRACKDOWN ON IDENTITY THEFT

More than 100 people have been arrested and 53 convicted in a global ID theft crackdown dubbed "Operation Web Snare" coordinated by the U.S. Justice Department. The operation involved some 150,000 victims who lost more than $215 million, according to Attorney General John Ashcroft -- a number he acknowledged represents only a small fraction of the crimes being committed on the Internet. Identity theft costs U.S. businesses more than $50 billion a year. "The Internet is stimulating the development of innovative products and services that were barely imaginable only a few years ago," says Deborah Majoras, chairwoman of the FTC which also took
part in the operation. "There is a risk, however, that these benefits will not be fully realized if consumers associate the Internet with fraudulent operators." (Reuters/CNet 26 Aug 2004)

Category 1C2 *Identity theft*

2004-10-27 **ID identity theft Florida Chey Cobb Stephen Cobb public records Web disclosure access**

NewsScan;

SAFE & SOUND IN THE CYBER AGE: FLORIDA'S ID THEFT KIT
(by Chey Cobb & Stephen Cobb)

A few years ago, when the dot com bubble was still bubbling, legislators in the State of Florida got the 'technology bug' and mandated that all Florida counties put all public records on 'The Web.' We have no idea if the companies that make the hardware and software used to implement the mandate handed out campaign contributions to encourage this technology leap. But a lot of money has been spent on such technology in the years since, from dozens of high speed scanners to terabytes of storage and thousands of lines of Web code. The result? A large group of people, and even the country as a whole, is probably a lot less safe than it used to be. To understand why, take a look at a Web page we have put up to demonstrate: <http://www.privacyforbusiness.com/example1.htm> The link on the right shows you a prime example of what can happen when people don't fully grasp the relationship between privacy, technology, and human nature. Anyone on the planet with an Internet connection can now find intensely personal details about individuals who have lived in, or passed through, Florida. One such class of persons is elderly folk whose relatives have filed power of attorney (these records sometimes include banking data along with SSN and signature). Another worrying class of victims is U.S. military personnel. You can find out what their specialties are, their Social Security Numbers, addresses, relatives, signature, and so forth. The example we give is one of these, from Duval County, the most populous county in Florida. What you will see is the record as it appears on the Web, except that we added red ink to blot out key portions of the name of this particular person. If you go to the Duval County Web site, from any country in the world, you can find thousands of records just like this, with the name and SSN in place, NOT crossed out. Many of these people are not Florida residents, they just happen to have left the service while in Florida. The legislators who mandated this state of affairs were not alone in their failure to realize that "The Web" is the same "World Wide Web" you can access from anywhere, from Boca Raton to Bulgaria, Tampa Bay to Turkistan. A number of federal government agencies took the same leap off the cliff of commonsense in their eagerness to save money by automating public access to information. The basic mistake was to think of the Internet as the American public. Perhaps their Internet bubble was a Venn diagram in which the set of all U.S. citizens neatly coincided with the set of all Internet users. In the very early days of the Internet that might have been forgivable, but these days, when the evening news routinely pulls its footage from Islamic fundamentalist Web sites, you would think we'd all be a bit wiser. Apparently not. Consider how you get to these records, many of which are the perfect starting point for the crime of identity theft. You would think that you would need to know a specific person's name to find public records pertaining to them. But no, in Duval County you can simply ask to see all records of a particular type within a valid date range. In other counties you can't browse all records at once, but a very lame search mechanism lets you enter a single letter for a last name, like "A," and thus browse all persons whose name begins with "A," from Aarnem to Aziz. At some sites, including Duval, you don't even need a document viewer like Acrobat because the county provides one for you. Needless to say, we think this type of access to people's private information is wrong. Our government does not have the right to publish to the world our Social Security Numbers, signatures, and other personal details (and this doesn't even get into the whole issue of Florida juvenile records wrongly placed in the public domain). Things need to be changed. If anyone would like to contact us about efforts to effect changes we will try to do what we can to help. What sort of changes are needed? Well, expunging all Social Security Numbers would be a start, but even easier would be the requirement that you need to know the name of the person whose public records you are seeking. And personally, we see no reason for military discharge papers to be made available at the county level. Why not make that a responsibility of the branch of the armed services in which the person served? In the broader scheme of things Americans need to do some serious thinking about what 'public record' means. Stephen is sitting in a bar in Amsterdam right now, looking at military service records of people from Alabama to Wyoming. He's also viewing aerial photographs of properties in our Florida neighborhood, then pulling up the names and addresses of the owners, seeing what they paid for their homes and if their taxes are current. Does he have a right to do that? From there? And what about the fundamentalist who might be sitting next to him in that bar? [Chey Cobb, CISSP, the author of "Cryptography for Dummies" and "Network Security for Dummies," is a former senior technical security advisor to the NRO. Her email is chey at aug dot com. Stephen Cobb, CISSP, is the author of "Privacy for Business" and Chief Security Executive of STSN. His email is scobb at cobb dot com.]

Category 1C2 *Identity theft*

2004-10-28 **ID identity theft operation firewall international police Web identity forgery documents counterfeit data theft**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A7614-2004Oct28.html

IDENTITY THEFT SUSPECTS CAUGHT IN STING OPERATION

"Operation Firewall" -- an international law enforcement dragnet conducted by the U.S. Secret Service, the Justice and Homeland Security departments, the Royal Canadian Mounted Police, Europol and local police departments -- has led to the arrest of 28 individuals on suspicion of operating Web sites created to steal, sell and forge credit cards and ID documents. The sites operated under names such as Shadowcrew, Carderplanet and Darkprofits, and were hosted on multiple Internet servers outside the United States. The suspects are thought to have bought or sold about 1.7 million stolen information and counterfeit documents such as credit cards, driver's licenses, birth certificates and foreign and domestic passports. A MasterCard security executive familiar with the operations says, "We're talking about an international network that has new sites popping up all the time. These aren't high-tech individuals. All it takes is a computer, a little bit of knowledge, and these guys can do a lot of damage." (Washington Post 28 Oct 2004)

Category 1C2 *Identity theft*

2004-11-22 **ACLU passport ID identity theft microchips privacy**

NewsScan; http://www.usatoday.com/tech/news/2004-11-22-hitech-passport_x.htm

ACLU ATTACKS MICROCHIP PASSPORT PLANS

The American Civil Liberties Union and some other privacy advocate groups are charging that international standards for "electronic" passports disregard a basic privacy approach protecting the security of the documents. New passports will have a chip containing the holders' name, birth date and issuing office, along with a "biometric" identifier that includes a photo of the holders' face. Barry Steinhardt of the ACLU says, "There's no security built into it. This will enable identity theft and put Americans at some risk when they travel internationally." A spokesman for the International Civil Aviation Organization and the State Department says those organizations are working on security concerns: "This is a process that is being implemented over the next few years, it is not something that happens overnight." The spokesman says that one way to fight identity theft is already in the standards, since the passports will have built-in encrypted authentication to let electronic readers know they are original documents and not forgeries. (AP/USA TODAY 22 Nov 2004)

Category 1C2 *Identity theft*

2005-01-12 **ID identity theft sentencing crime Teledata prison**

NewsScan; http://www.latimes.com/technology/la-fi-idtheft12jan12

IDENTITY THIEF DRAWS 14-YEAR PRISON TERM

A former help-desk worker at Teledata Communications, which provides banks with access to credit information, was sentenced to 14 years in prison for his role in the largest identity theft in U.S. history. U.S. District Court Judge George B. Daniels called the damage to victims caused by Philip A. Cummings "almost unimaginable," involving tens of thousands of individuals and caused losses of between $50 million and $100 million. Daniels noted the case "emphasized how easy it is to wreak havoc on people's financial and personal lives." (AP/Los Angeles Times 12 Jan 2005)

Category 1C2 *Identity theft*

2005-01-27 **ID identity theft wallet checkbook study offline study**

NewsScan; http://apnews.excite.com/article/20050127/D87SE8NO0.html

MOST IDENTITY THEFT OCCURS OFFLINE

Despite growing concerns over online fraud, a new study conducted by the Better Business Bureau and Javelin Research finds that most cases of identity theft can be traced to a lost or stolen wallet or checkbook, rather than vulnerable online financial data. Computer crimes make up just 12% of all ID fraud cases in which the origin is known, and half of those are attributed to spyware that sneaks onto computers and steals private information. (AP 27 Jan 2005)

Category 1C2 *Identity theft*

2005-02-13 **personal data leakage control confidentiality identity theft**

RISKS; http://www.washingtonpost.com/ac2/wp-dyn/A17506-2005Feb11 23 73

BREAK-IN AT SAIC RISKS ID THEFT

Monty Solomon contrtibuted a report from the _Washington Post_:

Some of the nation's most influential former military and intelligence officials have been informed in recent days that they are at risk of identity theft after a break-in at a major government contractor netted computers containing the Social Security numbers and other personal information about tens of thousands of past and present company employees.

The contractor, employee-owned Science Applications International Corp. of San Diego, handles sensitive government contracts, including many in information security. It has a reputation for hiring Washington's most powerful figures when they leave the government, and its payroll has been studded with former secretaries of defense, CIA directors and White House counterterrorism advisers.

Those former officials -- along with the rest of a 45,000-person workforce in which a significant percentage of employees hold government security clearances -- were informed last week that their private information may have been breached and they need to take steps to protect themselves from fraud.

David Kay, who was chief weapons inspector in Iraq after nearly a decade as an executive at SAIC, said he has devoted more than a dozen hours to shutting down accounts and safeguarding his finances. He said the successful theft of personal data, by thieves who smashed windows to gain access, does not speak well of a company that is devoted to keeping the government's secrets secure.…

Category 1C2 *Identity theft*

2005-02-17 **ChoicePoint ID identity theft data loss crime**

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/10921081.htm

DATABASE COMPANY WARNS OF ID THEFT CONCERNS

ChoicePoint, a Georgia company in the business of selling personal data on consumers, is alerting 145,000 people throughout the nation that a crime ring paid for their credit reports, Social Security numbers and other information. Con artists had posed as owners of debt-collection agencies, insurance agencies and other firms that told ChoicePoint they needed to run background checks on consumers. (San Jose Mercury News 17 Feb 2005)

Category 1C2 *Identity theft*

2005-02-22 **ChoicePoint theft consumers ID identity theft**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A45534-2005Feb22.html

PROTECTING YOURSELF AGAINST IDENTIFY THEFT

Consumers worried that their personal and financial data may have been captured by the criminals who scammed the ChoicePoint company are being assured by the Private Rights Clearinghouse: "If you don't receive a letter from ChoicePoint within the next 10 days, you can be assured you have not been a victim of this identity theft." Even so, you should always check your monthly bank and credit card statements to make sure all charges are valid, and you should review your credit reports at least once a year. If you do get a letter from ChoicePoint, follow its instructions, visit the FTC Web site, and obtain the affidavit credit bureaus require to place a long-term fraud alert on your account. And keep reviewing your credit history! (Washington Post 22 Feb 2005)

Category 1C2 *Identity theft*

2005-04-27 **software programs security data breach blame concerns identity theft fraud**

EDUPAGE; http://online.wsj.com/article/0,,SB111455367943717582,00.html

CONCERNS MOUNT OVER SOFTWARE'S ROLE IN DATA BREACHES

A number of retailers are pointing to software used at store checkouts as the weak link in the rash of recent security breaches. Magnetic strips on credit cards include--along with the credit card number--a three-digit code. Knowing that code can allow criminals to create counterfeit cards with embossed names that do not match the name attached to the account number. With that, a crook could present a photo ID that matched the name on a card, while the charge goes against an entirely different account. Software that handles credit card purchases is supposed to delete card numbers and the three-digit codes after a transaction, but several retailers now say that the systems keep those numbers in memory. John Shaughnessy of Visa USA said that a computer system that retained those numbers would be extremely tempting for criminals. Some retailers have filed suits against the makers of the software, seeking compensation for losses resulting from recent hacks. At least one software company, Micros Systems, rejected retailers' contentions, saying its products do not store such information. Wall Street Journal, 27 April 2005 (sub. req'd)

Category 1C2 *Identity theft*

2005-05-11 **social engineering fake bank machines identity theft fraud**

RISKS; http://tinyurl.com/cwhpd 23 89

FAKE ATMs IN ROMANIA USED FOR IDENTITY THEFT

Audacious thieves in Romania have constructed a complete automated teller machine (ATM), minus the cash box, to steal the details of account holders. Fake ATMs have appeared at apartment buildings or in areas of the capital where there are no banks. Usually criminals only place a fake panel over an existing ATM, and do not construct a complete machine. Romania's biggest bank, Banca Comerciala Romana (BCR), said customers should only use ATMs situated around bank branches. "Banks do not install ATMs in blocks of flats," BCR spokesman Cornel Cojocaru said.

[Abstract in RISKS by James Bauman]

Category 1C2 *Identity theft*

2005-05-18 **student report research John Hopkins University personal information harvesting**

EDUPAGE; http://www.nytimes.com/2005/05/18/technology/18data.html

STUDENTS SHOW EASE OF IDENTITY THEFT

Graduate students at Johns Hopkins University set out to see how much personal information they could collect on as many individuals as possible, using only the Internet and $50. The 41 students were in a course taught by Aviel D. Rubin, professor of computer science and technical director of the university's Information Security Institute, who divided them into groups of three or four and instructed them to use only legal, public sources of information. The exercise mimicked the activities of data brokers, such as ChoicePoint and LexisNexis, and the students were able to collect and aggregate vast amounts of information, even with limited time and budgets. Although Rubin was pleased that fewer Social Security numbers were among the data collected than he had anticipated, privacy advocates insisted that such information remains easy to obtain, posing enormous risk of identity theft. Even without Social Security numbers, the data collected represented for some individuals a very broad picture of who they are, where they live, and activities in which they participate. Such access to personal information worries many, including Sen. Ted Stevens (R-Alaska), who conducted a similar experiment, instructing his staff to try to steal his identity. Aside from information they discovered about Stevens, they were told they could buy his Social Security number for $65. New York Times, 18 May 2005 (registration req'd)

Category 1C2 *Identity theft*

2005-05-20 **identity ID theft personal information disclosure LexisNexis FBI US Secret Service**

EDUPAGE; http://online.wsj.com/article/0,,SB111653162281238311,00.html

FEDS CONDUCT SEARCHES RELATED TO DATA THEFTS

Federal authorities investigating the theft of personal information from LexisNexis this week conducted raids and searches at several locations around the country. LexisNexis, which collects and aggregates information on millions of people, recently reported that information on nearly 300,000 individuals had been stolen by hackers. Investigators from the Federal Bureau of Investigation and the Secret Service searched the homes and computers of close to one dozen people, resulting in at least three arrests. Spokespersons for the agencies conducting the raids as well as for LexisNexis declined to give many details other than that the investigations are ongoing. Wall Street Journal, 20 May 2005 (sub. req'd)

Category 1C2 Identity theft

2005-05-29 **identity ID theft education program Department of Education DVD thief interview**

EDUPAGE; http://www.nytimes.com/2005/05/30/national/30fraud.html

COLLEGES LEARN ABOUT IDENTITY THEFT FROM AN IDENTITY THIEF

As part of its efforts to increase awareness about student loan fraud, the Department of Education is distributing a DVD to colleges and universities of an interview with a convicted identity thief. As part of his plea agreement, John E. Christensen was interviewed by authorities to create the DVD, in which he describes how, over a period of three and a half years, he used the identities of more than 50 individuals to defraud the government of more than $300,000 in federal student grants and loans. Each year, the Department of Education disburses about $65 billion in financial aid. In the interview, Christensen, who is serving his prison sentence in Arizona, explains how he fraudulently obtained personal information and used it to register for classes and apply for financial aid. Because financial aid processes take place largely online, defrauding the government is "becoming easier and easier all the time," said Christensen. "You never have to see anybody." New York Times, 29 May 2005 (registration req'd)

Category 1C2 Identity theft

2005-06-13 **identity ID theft Liberty Alliance Protection Group fraud**

EDUPAGE; http://news.com.com/2100-7348_3-5744641.html

LIBERTY ALLIANCE ADDRESSES ID THEFT

The Liberty Alliance has announced the formation of an Identity Theft Protection Group, intended to address the problem of identity theft. The alliance was created in 2001 to establish standards for online authentication and now has a membership of more than 150 companies, nonprofits, and government organizations. Michael Barrett, co-chairman of the new group and a security executive at American Express, said he believes the problem of identity theft will continue to worsen such that "it is no longer a question if your identity gets stolen, but when." The new group will initially work to clearly define the problem and its parameters and later will try to develop solutions, which, according to Barrett, might include technical specifications, best practices, or business guidelines. James Van Dyke of Javelin Strategy and Research, which covers identity fraud, noted that despite perceptions otherwise, the incidence of identity theft has been decreasing over the past few years. CNET, 13 June 2005

Category 1C2 Identity theft

2005-08-12 **identity ID theft personal information disclosure notification law New York**

EDUPAGE;
http://www.theregister.com/2005/08/12/ny_security_breaches_disclosure/

NEW YORK ADDS DISCLOSURE LAW

New York State has enacted a law requiring corporate or public organizations to notify individuals in the event that personal information about them has been compromised. Similar in concept to a California law that went into effect two years ago, the New York law compels organizations that store sensitive information to contact consumers as quickly as is practical if there is evidence or suspicion that data including Social Security numbers or credit card numbers have been unlawfully accessed. At least 15 other states have passed similar legislation since California did. New York State Assembly member James Brennan, sponsor of the legislation, said, "If a person is not aware that he or she has been a victim of identity theft, then the damage done could be severe and irreversible," noting that the sooner people are made aware of security breaches involving sensitive data, the better their chances are of avoiding the worst repercussions. The Register, 12 August 2005

Category 1C2 Identity theft

2005-08-26 **cyber scam fraud identity ID theft security firms FBI Sunbelt Software keylogging virus dissemination**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4186972.stm

CYBERSCAM CONTINUES APACE

A recently discovered identity-theft scam continues to cause problems for Internet users, despite efforts by security firms and the FBI to stop it. Security firm Sunbelt Software uncovered the scam accidentally while investigating spyware. Sunbelt located an Internet server whose log files contained personal information harvested by keylogging from many thousands of users. The company notified the FBI, and the server was shut down soon afterwards, only to resurface later. Each time the servers are taken down, more of them appear elsewhere. The keylogging software, which is circulated by a computer virus, captures private information from users and transmits it to one of the rogue servers.
The FBI is working to find out who is operating the servers. In the meantime, Sunbelt has developed a tool that searches for the malicious software, which is has named Srv.SSA-KeyLogger. BBC, 26 August 2005

Category 1C2 *Identity theft*

2005-09-24 **computer breach lawsuit no disclosure identity theft ID credit card companies**

EDUPAGE; http://www.theregister.com/2005/09/24/data_id_theft_secret/

CALIFORNIA JUDGE RULES AGAINST DISCLOSURE

A California judge has ruled against plaintiffs who had accused CardSystems Solutions, Visa, and MasterCard of failing to notify them as required by state law following a computer breach that exposed the personal information of 40 million individuals. The breach happened in June, and, according to CardSystems Solutions, records on approximately 200,000 individuals were taken from the network. California law requires notification in most such cases, and a law firm in the state had brought a class action suit against the companies, which had refused to pursue notifications. The suit sought to compel the companies to notify all affected consumers and to cover any fees or other expenses incurred as a result of ID theft stemming from the incident. Judge Richard Kramer found for the defendants, however, saying he failed to see the emergency. "I don't think there is an immediate threat of irreparable injury" to consumers, he said. The Register, 24 September 2005

Category 1C2 *Identity theft*

2005-11-17 **identity theft Secret Service sting Operation Firewall fraud guilty plea**

EDUPAGE; http://www.wired.com/news/infostructure/0,1377,69616,00.html

FEDS WIN GUILTY PLEAS IN ID THEFT RACKET

Six individuals caught in a Secret Service sting called Operation Firewall pleaded guilty to conspiracy to commit credit and bank card fraud and ID document fraud. Two other individuals involved in the scam previously pleaded guilty to the same charge. All were among 19 who were indicted last year, charged with running a private-access Web site where people from around the globe bought and sold sensitive information, such as Social Security numbers, credit card numbers, and fake IDs. The ID theft ring is thought to have trafficked in more than 1.5 million credit card numbers, close to 18 million e-mail accounts, and other information that was used to buy and sell merchandise online. One who pleaded guilty, Wesley Lanning, specialized in making and selling fake IDs. His attorney, Marc Leibman, said that although Lanning sold most of the IDs to teens to use to buy beer, "obviously everyone is concerned that some…militant is going to get one of Wesley Lanning's fake IDs and use it to transport a bomb." Wired News, 17 November 2005

Category 1C2 *Identity theft*

2005-12-07 **study identity theft risk exaggerated ID Analytics fraud detection**

EDUPAGE; http://money.cnn.com/2005/12/07/technology/id_study.reut/

STUDY SAYS RISK OF ID THEFT EXAGGERATED

A new study conducted by California-based fraud detection company ID Analytics found that the risk of identity theft may not be as high as many believe it to be. The company analyzed data concerning four incidents in which sensitive information for roughly 500,000 people was compromised. ID Analytics followed the data for six months and found that the risk of having your identity stolen based on compromised information is relatively small. Further, the study showed that the greater the number of people affected in a breach, the lower the chances were that anyone would have their identity stolen. The company went on to say that efforts to notify every individual affected when sensitive information is illegally accessed might be doing more harm than good. Rather than notify everyone, according to ID Analytics, a company should spend its time and money helping consumers who are actually affected by a data breach. CNN, 7 December 2005

1C3 Pseudonymity

Category *1C3* *Pseudonymity*

1999-02-08 **privacy software Web Internet pseudonyms concealment**

LA Times

FREEDOM SOFTWARE TARGETS PERSONAL SECURITY
Zero Knowledge Systems has unveiled its Freedom software product, designed to provide a measure of personal privacy on the Internet by encrypting messages and provide up to five pseudonyms that can be used in electronic commerce, chat rooms or sensitive-topic discussion groups. The software also includes a spam filter and cookie protector. Analysts say the software could make electronic shopping a more attractive proposition, because buyers wouldn't have to divulge their personal information (other than their credit card numbers). "When users don't see themselves as having privacy, they'll just lie and give totally false (demographic and personal) data, so a lot of the data that marketers get today is useless," says Zero Knowledge chief scientist Ian Goldberg. Freedom software is expected to hit the shelves next month. (Los Angeles Times 8 Feb 99)

Category *1C3* *Pseudonymity*

2001-07-20 **pseudonymity risks marriage love affairs strangers husband wife fracas embarrassment rage**

RISKS 21 55

An unexpected risk of Internet pseudonymity was reported to RISKS by Gary Stock:

A married couple in China ended up brawling after realising they had unwittingly courted each other over the internet. The pair from Beijing sneaked online to flirt with their mystery girlfriend and boyfriend at a chat website called the Green, Green Schoolyard. After a month, the man arranged to meet up with his ideal new friend only to discover it was actually his wife. He had known only her user name, I Want You. They each agreed to carry a certain newspaper to identify themselves, but were shocked when they came face-to-face and started fighting in the street. Passers-by eventually alerted security guards who had to separate the two, reports Norway's main news agency NTB.

http://www.ananova.com/news/story/sm_354103.html ?menu=news.weirdworld.rockyrelationships

[MK adds: ironically, the two seemed to be ideally mated already -- each person's exciting new dream date was already their own spouse.]

Category *1C3* *Pseudonymity*

2004-09-02 **call blocking service privacy Star38 phone number masquerading spoofing caller ID**

NewsScan

SPY VERSUS SPY: UNBLOCK THAT CALL-BLOCK

A new computerized service from a company called Star38 will allow callers to create false outbound phone numbers and thereby fool call block software. Customers of the new service will be able to go to the company's Web site to enter the number they want to call and the number they want to appear on the caller ID screen of the recipient's phone. Some privacy-rights advocates are concerned that angry former spouses, stalkers or fraud artists could use the service for mischief, but Robert Atkinson of the Institute for Tele-Information at Columbia University, comments: "Some people see caller ID as an invasion of their privacy, while others see it as a protection of their privacy. It's spy versus spy." (New York Times 2 Sep 2004)

1C4 Anonymity

Category 1C4 *Anonymity*

1998-04-14 **privacy Web information survey**

EDUPAGE

EDUPAGE reported, "Vanderbilt University researchers Donna Hoffman, Tom Novak, and Marcos Peralta <http://www2000.ogsm.vanderbilt.edu/> say that 94% of Web users surveyed have refused to provide information to a Web site, and 40% have given fake information. (New York Times 13 Apr 98)"

Category 1C4 *Anonymity*

1999-04-15 **anonymity anonymizer vulnerability hacks weaknesses quality assurance**

New York Times

Richard M. Smith, President of Phar Lap Software of Cambridge, MA reported on weaknesses in anonymizer products promising users protection against disclosure of their identity. Peter Lewis wrote in the _New York Times_, "Anonymizer.com (www.anonymizer.com), the Naval Research Laboratory's Onion Router (www.onion-router.net), the Lucent Personalized Web Assistant service (www.bell-labs.com/project/lpwa) and . . . Aixs.Net (aixs.net) were scrambling this week to patch the security holes."

Category 1C4 *Anonymity*

1999-08-16 **privacy anonymity Web cloaking encryption cookies concealment law enforcement warrants**

New York Times

NEW WAY TO TRAVEL THE WEB WHILE LEAVING FEW FOOTPRINTS
Privacy software maker Privada today is expected to unveil its Web Incognito service, a $5-a-month, all-encompassing online anonymity protector. The service protects online users' privacy by encrypting outgoing information and directing it to the Privada service, where the data is cloaked before being sent to its destination. The service covers e-mail, online chat, Web browsing, and online purchases. Responses from Web sites or e-mail recipients go back through the Privada service before being sent to the user. The service does not hinder users' ability to surf the Web, as users' cookies are stored by the service. Privada CEO Barbara A. Bellissimo says the company may draw the ire of privacy rights groups because the company plans to share the identities of users with law enforcement officers who have valid warrants. "Our service is for protecting the privacy of consumers, not for hiding criminals or criminal activities," Bellissimo says. (New York Times 08/16/99)

Category 1C4 *Anonymity*

2002-11-22 **anonymity Internet surveillance law trace technology identifier research intelligence information**

NewsScan

PENTAGON CONSIDERED PLAN TO END ANONYMOUS NET ACTIVITY
After the head of DARPA, the Defense Advanced Research Projects Agency, wondered why it was not possible after the 9-11 terrorist attacks to trace hostile Internet communications back to the origin, a series of technical discussions were initiated, and those discussions led to a proposal called eDNA: "We envisage that all network and client resources will maintain traces of user eDNA so that the user can be uniquely identified as having visited a Web site, having started a process or having sent a packet. This way, the resources and those who use them form a virtual 'crime scene' that contains evidence about the identity of the users, much the same way as a real crime scene contains DNA traces of people." But the project was argued against by a number of angry participants, such as security consultant Mark Seiden who said: "Before people demand more surveillance information, they should be able to process the information they already have. Almost all of our failures to date have come from our inability to use existing intelligence information." DARPA has decided to discontinue funding of the project, and explained that it had been "intrigued by the difficult computing science research involved in creating network capabilities that would provide the same levels of responsibility and accountability in cyberspace as now exist in the physical world." (New York Times 22 Nov 2002)
http://www.nytimes.com/2002/11/22/politics/22TRAC.html

Category 1C4 *Anonymity*

2005-10-06 **blogger Delaware lawsuit shield identity First Amendment free speech anonymity cyberspace**

EDUPAGE; http://www.nytimes.com/2005/10/06/technology/06blog.html

DELAWARE COURT SHIELDS IDENTITY OF BLOGGER

The Delaware Supreme Court has rejected an effort to identify an anonymous blogger accused of defamatory remarks online. Patrick Cahill, a councilman in the city of Smyrna, had sought the blogger's identity from Comcast following several unflattering postings on the person's blog. Although a lower court judge had denied the blogger's request for protection, the Supreme Court said that court had applied the wrong standard. In the absence of substantial evidence of defamation, Cahill's petition to identify the blogger will be denied, according to the high court. In the ruling, the court said it found for the blogger to protect against what it called "the chilling effect on anonymous First Amendment Internet speech that can arise when plaintiffs bring trivial defamation lawsuits primarily to harass or unmask their critics." An attorney for the blogger said that statements on electronic bulletin boards and blogs are not generally considered factual but are seen as individuals' opinions. The court's judgment, however, did not identify the medium as pertinent in its application of legal standard. New York Times, 6 October 2005 (registration req'd)

Category 1C4 *Anonymity*

2005-12-11 **anonymity defamation libel risk threat Wikipedia free online encyclopedia**

RISKS 24 12

ANONYMITY AND BAD WIKIPEDIA CONTENT
John Seigenthaler Sr. (a former editor of *The Tennessean* in Nashville, and founder of the First Amendment Center) was startled to find an entry on himself in Wikipedia that included defamatory false personal information about him -- for example, suggesting that Mr. Seigenthaler had been involved in the assassinations of John and Robert Kennedy. Mr. Seigenthaler then wrote an op-ed article in *USA Today*, noting among other things that he was especially annoyed that he could not track down the perpetrator because of Internet privacy laws.

The culprit's IP address led to his employer by Daniel Brandt of San Antonio -- who has been a frequent critic of Wikipedia after reading false information about himself! See his www.wikipedia-watch.org.

This led Brian Chase in Nashville to admit having written the offensive material as a joke, stating that he thought that Wikipedia was a "gag" Web site.

[Abstract by Peter G. Neumann]

Dr Neumann adds:

Coincidentally, that story broke on about the same day that the December 2005 issue of the *Communications of the ACM* came out, the inside back cover Inside Risks column of which is "Wikipedia Risks" http://www.csl.sri.com/neumann/insiderisks05.html -- written by four long-time RISKS contributors, Peter Denning, Jim Horning, David Parnas, and Lauren Weinstein who are on my ACM Committee on Computers and Public Policy. This case points up just one of the risks associated with Wikipedia noted in the Inside Risks article, namely that of having an encyclopedia contributed by thousands of volunteers, with few controls on content.

RISKS contributor Ian Halliday follows up (RISKS-24.13) by saying he does not buy Brian Chase's argument:

The claim that "he thought Wikipedia was a gag site" (RISKS-24.12) seems unlikely, and I see it on a par with those who say "no, I was just doing research" when caught hacking/visiting dubious web sites. Yet this seems to have caught the attention of some parts of the media who don't usually see visiting those sites as plausible research. The suggestion is that it is reasonable for somebody to be so mistaken as to think Wikipedia is a "gag" site. While some of the information there may not be 100% accurate, it's hard to see how this apparently mistaken view can be seen as a genuine defence.

[Summary by Karthik Raman]

Category 1C4 *Anonymity*

2005-12-11 **GAO government accountability office bad WHOIS database anonymity spamming scamming phishing privacy**

RISKS; http://www.internetnews.com/ent-news/article.php/3569521 24 12

WHOIS DATABASE RISKS

A U.S. Government Accountability Office (GAO) report in Nov 2005 says that there are roughly 2,310,000 Web addresses for which the owner or contact information is unknown. That represents 5% of all .com, .net, and .org domain names. This provides anonymity for spammers, scammers, phishers, and other illegal activities, and untraceability for malware-containing sites.

[Abstract by Peter G. Neumann]

Dag-Erling Smørgrav rebuts (RISKS-24.13):

It also provides relative anonymity for people like paralegal Pamela Jones, who operates groklaw.net, an award-winning web site dedicated to reporting on and analyzing "legal events important to the [Free and Open Source Software] community". Her relentless digging into the SCO lawsuits has made her the target of harassment and defamation by SCO and its supporters, such as journalist Maureen O'Gara -- ask Google for the sordid details.

Also in RISKS-24.13, Dave Bell remarks:

I just hope that the GAO knows the difference between "unknown" and "withheld". My domain name is registered in the UK, and because of UK and European data protection laws applying to personal data, the WHOIS doesn't return certain information.

[Summary by Karthik Raman]

1C5 Phishing

Category 1C5 Phishing

2000-07-25 **impersonation Web site confidentiality password stealer Trojan horse phishing**

RISKS, MSNBC http://www.msnbc.com/news/435937.asp 20 97

Avi Rubin contributed the following summary to RISKS: "Somebody in the Ukraine registered PayPaI.com (note the resemblance to PayPal, especially with the upper-case I [in some fonts]), then copied Paypal's HTML and sent mail to a bunch of Paypal users saying 'J. Random has just transferred $827 to you using PayPal, log in at http://www.paypaI.com/ to claim it!' of course, as soon as you `logged in' your password was mailed to some free e-mail service."

Category 1C5 Phishing

2002-12-11 **Web hijacking imposter counterfeit spoofing fraud theft consumer**

NewsScan

IMPOSTOR EBAY SITE SET UP TO STEAL CREDIT INFO
A Web site called ebayupdates.com, having no relation to the eBay auction site, was created as part of a scam to obtain credit information fraudulently from eBay customers. The scam was discovered by the private Internet watchdog group SANS Institute Internet Storm Center, and was confirmed by an eBay executive who said: "Some members have reported attempts to gain access to their personal information through e-mail solicitations that are falsely made to appear as having come from eBay. These solicitations will often contain links to Web pages that will request that you sign in and submit information. eBay employees will never ask you for your password." (Reuters/San Jose Mercury News 11 Dec 2002)

Category 1C5 Phishing

2002-12-23 **pop-up advertising Web hijacking HTML**

NewsScan

POP-UP ADS 'KICK THROUGH'
Pop-up ads are becoming increasingly annoying, and the latest twist will make it harder for Web users to simply ignore them. A new technique called "kick through" enables advertisers to direct a person to another Web site if they simply move their cursor across the ad — no clicking is necessary. Many people are complaining that the new ads are overstepping the boundaries of an already intrusive form of online advertising. "When I tried to close the window it kicked me to the site, which is really annoying when I have six windows open and three of which were not by my own doing," says one irate victim. Orbitz, which appears to be the only advertiser currently using the kick through, defends its strategy: "The enormous success for Orbitz is directly related to these pop-unders. There's an enormous segment of the population that are appreciating these ads," says Mark Rattin, creative director for Otherwise, which devised the ads for Orbitz. He says there's only a 30% chance that viewers will be kicked through to the Orbitz site by rolling over the ads. (CNet News.com 20 Dec 2002)
http://news.com.com/2100-1023-978616.html

Category 1C5 Phishing

2003-02-27 **Canada Internet Service Provider ISP e-mail scam fraud**

NIPC/DHS

February 25, Reuters — Canada's Sympatico targeted in Internet scam.

Company officials at Sympatico, one of Canada's biggest Internet service providers (ISP), said Tuesday that organizers of a scam had sent out fraudulent e-mails to some 1,900 of Sympatico's 1.4 million customers last week. The e-mails told customers to fill out an online form to correct an error in their billing information and directed them to a fake site which asked for details, including driver's license, credit card and bank numbers and security codes. The fake site has since been shut down. "We did take immediate action to minimize the impact. E-mails that were going out to our customers were stopped and we contacted the ISP that was hosting this particular site," said Andrew Cole, a spokesman for Bell Canada. Cole said those who filled out the online forms should contact the police, their banks and credit card issuers. The company does not know who was behind the scam. "What we do know is the site was hosted in the United States. However, the e-mail itself was relayed through Japan...law enforcement and Bell security are certainly looking into the source," he said. He said the company did not think it was necessary to e-mail all of its customers, but that it had included several warnings about it on its sites. Sympatico.ca is owned by BCE Inc.'s Bell Canada unit, Canada's largest phone company.

Category 1C5 *Phishing*

2003-03-19 **pornography swindle extortion organized crime**

NewsScan

PORN SWINDLE
Federal prosecutors in Brooklyn, NY, have arrested three men for using pornography Web sites to obtain credit information from visitors and then charging them as much as $90 a month, which was funneled into the coffers of the Gambino crime family. The scam worked like this: visitors to a porn site were offered a "free tour" of explicit material on the site, and asked to provide credit information as proof they were "adults." (New York Times 19 Mar 2003)

Category 1C5 *Phishing*

2003-07-16 **virus Sophos antivirus ActiveX marketing trick**

NewsScan

'VIRAL MARKETING' STOOPS TO NEW LOW
Internet security company Sophos is warning of a new marketing scheme reported by its Australian tech support team, which tricks users into visiting a Web site featuring free comic video clips and then installs software that sends out e-mails from their computers to people listed in their address book. The Web site, run by Curacao-based Avenue Media, uses ActiveX to display a humorous video clip and at the same time downloads an additional software component called "Internet Optimizer" onto the PC, which then sends the e-mails. Peter Ducklin, head of technology at Sophos' Asia Pacific division, says: "What tricks a lot of people is that the ActiveX control which kicks the process off is digitally signed. Many users assume that a program which has been signed in this way is automatically both trustworthy and desirable. Ironically, even though Internet Explorer presents a 'security warning,' many people treat this as some kind of a 'security approval' and are more inclined to go ahead." (ZDNet Australia 16 Jul 2003)

Category 1C5 *Phishing*

2003-09-03 **Web pornography DNS domain name service spoofing mousetrapping diversion phishing**

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/6683165.htm

MAN ARRESTED FOR 'MOUSETRAPPING' CHILDREN
Federal agents have arrested a Florida man they say runs Web sites that exploit misspellings by computer users to redirect children looking for Disneyland or the Teletubbies to explicit porn sites instead. The government say it is the first prosecution under a provision of the new Amber Alert legislation that makes it a crime to use a misleading Web address to draw children to pornography. The man registered thousands of Internet addresses and was earning up to $1 million per year off them — much of it from sites that paid him when he sent Web users their way. The redirection technique is called "mousetrapping." U.S. Attorney James Comey said: "Few of us could imagine there was someone out there in cyberspace, essentially reaching out by hand to take children to the seediest corners of the Internet." (San Jose Mercury News 3 Sep 2003)

Category 1C5 *Phishing*

2003-11-13 **phishing scam bank account Canada URL**

RISKS 23 3

Bank scam with spaces in trick URL

Contributor Mark Brader discusses a fresh kind of phishing scam that exploits URL truncation by Internet browsers. The HTML code of the e-mail message purportedly coming from a Canadian bank had a URL that looked like: <a href="http://www.capcity.ab.ca :UserSession=00000000000000000000000000000000 &userrststе=SecurityUpdate&StateLevel=CameFrom@00000000000000.com">
Brader says that he replaced characters in the e-mail URL with 0's "to prevent anyone from following this link by accident." If someone clicked on the above link from their e-mail, their browser would truncate the row of spaces; they would be directed to the phisher site, yet believe they were at the real bank Website. Peter Neumann adds that this particular phisher site had been shut down.

Category 1C5 *Phishing*

2003-12-10 **PORN PURVEYOR GUILTY John Zuccarini deceptive domain names direct minors nudity adult content**

NewsScan

PORN PURVEYOR PLEADS GUILTY
John Zuccarini, of Hollywood, Florida, has pled guilty to 49 counts of using deceptive domain names to direct minors to nudity or other adult content, and to one count of child pornography possession. Prosecutors have recommended a three-year prison sentence with fines still to be determined. Zuccarini owned at least 3,000 domain names, most of which were misspelled versions of popular brands, such as www.dinseyland.com. (Wall Street Journal 10 Dec 2003)

Category 1C5 *Phishing*

2004-01-05 **phishing scam Bank of England e-mail fraud credit card money**

RISKS 23 12

VISA CUSTOMERS HIT BY PHISHING EXPEDITION SEEMINGLY FROM BANK OF ENGLAND

RISKS 23.11 included a scrambled summary of a phishing scam; the correction in 23.12 from Simon Hogg included the following clarification:

As I'm sure many of the RISKs readers are aware, the Bank of England is a Central Bank and hence does not issue its own Visa (or any other credit cards) at least for consumers. Similarly, it doesn't operate consumer bank accounts. I suppose you could say that the Bank of England is equivalent to the Federal Reserve, *not* Bank of America. Therefore the BoE is unlikely to be a 'victim' in the ordinary sense of the word.

Therefore, I thought there was something a bit fishy with the PGN version saying that the "This was reportedly the first time BoE was victimized by a "phishing" expedition that apparently fooled about 5% of their Visa customers into divulging their card and PIN numbers."

Looking at the original news story the 'phishing' quote apparently relates to a different episode, "A campaign that targeted Visa credit card holders was said to have fooled one in 20 victims into divulging their personal details, including their card and pin numbers" *i.e. not the BoE e-mail itself*.

The point of the story is to say that lots of people were sent an e-mail with an executable attachment with the message "Please install our special software, that will remove all the keyloggers and backdoors from your computer." The implication (for the sender the hopeful implication) was that since the e-mail was apparently from the BoE, the software was in some way 'official'. Imagine the same e-mail in the US from someone@federal-reserve.gov.

I think the problem here is wider than a standard someone@aConsumerBank.com e-mail since it is apparently from a 'trusted' central bank (the one who controls the 'normal' banks) but it doesn't cause any direct 'damage' to the apparent sending agency.

So, three apparent risks;

1. Mis- / Dis-information (scaremongering?), accidental or otherwise, caused by incorrect summary of other news stories.

2. E-Mails apparently from a trusted source (common / usual RISKs here, but the 'trusted source' in this case is a 'super-trusted source').

3. For me the most worrying RISK is that the UK's "National High-Tech Crime Unit" came out with the very enlightening statement "We have opened the attachment, but we have so far not been able to find out what it does, if anything." How many programmers does it need to be able to analyse a piece of code to be able to work out what it does? Anti-virus labs are pretty good at this, so why not the Government-funded anti-crime 'specialists'? At least they are apparently being honest here(!).

Category 1C5 *Phishing*

2004-01-05 **anti fraud phishing service UK Netcraft**

NewsScan

A PROACTIVE APPROACH TO 'NO PHISHING'

Netcraft, based in the U.K., has launched an anti-fraud service aimed at preventing "phishing" — the practice of luring unsuspecting users to counterfeit banking sites where they're encouraged to divulge their credit card or other financial information. The company keeps a database of about 20 million home pages as well as a record of all registered Web site names. It then scours its copies of the Net's DNS records for suspicious entries related to or using its customers' name and alerts the legitimate name holder when it finds something. "It gives you the opportunity to try to pre-empt attacks," says Netcraft director Mike Prettejohn, rather than relying on customers to alert banks to online scams. (New Scientist 5 Jan 2004)

Category 1C5 *Phishing*

2004-01-28 **spam e-mail address hacking cracking images CAPTCHA pornography Website redirection phishing**

RISKS 23 17

PORN VIEWERS WORK FOR HACKERS

Contributor Robin Burke summarizes an article about an online hack. Hackers are defeating the "CAPTCHAS" technique used to stop robots from registering for online services. Human beings can read what a CAPTCHA image asks for, and do its bidding, but robots can't because they're not intelligent enough. Now, hackers are "routing the CAPTCHA image to a page that advertises free porn." Viewers of these porn sites are given access to more free porn only after they decode a CAPTCHA image and complete a form to explain the image. Bots then use information from these porn-site forms to register for online services by seeming humanly intelligent.

Category 1C5 *Phishing*

2004-02-04 **phishing Internet Explorer fix patch URL**

RISKS 23 17

PHISHING AND A NEW IE SECURITY PATCH

Contributor Sidney Markowitz notes that Microsoft has issued a security update to address an Internet Explorer phishing vulnerability. IE used to suppress portions of a URL after an '@', which was exploited by phishers to craft authentic-looking URLs. With this new patch, IE will suppress by default all URLs of the form "username:password@hostname". However, this can be changed in the Windows registry as needed.

Category 1C5 *Phishing*

2004-03-16 **phishing scams corporate information risk steal business secrets**

NewsScan

PHISHING SCAMS 'LIKELY TO TARGET CORPORATE INFO SOON'

Phishing scams will continue to flourish but their focus will change: they will increasingly target corporate information, the Asia-Pacific vice-president of one of the world's premier security company says. Richard Turner of RSA Security said the current rash of phishing scams was just the proverbial tip of the iceberg and those who were perpetrating them would turn to the more lucrative field of stealing business secrets. "Australian businesses are rapidly opening their networks to remote users, be they employees who want to work from home, customers or those from other companies who share information. As soon as you do this, you need to apply good policy to information systems and business systems," said Turner, who has been with RSA for the last eight years. "Once this stage is reached, the need to implement well-configured software becomes paramount, in order to provide protection against unauthorised connections." (The Age, 16 March 2004)

Category 1C5 Phishing

2004-04-01 **computer tools counter scams anti-phishing anti-fraud**

DHS IAIP Daily;
http://story.news.yahoo.com/news?tmpl=story&cid=562&ncid=738
&e=2&u=/ap/20040401/ap_on_hi_te/online_scams

April 01, Associated Press — Companies sharpen tech tools to counter scams.

As Internet scams, also known as phishing, proliferate, companies are sharpening technological tools to counter them. Education alone, many agree, isn't enough. Anti-phishing software is apt to soon be added to the arsenal of digital shields forged to stop spam, viruses and hacking. Security companies are also building tools for banks and merchants to use behind the scenes. Phishing scams have been around for years but have in recent months become more numerous — and sophisticated. Scammers now copy and paste Web coding from real sites like Citibank's to give their fraudulent messages and the sites they lead to an aura of authenticity. They register Internet addresses that look real, subbing the letter "l" with the numeral "1," for instance. A few messages even carry ads for that aura of authenticity. The Anti-Phishing Working Group, formed in October by industry and law enforcement, identified 282 new phishing scams in February, up from 176 a month earlier. About 70 percent have been traced to eastern Europe or Asia, said David Jevans, the group's chairman.

Category 1C5 Phishing

2004-04-23 **fraud e-mail credit card banks FDIC personal information virus**

NewsScan

BANKS WARNED ABOUT FRAUDULENT E-MAILS

The Federal Deposit Insurance Corp. (FDIC) is warning banks that consumers are receiving fraudulent e-mail messages claiming that the FDIC has collaborated with credit card providers to provide a new service and that by following a link in the message the recipient can get a free trial membership for discount coupons at various online retail outlets. The FDIC says: "The e-mail was not sent by the FDIC and may be a fraudulent attempt to obtain personal information from consumers or to implant a computer virus onto the recipient's computer. Financial institutions and consumers should not access the link or attached files provided in the body of the e-mail and should not, under any circumstances, provide any personal information to unknown sources." (AP/San Jose Mercury News 23 Apr 2004)

Category 1C5 Phishing

2004-05-05 **banking phishing fraud organized crime**

DHS IAIP Daily; http://www.timesofmalta.com/core2/article.php?id=153129

May 05, Reuters — BIS warns of consumer banking scams using its name.

The Bank for International Settlements (BIS) on Tuesday, May 4, warned that its name and logo were being used in scams to defraud the public with offers of consumer banking services. The BIS is a central bank to the world's central banks. Its functions are purely official and it offers no services to private individuals or companies. "The BIS strongly cautions the public against sending money or disclosing bank or credit card details to any person who claims to represent the BIS or to have a banking relationship with the BIS," the bank said in a statement. The BIS named two "fraudulent websites" which are currently misusing its name, www.bfisonline.net and www.bisettlement.com. The BIS said fraud may be attempted via letter or e-mail as well.

Category 1C5 Phishing

2004-05-05 **phishing credit card fraud internet café cyber café**

DHS IAIP Daily; http://straitstimes.asia1.com.sg/asia/story/0,4386,249296,00.html

May 05, The Straits Times (Singapore) — Online credit card fraud rocks Indonesia.

A briefing released by VeriSign, a U.S.-based company that monitors Internet activity, in January said that as more and more people around the globe go shopping online, the number of fraudulent transactions or transaction attempts has skyrocketed. An increasing number of fraud 4 attempts is being traced back to Indonesia. The VeriSign report also said that when researchers looked at the ratio of fraud attempts to total transactions from any single country, Indonesia topped the list. One reason why this type of crime is growing in Indonesia, experts said, is the proliferation in recent years of loosely regulated warnets, the local version of cybercafes. Most Indonesians cannot afford home computers and many who need to use the Web frequent the thousands of warnets in urban centers. Donny Budi Utoyo, of the Information Communication Technology Watch group, said, "the warnets do not keep a register of users and what they're doing while online. These kiosks present the perfect shields for offenders." The criminals' growing sophistication adds to the problem. Many criminals have formed syndicates with people living in other countries to better their chances of making money and avoid being traced.

Category 1C5 Phishing

2004-05-05 **phishing survey consumer confidence fraud**

DHS IAIP Daily; http://www.theregister.co.uk/2004/05/05/phishing_fears_survey/

May 05, The Register (UK) — Fear of phishing hits e-commerce.

Concerns about falling victim to phishing scams are eroding U.S. consumer confidence in online banking and e-commerce. A survey out Tuesday, May 4, points to fears about online fraud based on widespread misconceptions about the minimal impact of phishing in overall fraud losses. Almost three in four online account holders responding to an online survey by software developer Cyota said they were less likely to shop online because of phishing. Cyota's poll revealing that 75 percent of account holders are less likely to respond to e-mail from their banks, and over 65 percent said they were less likely to sign up or continue to use their bank's online services as a result of fraud fears. Only 30 percent of the 650 respondents to the survey expressed a high level of confidence that they could distinguish between a real e-mail and a fraudulent one.

Category 1C5 Phishing

2004-05-05 **banking phishing fraud organized crime**

DHS IAIP Daily; http://www.reuters.co.uk/newsArticle.jhtml?type=internetNews&storyID=5047532&section=news

May 05, Reuters — Twelve held in phishing bank scam.

The National Hi-Tech Crime Unit of the United Kingdom (UK) Police have arrested a dozen Eastern European men and women on suspicion of defrauding UK online bank customers out of hundreds of thousands of pounds and diverting the money to a Russian crime gang. Some of the largest retail banks in the world, including Barclays, Lloyds TSB and NatWest in the UK, have been hit by the scam in which spoofed e-mails and Websites are used to trick online customers out of their bank and credit card details. Police say the group had money transferred from the defrauded accounts to bank accounts they had set up with false documents. They would then withdraw the money and ship it to Russia via wire transfers and money orders. Police described the suspects, whom they declined to name, as "mules" recruited by a single Russian organized crime gang to move the money out of a targeted country. Globally, the phishing crime wave has claimed victims in North America and Australia. The suspects are Estonian, Latvian, Russian and Ukrainian nationals. Also seized were computers and other electronic media, passports, check books and bank cards, money and crack cocaine.

Category 1C5 Phishing

2004-05-06 **phishing banking scam theft**

DHS IAIP Daily; http://www.reuters.com/newsArticle.jhtml?type=reutersEdge&st oryID=5062630

May 06, Reuters — Billions of phishing scam e-mails sent monthly.

Fraudulent e-mails designed to dupe Internet users out of their credit card details or bank information topped the three billion mark last month, according to one of the largest spam e-mail filtering companies. Over the past nine months, the monthly volume of phishing e-mails has risen nearly ten-fold to 3.1 billion worldwide in April, San Francisco, CA-based e-mail filtering firm Brightmail said. Brightmail said its spam filters sift through 96 billion e-mails each month. Police suspect organized crime gangs from Eastern Europe are the main culprits in the multi-billion dollar racket. The economic toll from phishing cost U.S. banks and credit card companies $1.2 billion in 2003, Gartner Research said on Thursday, May 6. The Gartner study projected 1.78 million Americans reported giving personal information or financial details about themselves to the fraudsters. Police say the scam is concentrated on English-speaking countries such as the UK, U.S. and Australia, but is expected to target new territories as more people transact and bank online.

Category 1C5 Phishing

2004-05-14 **phishing banking identity theft trick**

DHS IAIP Daily; http://www.theage.com.au/articles/2004/05/14/1084289857949.h tml

May 14, The Age (Australia) — Phishers strike with a new trick.

Phishers in recent scam cases have created a fake address bar in the Web browser, making the e-mail look even more legitimate, according to a media release from the SurfControl Internet Research Center. The e-mail, targeting customers of US Bank, was issued on Wednesday, May 12. The Sydney-based research center says this new technique makes it even harder to identify if the e-mail is fake. In the latest scam, users who click the link in the spam e-mail are taken to a page that displays a fake address bar containing the real US Bank Website address. This address bar has been constructed to overlap the users existing address bar that normally identifies that the address was the scammer's server. Phishers use a Javascript code that calculates where the address bar is located on the user's Web browser, so it can be covered with the allegedly "legitimate" address details, the research center says.

Category 1C5 Phishing

2004-05-18 **phishing identity theft fraud email**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/cybercr ime/story/0,10801,93247,00.html

May 18, IDG News Service — Phishing scam reports skyrocket in April.

Reports of a type of online crime known as "phishing" surged last month, according to figures from a computer security industry group. The Anti-Phishing Working Group (APWG) received reports of more than 1,100 unique phishing campaigns in April, a 178% increase from the previous month, according to figures shared with the IDG News Service. The large increase comes on the heels of a 43% rise between February and March, and financial services and retail companies were hit particularly hard, said Dan Maier, director of product marketing at Louisville, KY-based Tumbleweed Inc. and an APWG spokesperson. Although each report recorded by the APWG corresponds to a unique phishing campaign, the type of attack that's used may not be new in every case, Maier said. In fact, the APWG has evidence that phishing Web pages are being traded online, in the same way that e-mail addresses are traded and sold by spammers. The growing problem also points to increasing interest in the scams by malicious hacking groups and organized crime, Maier said.

Category 1C5 Phishing

2004-05-19 **phishing identity theft fraud email**

DHS IAIP Daily; http://www.kommersant.com/page.asp?id=475549

May 19, Kommerant (Russia) — Citibank Russia hit by phishing scam.

Citibank distributed a statement Tuesday, May 18, denying it was involved in a mass e-mailing of letters requesting more precise credit card information. A client who clicked on the link ended up on a phony Citibank Website where he was asked to enter his card number and PIN code. This type of fraud is known as "phishing," and was the first such case in Russia and a number of clients have already taken the bait. "These messages were actually sent to Citibank clients by frauds," the bank warns in its statement. Citibank's Russian branch was not only the first bank in Citigroup, but also in Russia to have these letters sent in its name. Citibank President Allan Hirst promised that, "in the event of receiving notification from clients of a loss of funds, Citibank is prepared to act in the interests of the client on an individual basis in evaluating each notification." However, the client's best chance of keeping his money in this case is to block the card on time.

Category 1C5 Phishing

2004-05-19 **spammer caught texas man plead guilty luring people fake websites 46 months prison PayPal**

NewsScan

SPAMMER GETS 46 MONTHS IN PRISON

A 20-year old Texas man who pleaded guilty of luring people to fake websites has been sentenced to 46 months in prison. The U.S. Justice Department said the sentence in Houston, Texas, for Zachary Keith Hill was linked to a phishing scam that used emails purported to come from AOL and the online payment service PayPal. The e-mail messages identified the sender as "billing center" or "account department" and the subject line carried warnings such as "AOL Billing Error Please Read Enclosed Email" or "Please Update Account Information Urgent!" (The Australian 19 May 2004) Rec'd from John Lamp, Deakin Univ.

Category 1C5 Phishing

2004-05-21 **phishing identity theft social engineering adjusting attacks**

DHS IAIP Daily; http://www.finextra.com/fullstory.asp?id=11879

May 21, Finextra Research — Fake order confirmations provide new phishing twist.

UK security outfit SecureTest is warning of a new twist on the familiar phishing scam, in which fake e-mail order confirmations direct recipients to a Web server that writes a malicious file to the user's PC. The e-mail, a bogus order confirmation for an IBM Laptop PC, tells the recipient that their bank account has been debited for $1969.03 and provides a link to check or cancel the order. Following the link leads to a Web server which exploits an unpatched weakness in Microsoft's Internet Explorer to write a potentially malicious file to the user's hard drive. Ken Munro, managing director at SecureTest, says the malicious code exploits a known threat which is listed by some of the major anti-virus vendors. "The danger here is in the new format for the scam, and the new form of social engineering," he says. "Many people, on receiving an e-mail saying their bank account has been debited for $1969.03 will at least click on the link and take a further look."

Category 1C5 Phishing

2004-05-26 **phishing attack schemes alerts Department of Treasury**

DHS IAIP Daily; http://gcn.com/vol1_no1/daily−updates/26054−1.html

May 26, Government Computer News — Treasury issues phishing schemes alert, advice.

The Department of Treasury on Wednesday, May 26, warned against schemes in which identity thieves spoof government agencies and financial firms to gain sensitive and financial information from unsuspecting consumers in a report that also offers some tips on how to prevent "phishing." Recent phishing e-mails have purportedly come from government agencies, legitimate financial-sector firms, Internet auction sites and electronic payment services. The government agencies include the Federal Deposit Insurance Corp., the Office of the Comptroller of the Currency, the Securities Investor Protection Corp. and others. A recent private-sector report found that 1,125 instances of phishing were reported in April, 180 percent more than in March. The report found that financial-services Websites are the most commonly spoofed. Treasury's report is on "Lessons Learned by Consumers, Financial Sector Firms, and Government Agencies during the Recent Rise of Phishing Attacks." "The report gives consumers even more information on how to detect, prevent and mitigate the effects of the identity theft scheme known as phishing, a crime that costs American consumers and businesses billions of dollars every year," said Assistant Secretary of Treasury Wayne Abernathy. Report: http://www.treas.gov/offices/domestic-finance/financial-inst itution/cip/pdf/fbiic-fsscc-report-2004.pdf.

Category 1C5 Phishing

2004-05-26 **identity theft credit offers snail mail financial services federal reserve**

DHS IAIP Daily;
http://www.yorkweekly.com/news/05262004/biz_nati/18181.htm

May 26, Wall Street Journal — Federal Reserve scrutinizes credit offers.

With billions of credit solicitations mailed to consumers each year, the Federal Reserve is trying to figure out whether the offers for preapproved credit are fueling identity theft and encouraging consumers to take on excessive debt. While federal law lets lenders and insurance companies offer credit to consumers based on personal data from credit reports, the Federal Reserve is weighing whether the government needs to beef up a program that lets consumers block release of their credit reports. Evan Hendricks, editor of Privacy Times, a Washington-based newsletter, said it is easy for identity thieves to pick up preapproved solicitations by rifling through mailboxes. They can fill out the forms with a new address -- theirs -- and wait for the card to show up. While most credit companies won't send new cards to a new address, some credit unions and others do. Even if a thief can't obtain a credit card, the information in the solicitation itself is valuable, Hendricks said. An offer for a platinum card means a great credit rating, and a thief can sell that personal information to a "fence" who compiles the data and helps other identity thieves.

Category 1C5 Phishing

2004-07-12 **pshishing cybercrime legislation US Senate jail fine scam fraud**

NewsScan

THE PHIGHT AGAINST PHISHERS

The U.S. Senate is now considering legislation to fight "phishers" -- scam artists who use fake Web sites to dupe people into revealing their financial or other private information. The proposed law could cost phishers up to five years in jail and as much as $250,000 in fines. Typically, a scammer who goes phishing will send a message doctored to look like an official notice from some respectable bank or online store, and will use the phony site to trick consumers into giving out their account information. Avivah Litan of Gartner Research warns: "The Internet's becoming a very dangerous place to conduct financial business unless you're willing to scrutinize your activities very closely." (Washington Post 12 Jul 2004)

Category 1C5 Phishing

2004-12-09 **phishing prediction confidentiality PhishNet defenses**

NewsScan;
http://www.usatoday.com/tech/news/computersecurity/infotheft/2004-12-09-phish-starving_x.htm

AN END TO PHISHING?

Former White House Web security chief Howard Schmidt, is predicting that "at this time next year" technology companies and law enforcement agencies will have forced an end to most kinds of Internet "phishing" scams that trick people into revealing their personal and financial information. Schmidt, who has worked with the group that created Digital PhishNet, promises that the major technology companies "are all working together to get the sites shut down as quickly as possible so they won't be around to collect your information." (Reuters/USA Today 9 Dec 2004)

Category *1C5* *Phishing*

2005-01-18 **phishing policy e-mail URL link authenticity**

RISKS 23 68

A REAL PHISHING PAL

Tim Huckvale contributed this observation about the gap between security advice and performance:

I just received an e-mail from PayPal warning me that my credit card was about to expire. Naturally my first thought was that it was a phishing trip, but closer inspection showed it to be genuine.

It ended with the following warning:

> -
> PROTECT YOUR PASSWORD
>
> NEVER give your password to anyone and ONLY log in at
> https://www.paypal.com/. Protect yourself against fraudulent websites
> by opening a new web browser (e.g. Internet Explorer or Netscape) and
> typing in the PayPal URL every time you log in to your account.
>
> -

Typing in the URL is excellent advice. Such a shame that they defeated it by making the link clickable.

Category *1C5* *Phishing*

2005-02-01 **phishing authentication digital signatures e-mail Web URL**

RISKS 23 69

LOOKS LIKE A PHISH, SMELLS LIKE A PHISH….

John Pettitt wonders in RISKS why institutions are failing to use digital signatures on what otherwise look like phishing scams:

I just got this in my e-mail.

>Dear Cardmember,

Your 2004 Year-End Summary is now ready to view online. To access your Year-End Summary, please log in to http://americanexpress.com/yearendsummary2004 <http://www65.americanexpress.com/clicktrk/Tracking?mid=IUYES03020050201053636024433&msrc=ENG-YES&url=https://www124.americanexpress.com/cards/yes/yes_home.jsp?campaignid=Jan_email_05>.

With the online version you can view charges by merchant name, date, or charge amount; view your spending, spending of an Additional Card, or everything at once; and print and save your Year-End Summary for future use. As a *new* feature this year, you can also use business and personal check boxes to sort your annual transactions.

We look forward to serving you.<

As far as I can tell it's real - the sites it links to have certificates that are issued to Amex. However there is no way to tell without clicking the link and checking the certificate (something I teach my users not to do) that the mail really came from Amex. Even the message headers show it originating from aexp.com which sounds close but then so do the best phishing scams.

Given that a large percentage of the world now uses s/mime capable mailers (Outlook, Outlook express, Thunderbird, Mozilla, etc.), why is it that institutions are still sending unsigned e-mail?

Category 1C5 Phishing

2005-02-02 **phishing Harry Potter books Rowling scam fraud electronic copies intellectual property copyright organized crime**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A56379-2005Feb2.html

J.K. ROWLING DENOUNCES INTERNET FRAUDSTERS

J.K. Rowling, author of the mega-popular Harry Potter series, is warning fans to beware of Internet "phishing" scams claiming to sell electronic copies of her latest book, "Harry Potter and the Half-Blood Prince." "The only genuine copies of Harry Potter remain the authorized traditional book or audio tapes/CDs distributed through my publishers," says Rowling, and her copyright lawyer, Neil Blair, notes that Rowling has never granted licenses for electronic versions of her books. "Please, please protect yourselves, your computers and your credit cards and do not fall for these scams," says Rowling. Police say they suspect organized crime gangs in Eastern Europe are behind the fraudulent e-mail offers. (Reuters/Washington Post 2 Feb 2005)

Category 1C5 Phishing

2005-02-15 **phishing redirection URL identity theft eBay trick subterfuge**

RISKS 23 73

EBAY REDIRECTS TO PHISHERS FROM THEIR OWN SITE

Pete Krawczyk found another exploit that might fool naïve users of eBay. He wrote:

>eBay fraudsters have a new trick up their sleeve: using eBay's servers to link to a fraudulent web site.

In the past, it was easy to pass a URL through a decoder and find that the actual server hosted behind a URL was not owned by eBay, since phishers would use @, %40, or other domain misdirection tactics. However, I recently received an eBay fraud mail that contained the following URL, which has been edited to point to Google:
http://cgi4.ebay.com/ws/eBayISAPI.dll?MfcISAPICommand=RedirectToDomain&DomainUrl=http://www.google.com/

As you can see, that URL will access cgi4.ebay.com, and eBay will gladly hand the browser over to Google for further action. That URL can be trivially changed to any web site.

The RISK is obvious: allowing untrusted URL redirects in this case will fool many more people who may now believe that eBay is truly asking for account details, and may lead to further identity theft.<

Category 1C5 Phishing

2005-03-10 **phishing fraud criminals Web redirection China proxy server hijacking session**

RISKS 23 78

WEBSITE HIJACKINGS, 302 REDIRECTS, AND SECURITY ISSUES

Tim Chmielewski wrote:

I have been reading about the problems with the 1bu.com site on the forum Webmaster World and decided to try it myself.

Basically what it is that if you type in any site with the format:
http://www.sitename.com.1bu.com
you will get redirected to another site (actually a proxy server in China) that looks exactly like your site, but none of your pages that use scripting will work.

Using the same technique other sites could hijack banking or online shopping sites and redirect input so they collect your credit card and other information.

While this has been a popular topic of discussion in the webmaster forums, Google itself is silent on the issue.

Category 1C5 Phishing

2005-03-31 **Microsoft lawsuits John Doe phishing scams**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=8051350

LAWSUITS TARGET PHISHERS

Microsoft has filed 117 "John Doe" lawsuits against operators of Web sites involved in phishing scams. Phishers send e-mail messages that purport to be from a bank or other financial services institution. The e-mails tell recipients that they must visit a Web site and disclose personal information, typically under the pretense of updating account records or something similar. Disclosed information is then used for credit card fraud and other types of identity theft. Microsoft said it was filing the lawsuits in an effort to discover who is behind the largest phishing operations and put them out of business. Microsoft's Aaron Kornblum said, "We must work together to stop these con artists from misusing the Internet as a tool for fraud." Reuters, 31 March 2005

Category 1C5 Phishing

2005-06-29 **phishing phishers prison sentence UK Britain personal information stolen money trafficking FBI Hi-Tech Crime Unit US Secret Service**

EDUPAGE; http://news.com.com/2100-7348_3-5766860.html

PHISHERS LOCKED UP

Two men have been sentenced to prison in Britain for orchestrating a phishing scheme that used stolen identities to pilfer as much as 6.5 million pounds over two years. Douglas Harvard and Lee Elwood were sentenced to six and four years respectively for their parts in the phishing ring, which authorities said garnered at least 750,000 pounds during one 10-month period. The men allegedly worked with individuals in Russia to traffic in personal information and the money stolen using that information. Mick Deat, deputy head of Britain's National Hi-Tech Crime Unit, issued a statement thanking the U.S. Secret Service and the FBI for their assistance in the investigation. The statement also expressed Deat's hope that the convictions will discourage others who might consider such scams. CNET, 29 June 2005

Category 1C5 Phishing

2005-07-01 **Phishing MSN Input sanitized URL passport**

DHS IAIP Daily; http://www.zone−h.org/advisories/read/id=7764

PHISHING PROBLEMS ON MSN

Multiple phishing problems exist on support.msn.com, permitting to a possible attacker to conduct phishing attack against a user. 1) Input passed to the "ru" parameter in "pplogin.aspx" isn't properly sanitized before being returned to the user. 2) Input passed to the 'mspplogin' parameter isn't properly sanitised, and by using specialy crafted URL an attacker can cause the user to be redirected to an arbitrary URL for the passport authentication. Another phishing problem exists on login.passport.net.The problem is caused due to input passed to the "ru" in "uilogout.srf" isn't properly sanitised. By using specialy crafted URL an attacker can cause the user to be redirected to an arbitrary URL for the passport authentication.

Category 1C5 Phishing

2005-07-25 **anti-phishing software password scrambling hiding Stanford University**

EDUPAGE; http://www.siliconvalley.com/mld/siliconvalley/12218576.htm

SOFTWARE HIDES PASSWORDS FROM PHISHERS

Two professors at Stanford University are set to unveil software designed to foil phishers by scrambling passwords entered into Web sites. John Mitchell and Dan Boneh developed the software, called PwdHash, to deal with the growing problem of Web sites that lure computer users into disclosing personal information. The software creates a unique password for each Web site a user visits. If the user goes to a bogus version of a legitimate Web site, the software creates a separate password, leaving the operator of the bogus site with a password that will not work at the real site. Previously, the pair of professors have written software that tries to identify fraudulent Web sites and notifies the user when such a site is suspected. San Jose Mercury News, 25 July 2005

Category 1C5 *Phishing*

2005-09-26 **phishing fraud data leakage surveillance password userID capture Web site social engineering**

Computerworld

YAPS (YET ANOTHER PHISHING SCAM): YAHOO!

Criminals fielded yet another phishing scam in late September 2005 in which they tricked people into visiting fake Yahoo Web sites to capture login information but forwarded the session to a real part of the Yahoo portal. The phishing site was located in a Geocities section of Yahoo, making it more difficult to detect the fraud through inspection of the URLs involved.

Category 1C5 *Phishing*

2005-09-26 **phishers phishing Yahoo! Photos target fake sign-in**

DHS IAIP Daily; http://www.snpx.com/cgi−bin/news55.cgi?target=110977854?−2622

PHISHERS TARGET YAHOO! PHOTOS

Phishing attacker are attempting to capture a user's Yahoo! ID and password by sending out fake sign-in pages. Users are receiving an email or instant message that claims to be from a friend wanting to show off photos. The message contains a link to a phishing site, which records the user's Yahoo! ID and password, and then forwards the Yahoo! ID and password on to the real Yahoo! Photos site.

Category 1C5 *Phishing*

2005-10-03 **phishing Anti-Phishing Act 2005 scam fraud California law**

EDUPAGE; http://informationweek.com/story/showArticle.jhtml?articleID=17120267

CALIFORNIA PASSES ANTI-PHISHING LAW

A tough new anti-phishing law makes California the first state to pass legislation targeting that particular brand of online scam. The Anti-Phishing Act of 2005 makes it a crime to use "the Internet or other electronic means, to solicit, request, or take any action to induce another person to provide identifying information by representing itself to be a business without the approval or authority of the business." Identifying information includes Social Security numbers, credit card numbers, passwords, PINs, and other information that can be used to steal from individuals. Those found guilty of phishing are subject to fines of $2,500 per violation, as well as damages to victims of either actual losses or $500,000, whichever is greater. InformationWeek, 3 October 2005

Category 1C5 *Phishing*

2005-11-29 **fraud scam identity theft phishing anti-phishing DHS SRI report**

RISKS; http://www.anti-phishing.org/Phishing-dhs-report.pdf ; 11

DHS ANTI-PHISHING REPORT

Online identity theft, a.k.a. "phishing," refers to attacks that exploit a wide variety of RISKS, using both technology and social engineering, to illicitly obtain and profit from confidential information. A new report on online identity theft, sponsored by the US Department of Homeland Security and SRI International, provides a holistic treatment of the subject. The report discusses technologies used by phishers, breaks down the flow of information in a phishing attack, identifies chokepoints at which an attack can be thwarted, and discusses technical countermeasures that can be applied at each chokepoint. While technology alone cannot solve the phishing problem, substantial opportunities to mitigate the losses are identified. The report is titled "Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures."

[Summary from Aaron Emigh]

Category 1C5 *Phishing*

2006-03-20 **Microsoft phisher target phishing scam bogus Web sites fraud theft trademark violation intellectual property rights issues**

EDUPAGE; 23
http://news.zdnet.co.uk/internet/security/0,39020375,39258528,00.htm

MICROSOFT TARGETS PHISHERS

Microsoft has announced its intention to use trademark laws to confront the operators of phishing scams. Phishers set up bogus Web sites designed to look like legitimate sites and trick users into entering confidential information. At a press conference in Brussels, Microsoft said it would level trademark-violation charges against outfits that pose as Microsoft sites such as Hotmail or MSN. The Global Phishing Enforcement Initiative will target more than 100 sites in Europe, the Middle East, and Africa. Also part of the initiative will be stronger ties between Microsoft and international law enforcement agencies, including Interpol, to fight phishers. Microsoft's strategy may prove more successful at defeating phishers than prosecutions that depend on evidence that the sites in question had actually defrauded users. Microsoft's legal approach would simply need to demonstrate that site operators infringed on the company's trademarks.

1D Law Enforcement & Forensics (technology, organizations, proposals, litigation, rulings, judgements)

Category 1D *Law Enforcement & Forensics (technology, organizations, proposals, litigation*

1997-04-07 **identity theft**

RISKS 19 5

The San Francisco Chronicle published a detailed article by Ramon G. McLeod on theft of identity. The author discussed several cases of identity theft and provided telephone numbers for several organizations and law enforcement agencies to whom victims could turn for (various degrees of) help.
See <http://www.sfgate.com/cgi-bin/chronicle/article.cgi?file=MN48551.DTL&directory=/chronicle/archive/1997/04/07>.

Category 1D *Law Enforcement & Forensics (technology, organizations, proposals, litigation*

1997-08-07 **identity collision theft SSN**

RISKS 19 28

In August, Antonio Picazo Mendoza Jr. of Stockton, CA, was taken to a local hospital after being beaten and robbed. When his first and last names, birthday, and Social Security Number matched those of a convicted criminal, Antonio Blanco Mendoza, the victim was thrown in jail for 17 days. It was unknown whether this was a case of mistaken identity or deliberate theft of identity.

Category 1D *Law Enforcement & Forensics (technology, organizations, proposals, litigation*

1998-06-15 **identity theft impersonation fraud**

Los Angeles Times

The FTC & GAO reported on the growing problem of identity theft. Some key problems include the lack of specific definition of identity theft; enforcement fragmented among Secret Service, SSA, FBI, USPS Inspection, and the IRS; poor tracking of incidents; and the fact that legally, the victims are viewed as the banks, not the individuals whose identities have been misappropriated. Losses due to identity theft and fraud were U$745M in 1997 vs U$450M in 1996.

Category 1D *Law Enforcement & Forensics (technology, organizations, proposals, litigation*

1998-07-23 **identity theft impersonation fraud**

AP

Ann Pulliam spoke in favor of new laws to make theft of identity a felony. She and her husband's Social Security Numbers and names were fraudulently used to set up a company and bank accounts; the thieves stole $5,000 and ruined the Pulliams' credit record. Although the culprit was eventually arrested and tried (he was jailed for attempted murder when he tried to run over a Secret Service agent assigned to the case), the Pulliams are still trying to track down and correct the wrong information in many different credit-record databases.

Category 1D *Law Enforcement & Forensics (technology, organizations, proposals, litigation*

1998-10-31 **identity theft impersonation fraud**

US Newswire, OTC

H.R. 4151, the "Identity Theft and Assumption Deterrence Act of 1998," signed into law 1998.10.30. Law makes identity theft a felony: "This legislation will make identity theft a Federal crime, with penalties generally of up to 3 years imprisonment and a maximum fine of $250,000. Specifically, the legislation would penalize the theft of personal information with the intent to commit an unlawful act, such as obtaining fraudulent loans or credit cards, drug trafficking, or other illegal purposes. It would also direct the Federal Trade Commission to help victims deal with the consequences of this crime."

Category 1D *Law Enforcement & Forensics (technology, organizations, proposals, litigation*

1999-05-06 **identity theft impersonation fraud credit card bank e-mail**

Globe and Mail (Canada)

Tyler Hamilton wrote a good review of identity theft in Canada's _Globe and Mail_ newspaper on May 6, 1999. The article included practical advice from Anne Cavoukian, Canada's Privacy Commissioner; excerpts:

HOW TO FOIL THE IDENTITY THIEVES

* Never send any personally identifying information in an E-mail. Look into buying encryption software that will ensure that the only eyes that see the message belong to the person you're E-mailing.

* When you go to a Web site, don't provide any identifying information, unless you and the business have established a trusting relationship. Banks, for example, are usually safe bets.

* Avoid chat groups and news groups, or at least use an alias when posting messages in these open areas on the Internet.

* Ask to be taken off commercial mailing lists.

* Ask your credit bureau to attach a "fraud alert" note to your records, meaning that any request to change or access information in your file must be followed up by a call to your home. If your credit bureau doesn't have a fraud alert service, ask why and explain its importance to the bureau.

* Finally, empower yourself on the Internet by buying privacy-enhancing technologies, such as "anonymizer" software. The software lets you surf the Web and engage in E-commerce transactions under a pseudonym without having to compromise your privacy.

1D1 Organizations, cooperation for law enforcement

Category 1D1 *Organizations, cooperation for law enforcement*

1998-01-04 **banking audit trails money laundering police investigation international cooperation**

Economic Times of India

Police investigating economic crimes and illegal drug distribution are concerned about the growing use of the Internet to send money through a number of national banking systems, causing problems of tracking and jurisdiction. In India, the government set up a subgroup of the Economic Intelligence Council to explore the situation and coordinate efforts with other law-enforcement authorities around the world.

Category 1D1 *Organizations, cooperation for law enforcement*

2000-01-10 **law enforcement cybercrime initiative proposal plan federal government**

NewsScan, Los Angeles Times, Edupage, EPIC Alert

The Clinton administration proposed a national plan for fighting cybercrime. In January 2000, Attorney General Janet Reno described an information-sharing network for law enforcement and several new cybercrime labs staffed by law enforcement personnel from the federal, state and municipal levels. She proposed that law enforcement agencies have cybercrime coordinators on call. The administration plan would increase funding for academic research in INFOSEC and undergraduate scholarships by $160M to a total of $621M; the new federal Institute for Information Infrastructure Protection would also foster joint government-industry task forces for security research.

Category 1D1 *Organizations, cooperation for law enforcement*

2000-01-10 **law enforcement network Law Net US government crime initiative investigation criminal hackers Web vandalism international cooperation federal state local cybercrime**

AP

In the wake of high-profile criminal attacks on e-commerce, US Attorney General Janet Reno announced her intentions to set up an information-sharing network among federal, state and local law-enforcement authorities to fight cybercrime. The "LawNet" proposal would include setting up cybercrime laboratories whose costs could be shared among participating agencies. In addition, the AG recommended a new system for speeding interstate transfers of subpoenas and warrants necessary for investigations of Internet-related crime. New York Attorney General Eliot Spitzer said, "It is perhaps not Big Brother we should be worried about, but Big Browser."

Category 1D1 *Organizations, cooperation for law enforcement*

2000-01-17 **government law enforcement police Internet cybercrime**

Times of London

The British Home Secretary, Jack Straw, announced plans for a national computer-crime squad. He authorized the National Criminal Intelligence Service (NCIS) to develop a specialized team to attack Internet crimes such as fraud, money laundering, pornography, illegal gambling and pedophile rings. The squad would collaborate with other agencies such as the taxation department (Inland Revenue), domestic security intelligence (MI5) and the international surveillance center (GCHQ).

Category 1D1 *Organizations, cooperation for law enforcement*

2000-02-17 **law enforcement international cooperation networking sharing information Europe**

Daily Telegraph (London)

The European Commission began a process for improving the battle against cybercrime. The Commission was considering setting up a special school for law enforcement to learn more about fighting cyberspace crime; another idea was increased involvement by Interpol in criminal investigations involving computers and networks.

Category 1D1 *Organizations, cooperation for law enforcement*

2000-02-18 **law enforcement fraud cyberspace securities funding**

Newsbytes

The Securities and Exchange Commission (SEC) announced that it was hiring about 100 new officials to fight cyberspace fraud, of which 60 will police the Web. There were already 250 workers scanning the Web full time, said the Chairman, Arthur Levitt in mid-February 2000. He cited a "frightening" recent case in which a criminal hacker inserted false news of a merger on a company Web site. Stock manipulations include rumor-mongering to drive up the price of stock already held and also to drive down the price of stocks already sold on the futures market at a higher price than the desired target.

Category 1D1 *Organizations, cooperation for law enforcement*

2000-03-24 **fraud law enforcement government agency investigation prosecution international cooperation**

NewsScan

The U.S. Federal Trade Commission . . . [said] it's been working with other international organizations in an unprecedented global effort to crack down on fraudulent, get-rich-quick schemes that are promoted through the Internet. The sweep, which began in February, involved 28 countries and targeted 1,600 suspect Web sites. Typical scams included pyramid schemes, unrealistic investment opportunities and easy-money come-ons. Domestically, the FTC has enlisted the help of the Postal Service and the Securities and Exchange Commission enforcement units to assist in monitoring online fraud. FTC officials say the sites have now been warned that they must change their claims or it will attempt to have them shut down. "We're going to run them off the Web and where appropriate, put them in jail," says Drew Edmondson, attorney general of Oklahoma. (Financial Times 24 Mar 2000)

Category 1D1 *Organizations, cooperation for law enforcement*

2000-05-08 **fraud law enforcement consumer report investigation prosecution Web Internet**

NewsScan

The U.S. Department of Justice and the Federal Bureau of Investigation are collaborating on the creation of an Internet Fraud Complaint Center, which will give consumers and businesses a one-stop shop for reporting incidents in which a computer was used for criminal activity, such as fraudulent claims made over a Web site, via e-mail, or in chat rooms. It will not cover crime in which computers were the target, such as the distributed denial of service attacks that crippled some major businesses' computers recently. Those problems should be addressed by the National Infrastructure Protection Center. (TechWeb 8 May 2000)

Category 1D1 *Organizations, cooperation for law enforcement*

2000-05-14 **computer crime international cooperation jurisdiction laws legislation regulations investigations treaty standards**

NewsScan, San Jose Mercury News http://www.sjmercury.com/svtech/news/breaking/merc/docs/011053.htm, Los Angeles Times http://www.latimes.com/business/20000518/t000046914.html

With the "Love Bug" virus providing a recent reminder of the problem of cybercrime and other kinds of mischief on the Internet, leaders from the Group of Eight countries . . .[met] to see what can be done, and the 41-nation Council of Europe is working with the U.S., Canada, Japan and South America to draft a treaty to standardize laws against Internet crime. Jonathan Fornici of the Internet security consulting firm AtomicTangerine says that governments need to write laws that make the punishment clear, because the way things are now, people know security violations are wrong — "but what's the repercussion?" In the Love Bug case, investigators in the Philippines delayed a raid for several days until prosecutors found a law that might apply. (AP/San Jose Mercury News 14 May 2000)

[When] Envoys from the world's leading industrialized nations and private business met . . . in Paris to discuss cooperation in fighting Internet-based crime, [there were] . . . widespread differences in national approaches [that] could stymie efforts. At the heart of those differences is the degree to which governments are willing to monitor the Net for illegal behavior, which inevitably occurs at the expense of citizens' privacy. In addition, e-commerce businesses tend to discourage more government involvement, which they view as a menace to both economic growth and individual liberty. On April 27, the Council of Europe published a draft treaty proposing uniform international law enforcement standards in cyberspace, including the requirement that all messages and content sent via the Internet be stored for three months before deleting. That proposal has met with mixed reactions among both governments and industry representatives. The U.S., which held observer status during the drafting, . . . [did not endorse] that proposal. (Los Angeles Times 18 May 2000)

Category 1D1 *Organizations, cooperation for law enforcement*

2000-07-19 **civil liberties investigation monitoring interception privacy law enforcement government program encryption keys passwords**

NewsScan, San Jose Mercury News
http://www.sjmercury.com/svtech/news/breaking/internet/docs/374641.htm,
New York Times
http://www.nytimes.com/library/tech/00/07/biztech/articles/19britain.html,
USA Today

The British government . . . [said] its plans to allow security services to monitor Internet traffic . . . [would] not create an overly intrusive cyberspace spy agency, but civil liberties groups argue the Regulation of Investigatory Powers (RIP) bill would give police free rein to snoop on the Internet and could result in people being jailed for forgetting their passwords. The bill would require citizens to reveal encryption keys to the police or face a two-year jail term. "The police have to prove the encryption key was deliberately withheld," says a Home Office spokesman. "We're not talking about people going to prison for forgetting passwords... Interception of communications is only used on the authorization of the Home Secretary himself. And it's only used in defense of national security or on suspicion of serious crime, like narcotics smuggling or terrorism." (Reuters/San Jose Mercury News 26 May 2000)

[In July,] UUNet and Nokia . . . [participated] in a last-ditch effort to derail the controversial U.K. Regulation of Investigatory Powers Bill, which would allow law enforcement officials to require ISPs to intercept e-mail messages and other data on their systems. Individuals or companies sending encrypted data could be required to provide it in plan text or surrender a software encryption key to decode the message. UUNet called the legislation, to be debated today in the House of Lords, "fundamentally flawed" and "draconian," and added, "It would be tragic if by imposing a new requirement on ISPs, the U.K. were to make itself uncompetitive in the provision of Internet services. We would ask the government to step back and re-think the whole bill." Meanwhile, Nokia is the first company to voice concern over the legislation based on its impact on future wireless services. (Financial Times 12 Jul 2000)

[Also in July,] . . . . A government official argued that "the powers in the bill are necessary and proportionate to the threat posed by 21st century criminals, no more, no less." The bill has angered civil libertarians, and a spokesperson for Amnesty International in London said: "What this does is contravene a large number of fundamental rights in the European convention on human rights and other international standards, which include the right to privacy, the right to liberty, the right to freedom of expression, and the right to freedom of association." (New York Times 19 Jul 2000)

[At the end of July, the British] Parliament . . . passed legislation that will allow law enforcement authorities to demand records of Internet traffic for scrutiny by MI5, the country's domestic intelligence agency. The rationale for the new law is that it's necessary to counter the increasing technological sophistication of organized criminal efforts; however, one Labor Party dissenter said that certain provisions of the bill "are born of complacency, are unsatisfactory, and have little regard for the protection of privacy and commercial confidences." (AP/USA Today 28 Jul 2000)

Category 1D1 *Organizations, cooperation for law enforcement*

2000-09-26 **fraud prevention investigation law enforcement international commerce organization alliance consortium teaching support resources clearinghouse best practices**

NewsScan, E-Commerce Times
http://www.ecommercetimes.com/news/articles2000/000926-3.shtml

A group of leading U.S. e-commerce merchants and payment processing companies have formed an industry coalition to reduce online fraud. The Worldwide E-Commerce Fraud Prevention Network, which includes American Express, Buy.com and Expedia, will serve as a clearinghouse for information on best fraud prevention practices and current fraud prevention trends, as well as security seminars, law enforcement resources and security software vendors. One of the main concerns for members is that online merchants are often held liable for the cost of goods purchased with stolen credit cards. "More than 41% of the merchants we canvassed didn't know that they — not the credit card companies — are liable for fraud," says one security software firm executive. "Online credit card fraud is projected to cost merchants US$9 billion annually by next year." (E-Commerce Times 26 Sep 2000)

Category 1D1 *Organizations, cooperation for law enforcement*

2001-01-16 **cooperation alliance technology hacking ISAC**

NewsScan

TECH ALLIANCE TO SHARE DATA ON HACK ATTACKS
Nineteen big-name companies, including AT&T, Microsoft, Oracle, Cisco, IBM and Hewlett-Packard, are banding together to launch a private, nonprofit alliance to share sensitive data about cyber-attacks and vulnerabilities in their hardware and software products. "The overriding goal is to protect ourselves from cyber-hazards, whether they be deliberate attempts or accidental events," says Guy Copeland of Computer Sciences Corp., a board member of the new Information Technology Information Sharing and Analysis Center (IT-ISAC). "We've known that each of us have a little bit of the picture... By sharing the information, we can be that much smarter." Other technology firms will be invited to join the alliance for $5,000 a year. Three similar private alliances to deter cyber-attacks exist already, covering the banking, telephone and electrical industries, and more are planned for oil and gas companies and the transportation sector. (Wall Street Journal 16 Jan 2001)
http://interactive.wsj.com/articles/SB97959775829133953.htm

Category 1D1 *Organizations, cooperation for law enforcement*

2001-04-25 **international cooperation law enforcement police fraud laws consumer information investigations**

NewsScan

COUNTRIES TEAM UP TO FIGHT E-FRAUD
Thirteen countries have agreed to back a project aimed at stifling cross-border Internet fraud and improving consumer confidence in e-commerce. A multilingual Web site -- www.econsumer.gov -- will provide information on consumer protection laws in the 13 countries and offer consumers a way to file complaints online. The cooperating governments will use a parallel, but secure, site to share complaint data and information on e-commerce fraud investigations. The 13 countries are: Australia, Canada, Denmark, Finland, Hungary, Mexico, New Zealand, Norway, South Korea, Sweden, Switzerland, the U.K., and the U.S. The plan is also backed by the Organization for Economic Cooperation and Development. (Financial Times 25 Apr 2001)
http://news.ft.com/news/industries/internet&e-commerce

Category 1D1 *Organizations, cooperation for law enforcement*

2001-11-08 **international agreement convention cybercrime investigation fraud child pornography cooperation law enforcement investigation extradition**

NewsScan

EUROPEAN COUNCIL ADOPTS FIRST CYBERCRIME TREATY
The 43-nation Council of Europe has adopted a convention on cybercrime that criminalizes activities such as fraud and child pornography committed over the Web and sets up global law enforcement procedures for conducting computer searches, intercepting e-mail messages, and extraditing criminal suspects. The convention marks the first treaty on criminal offenses committed via the Internet. It will enter into force once five states, including at least three Council of Europe member nations, have ratified it. States will have that opportunity at a conference on cybercrime to be held in Budapest on November 23. (Reuters 8 Nov 2001)
http://news.excite.com/news/r/011108/13/net-europe-cybercrime-dc

---

Category 1D1 *Organizations, cooperation for law enforcement*

2002-01-14 **ISP Internet service providers association group security cooperation collaboration information sharing critical infrastructure protection law enforcement investigation**

NewsScan

ISPs FORM A NEW ASSOCIATION
Several Internet companies have banded together to form a new group that will focus on compliance and liability issues. The U.S. Internet Service Provider Association (US ISPA) will replace the Commercial Internet eXchange, which is folding. Founding members of the new group including AOL, Cable & Wireless, Earthlink, eBay, Teleglobe, Verizon Online and WorldCom. US ISPA vice president Tom Dailey says the group will examine such issues as online security, liability and compliance with the new antiterrorism law, the [U.S.A.P.A.T.R.I.O.T.] Act, and the Council of Europe Convention on Cybercrime. In addition, the US ISPA will raise "a variety of other policy and legal issues of concern to ISPs, such as Internet privacy, content regulations and intellectual property." (Wall Street Journal 14 Jan 2002)
http://interactive.wsj.com/articles/SB1011053572133523720.htm (sub req'd)

Category 1D1 *Organizations, cooperation for law enforcement*

2002-04-22 **mandatory reporting computer crime government law enforcement police proposal statistics knowledge base incidence rates risk management**

Security Wire Digest 4 31

*PROSECUTOR SAYS HACK ATTACKS MUST BE REPORTED
Companies need to come forward and admit when they've been hacked, urged U.S. prosecutor David Green at Microsoft's Government Leaders' Conference last week. So long as companies fail to report attacks, the government will be limited in its ability to find culprits and bring them to justice, said Green, the principal deputy chief of the Department of Justice's computer crime division. "We have to make the reporting of these attacks the norm. We need corporate cooperation to report these sorts of vulnerabilities to law enforcement in order that they are able to deal with it," he told delegates, according to a published report. A key, he added, is creating a public-private partnership that promotes trust and honors confidentiality. Congress is currently considering legislation that would exempt security information shared with the government from the Freedom of Information Act.

Category 1D1 *Organizations, cooperation for law enforcement*

2002-06-17 **surveillance investigation law enforcement government legal guidelines Web tax intelligence**

EDUPAGE

UK WEB SITE GUIDES LEGAL SNOOPERS
The British government has set up a Web site to advise qualified UK government departments and organizations how to stay within legal bounds in carrying out covert surveillance of British citizens' use of their telephones, fax machines, Web browsers, and e-mail accounts. Passage of the Regulation of Investigatory Powers Act in 2000 made it easier for customs, tax, police, and intelligence services to get permission to spy on criminals and citizens. The RIP Act removed the requirement to obtain permission for surveillance from a judge and put approval and oversight into the hands of the Office of Surveillance Commissioners. BBC, 17 June 2002
http://news.bbc.co.uk/hi/english/sci/tech/newsid_2049000/2049593.stm

---

Category 1D1 *Organizations, cooperation for law enforcement*

2003-01-31 **database sharing collaboration law enforcement State Department**

NewsScan

VISA APPLICATIONS TO BE SHARED WITH LAW ENFORCEMENT
The U.S. State Department will soon give law enforcement officials access to a database containing 50 million overseas applications for U.S. visas. The information will be accessible by intelligence agencies, the FBI, and police departments throughout the country. Although the database will not be making any new information available (but simply making existing information more accessible to law enforcement agencies), a Justice Department official says: "There is a potential source of information that isn't available elsewhere. It's not just useful for terrorism. It's drug trafficking, money laundering, a variety of frauds, not to mention domestic crimes." But some civil liberties advocates say they are worried that the system will be abused by over-use: "The availability of this information will change police conduct. You are more likely to stop someone if you have the ability to query a database. The data chases applications." (New York Times 31 Jan 2003)

Category 1D1 *Organizations, cooperation for law enforcement*

2003-02-12 **Europe coordination network information security agency infowar defense**

NewsScan

EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY
The European Commission is planning the creation of a European Network & Information Security Agency intended to coordinate computer security activities of the 15 EC member states. Erkki Likanen, the EC's commissioner for the information society, said that the European Union "will benefit from increased coordination between member states to achieve a sufficiently high level of security in all member states. The Internet is a wonderful tool, but to be able to benefit from it, you have to guarantee security." (Computerworld 10 Feb 2003)

Category 1D1 *Organizations, cooperation for law enforcement*

2003-03-17 **Pakistan cyber crime wing security intelligence**

NIPC/DHS

March 13, Wired — Pakistan creates cyber crime wing.

A Pakistani security agency has launched a special wing to combat cyber crimes in part because the country had to rely on U.S. investigators to trace e-mails sent by the kidnappers of American journalist Daniel Pearl a year ago. "The purpose of establishing the National Response Center for Cyber Crimes is to stop misuse of the Internet and trace those involved in cyber-related crimes," Iftikhar Ahmad, spokesman for Pakistan's Interior Ministry, told the Associated Press on Wednesday. "The importance of this special wing was felt when Daniel Pearl was kidnapped, and his captors started sending e-mails to newspapers," he said. The Wall Street Journal correspondent disappeared on January 23, 2002, from Pakistan's southern city of Karachi. "The National Response Center for Cyber Crimes will play a key role in the days to come in tracing those terrorists who often use the Internet or prepaid telephone cards to communicate messages to their associates for carrying out acts of terrorism and other purposes," Ahmad said. The special wing has been established at the headquarters of an intelligence agency in Islamabad, Pakistan's capital.

Category 1D1 *Organizations, cooperation for law enforcement*

2003-03-18 **anti-hacking anti-virus hotline Korea network emergency report**

NIPC/DHS

March 11, SC Infosecurity News — Korean government opens anti-hacking and virus hotline.

The Korea Information Security Agency (KISA) has teamed up with 13 major ISPs and other internet bodies in Korea to create a national anti-hacking and virus hotline and information service. Their aim is to take rapid action in the event of a cyberattack. KISA, which is affiliated with the Korean government's Ministry of Information and Communication, defines a network emergency as where the volume of Korean internet traffic varies by 20 per cent internationally and 50 per cent nationally, within the space of five minutes. All Korean ISPs and internet data centers (IDCs) in Korea are expected to report their operational status twice a day to the hotline, as well as keeping the hotline staff informed of their status and countermeasures taken in the event of a network emergency.

Category 1D1 *Organizations, cooperation for law enforcement*

2003-04-14 **Pakistan Network Security Working Group ISP IT intelligence defense virus Trojan**

NIPC/DHS

April 09, The International News — Pakistan sets up Working Group for Network Security.

The ministry of information technology in Karachi, Pakistan, has set up a Working Group for Network Security to outline measures for cyber safety in the country. "The Working Group would comprise around 25 persons belonging to ministry of IT, intelligence agencies, representatives from internet service providers (ISPs) and the country's renowned software houses," said an official at the ministry who wished not to be named. "You can call it a professionals' forum with objectives to oversee and drive the development of network security, threat assessment, defensive and offensive mechanisms, viruses and Trojans. The Group will bring together various public and private sector entities to create synergies and establish direct contact among the specialists," the official informed. Initially, the Group would discuss growing threat of insecure networks, intrusions, web page defacements and cyber terrorism. It will then discuss formulation of policies and guidelines and encourage ideas related to strong authentication mechanism such as smart cards, PKI, biometrics, Kerberos, tokens, digital certificates.

Category 1D1 *Organizations, cooperation for law enforcement*

2003-04-24 **hacker hacking Pakistan information telecommunication Working Group Network Security**

NIPC/DHS

April 22, The International News (Pakistan) — Pakistan to use hackers against hackers.

The ministry of information technology and telecommunications in Karachi, Pakistan, has decided to hire hackers to confront cyber attacks on government websites and silicon networking. The decision came at a meeting held last week to set up a Working Group for Network Security — one of the steps to counter hackers' moves. The group is composed of ministry officials, intelligence agencies sleuths and representatives from private sector internet service providers (ISPs) and software houses in Pakistan.

Category 1D1 *Organizations, cooperation for law enforcement*

2003-05-09 **New South Wales counter-terrorist police hackers fight terrorism mobile phones cars chips organizations court**

NIPC/DHS

May 09, Sydney Morning Herald (Australia) — Australian police enlist hackers to fight terrorism.

Australian police are offering 20 computer IT specialists the opportunity to become highly paid operatives working for the New South Wales (NSW) counter-terrorist unit. The successful applicants will join a newly created unit within the police Special Service Group that will be called the State Electronic Evidence Branch. The computer specialists will examine computer drives and even microchips from cars and mobile phones of people suspected of having links with terrorist organizations. Superintendent Tony Jeffries said the cyber sleuths would examine computer pathways for hidden information and undergo training in forensic analysis so that any potential data relating to terrorist activities in NSW could be used in court in prosecutions of suspects.

Category 1D1 *Organizations, cooperation for law enforcement*

2003-05-16 **intrenet fraud scams identity theft goods purchase online pharmaceutical drugs**

NewsScan

U.S. CRACKS DOWN ON INTERNET FRAUD
The Justice Department has charged more than 130 people with perpetrating a variety of Internet scams, as well as identity theft and failure to deliver goods purchased online. The crackdown, dubbed Operation E-Con, involved more than 90 investigations involving 89,000 victims whose losses totaled at least $176 million. In one case, the suspects used a Web site to sell more than $2 million worth of pharmaceutical drugs without any prescriptions or physician involvement with the purchasers. In another scam, about 400 men lost about $3,000 each when they sent money off in the hope of winning the hand a Russian bride. Other scams promoted fraudulent investment opportunities, Ponzi-type pyramid schemes and the illegal sale of copyright-protected software, games and movies. Officials say they've managed to recover about $17 million from alleged perpetrators. (AP/Siliconvalley.com 16 May 2003)

Category 1D1 *Organizations, cooperation for law enforcement*

2003-05-16 **south korea security hackers cyber-warfare north Seoul Defense Security Command Song Young business**

NIPC/DHS

May 16, Reuters — South Korea fortifying computer security.

North Korea is training around 100 computer hackers each year to boost its cyber-warfare capabilities, pushing the South to fortify its own computer security, a South Korean military official said Friday. South Korea is one of the world's most wired countries, making it vulnerable to cyber attacks, Song Young-keun, commanding general of Seoul's Defense Security Command, was quoted as saying. 70 percent of households in South Korea have Internet access. Song said the military would also need the combined efforts of research institutions and private sector businesses to strengthen cyber security, the report added.

Category 1D1 *Organizations, cooperation for law enforcement*

2003-05-27 **UK police cyber crime victims National High Tech Crime Unit NHTCU Lyons leaks confidentialty charter report computer**

NIPC/DHS

May 27, vnunet.com — UK police provide PR help to cyber crime victims.

The UK's National High Tech Crime Unit (NHTCU) is to help handle PR for firms that have been the victims of computer crime, in an attempt to encourage more prosecutions. In December the unit launched a confidentiality charter, which allows companies to report computer crime without fear of public disclosure, but some firms are pulling out of prosecutions just before they go to court, according to John Lyons of the NHTCU. Lyons said one problem is companies fear bad publicity from prosecutions. In the event of a prosecution the unit's PR staff will work to avoid leaks and promote a positive image of companies helping the police, he said.

Category 1D1 *Organizations, cooperation for law enforcement*

2003-06-04 **hawaii cybercrime FBI office explosive growth computer crimes raud Honolulu**

NIPC/DHS

June 04, Honolulu Advertiser — Hawaii fights rising cybercrime.

The Federal Bureau of Investigation's (FBI) Hawaii office established its first cybercrime squad this year, responding to what investigators are calling "explosive growth" in computer-related crimes. Larry Futa, supervisory special agent of the Cybercrimes Squad at the FBI's Hawaii field office, said protecting the United States against cyber-based attacks and high-technology crimes is only behind fighting terrorism and espionage on the agency's list of priorities. With about 400 computer fraud complaints reported to the fraud center in 2002, Hawaii was the second highest per capita in the United States for Internet fraud complaints, second only to the District of Columbia. Futa's cyberagents work closely with the Honolulu Police Department, the attorney general's office, the Bureau of Immigrations and Customs Enforcement, the Secret Service and other federal, state and local agencies.

Category 1D1 *Organizations, cooperation for law enforcement*

2003-06-06 **cyber security government homeland cyberspace national**

NewsScan

HOMELAND SECURITY DEPARTMENT TARGETS CYBERSPACE
The Department of Homeland Security has created a National Cyber Security Division — a 60-person unit that will operate under the Department's Information Analysis and Infrastructure Protection Directorate. The new division will build on existing expertise developed at the former Critical Infrastructure Assurance Office, the National Infrastructure Protection Center, the Federal Computer Incident Response Center and the National Communications System. "Most businesses in this country are unable to segregate the cyberoperations from the physical aspects of their business because they operate interdependently. This new division will be focused on the vitally important task of protecting the nation's cyberassets so that we may best protect the nation's critical infrastructure assets," said Homeland Security Secretary Tom Ridge in a statement. (CNet News.com 6 Jun 2003)

Category 1D1 *Organizations, cooperation for law enforcement*

2003-06-06 **cybersecurity offile Tom Ridge DHS Department of Homeland Security 60 employees Critical Infrastructure Assurance Office NIPC Protection**

NIPC/DHS

June 06, Washington Post — Government creates new cybersecurity office.

The Department of Homeland Security said Friday it will establish an office to focus on U.S. cybersecurity. The National Cyber Security Division will "conduct cyberspace analysis" and issue warnings and alerts about online attacks, the department said. The division also will respond to major Internet attacks and assist in "national-level recovery efforts." Homeland Security Secretary Tom Ridge said the division will have 60 employees. Part of the new division's mission will be to coordinate the efforts of several cybersecurity offices that were folded into the Homeland Security Department this year. Among the former offices that will be put into the division are the Critical Infrastructure Assurance Office, the National Infrastructure Protection Center, the Federal Computer Incident Response Center and the National Communications System. The office will be part of the department's Information Analysis and Infrastructure Protection division.

Category 1D1 *Organizations, cooperation for law enforcement*

2003-06-14 **India fight hackers internet security centre business government establishment Carnegie Mellon IIT Information Technology**

NIPC/DHS

June 14, BBC News — India gears up to fight hackers.

India's first internet security centre is due to become operational in July. The centre will aim to prevent cyber attacks on key defense, business and government establishments. The project is being handled by the central information technology ministry with the help of the U.S.-based security group, CERT, a research and development centre run by the Carnegie Mellon University. The date for the launch of the net security centre was announced by India's Information Technology Secretary Rajiv Ratan Shah in the southern Indian city of Bangalore. Based in the capital, Delhi, the centre is expected to cost up to $20 million. A second centre will be set up in Bangalore at India's leading research organization, the Indian Institute of Science.

Category 1D1 *Organizations, cooperation for law enforcement*

2003-09-16 **global war hackers U.S. cyver-attacks DHS CERT watchdog Cyber Security national international**

NIPC/DHS

September 16, vnunet.com — U.S. Declares global war on hackers.

The increasing sophistication and speed of cyber-attacks has prompted the launch of a U.S.-led global internet monitoring service. The Department of Homeland Security will join with Carnegie Mellon University's Computer Emergency Response Team Coordination Center (Cert/CC). Dubbed US-Cert, the watchdog aims to act as a "coordination point for the prevention, protection and response to cyber-attacks across the internet." It will coordinate national and international efforts to prevent cyber-attacks, protect systems and respond to the effects of attacks across the internet. "Our nation's growing use of the internet for safety-critical applications as well as business transactions, coupled with the increased sophistication and speed of cyber-attacks, increases the risk [of] significant damage in short periods of time," said Richard Pethia, director of Cert/CC. US-Cert will begin as a partnership between Cert/CC and the National Cyber Security Division of the Department of Homeland Security.

Category 1D1 *Organizations, cooperation for law enforcement*

2003-10-18 **Internet drug sales law enforcement task force**

http://www.nytimes.com/2003/10/18/technology/18DRUG.html?th

Two federal agencies have formed a task force, Operation Gray Lord, to crack down on the growing tide of illicit sales of prescription narcotics on the Internet. FDA and DEA officers will be working with the DoJ and the RCMP in Canada to stop the illegal trade.

Category 1D1 *Organizations, cooperation for law enforcement*

2003-10-27 **Brazil cybercrime lab identity data theft attack internet violent crime police officials Sao Paulo hacker commission vandalism**

NIPC/DHS

October 27, New York Times — Brazil becomes a cybercrime lab.

Brazil is becoming a laboratory for cybercrime, with hackers specializing in identity and data theft, credit card fraud and piracy, as well as online vandalism. So far this year, nearly 96,000 overt Internet attacks—ones that are reported, validated or witnessed —have been traced to Brazil. Already overburdened in their fight to contain violent crime, police officials are finding it difficult to keep pace with hacker syndicates. The 20 officers working for the electronic crime division of the São Paulo police catch about 40 cybercrooks a month. But those criminals account for but a fraction of the "notorious and ever increasing" number of cybercrimes in São Paulo, Brazil's economic capital, said Ronaldo Tossunian, the department's deputy commissioner. The São Paulo department's effort is not helped by vague legislation dating back to 1988. Under that law, police officers cannot arrest a hacker merely for breaking into a site, or even distributing a software virus, unless they can prove the action resulted in the commission of a crime.

Category 1D1 *Organizations, cooperation for law enforcement*

2003-11-13 **security chiefs think tank prevent hackers crackers secure coding software programs better internet**

NewsScan

TOP TECH SECURITY CHIEFS FORM THINK TANK
A group of top technology luminaries is forming a new think tank that will focus on ways to elevate the status of chief security officers in the private sector — a move that they say will help significantly in the escalating battle against hackers and crackers. In addition, the Global Council of Chief Security Officers will consult with technology vendors and industry groups to help design more secure products for the next-generation Internet, and will work to encourage increased compatibility between different and competing technologies. Among the Council members are top security officials from Microsoft, Sun Microsystems, Oracle, Motorola, MCI, Washington Mutual, Bank of America, Citigroup and the New York State Office of Cyberspace Security. "Many of us have a long-term connection with the Internet and an interest in seeing it survive well into the 21st century, and there is a great deal going on that could potentially threaten its stability," says MCI's Vint Cerf, often referred to as "the father of the Internet" for his early work with Darpanet. The Council is the brainchild of former White House cybersecurity adviser Howard Schmidt, who's now the chief security officer for eBay. (Washington Post 13 Nov 2003)

Category 1D1 *Organizations, cooperation for law enforcement*

2003-11-24 **Europe EU Internet security agency crime online prevention**

NIPC/DHS

November 22, Associated Press — EU sets up Internet security agency.

The European Union (EU) governments agreed Thursday, November 20, to launch an agency to protect the Internet by alerting the public about computer viruses, identity theft and other crimes committed online. The European Network and Information Security Agency is to be operational in early 2004. It is to help governments, businesses and consumers protect their computer systems and data and inject some order in the varying approaches EU nations have taken so far to combat Internet crimes. "Trust and security are crucial components in the information society," Erkki Liikanen, the EU's information society commissioner, said in a statement.

Category 1D1 *Organizations, cooperation for law enforcement*

2003-12-17 **cyber crimes task force Ohio federal violation network attack critical infrastructure**

NIPC/DHS

December 16, Cyber Crimes Task Force of Central Ohio — Cyber task force opens in Ohio. The Central Ohio Cyber Task Force (CCTF) officially opened on on Monday, December 15. The CCTF is a joint federal task force which investigates federal violations of cyber crime in central Ohio, and is the first of its kind in Ohio. The primary crime areas the CCTF investigates and is also willing to serve as a resource for local and state law enforcement agencies are those where a computer is the primary target or tool of a criminal subject to commit any of the following: computer network attacks and intrusions, particularly for all critical infrastructure, government and the Department of Defense servers/networks and for severe commercial losses; sexual exploitation of children; Internet fraud; and intellectual property rights. The CCTF is a cooperative effort of the FBI, U.S. Department of Defense, Defense Criminal Investigative Service, the Ohio State University Police Department, City Columbus Police Department, City of Grandview Police Department, and Ohio Attorney General's Office. It is also supported by the United States Attorney's Office and Southern District of Ohio Franklin County Prosecutor's Office.

Category 1D1 *Organizations, cooperation for law enforcement*

2004-02-02 **Internet fraud scam e-mail Nigerian 4-1-9 419 caught Netherlands**

NewsScan

FINALLY! THE NIGERIAN E-MAIL SCAMMERS CAUGHT

Police in the Netherlands have arrested 52 people suspected of using the so-called "Nigerian e-mail scam" to defraud Internet users by sending them spam e-mails asking for their help in transferring a large sum of money out of Nigeria or some other troubled country in exchange for a generous percentage-fee. A task force of 80 officers raided 23 apartments, seizing computers, fake passports and 50,000 euros ($62,000) in cash. Most of those arrested were believed to be Nigerian. (Wired 2 Feb 2004)

Category 1D1 *Organizations, cooperation for law enforcement*

2004-05-17 **Homeland Security DHS information sharing federal government**

DHS IAIP Daily; http://www.govexec.com/dailyfed/0504/051404tdpm1.htm

May 17, National Journal's Technology Daily — Officials announce plan to share terrorism intelligence.

Attorney General John Ashcroft on Friday, May 14, unveiled an initiative to foster greater information sharing among federal, state and local law enforcement agencies. "No single government agency, or government, can win the war on terrorism," Ashcroft said. FBI Director Robert Mueller and Homeland Security Department Undersecretary Frank Libutti attended the announcement. Details of the National Criminal Intelligence Sharing Plan were developed at a 2002 law-enforcement summit convened by the International Association of Chiefs of Police to examine the requirements necessary for a national network that would gather, analyze and share information and intelligence on criminal and terrorist activities. On Friday, Ashcroft said the greatest structural failure in thwarting the September 11, 2001, terrorist attacks involved the "impediments to communication and information sharing among the men and women charged with keeping America safe."

Category 1D1 *Organizations, cooperation for law enforcement*

2004-06-22 **Gypsy group lawsuit IBM Nazi Holocaust assistance compensation**

NewsScan

GYPSY HOLOCAUST SURVIVORS SUING IBM IN SWISS COURT

Gypsies are suing IBM in Swiss court, alleging that IBM's expertise helped the Nazis commit mass murder more efficiently. A Gypsy group chose Geneva to file the lawsuit because IBM's wartime European headquarters were in that city. A Swiss appellate court has ruled: "IBM's complicity through material or intellectual assistance to the criminal acts of the Nazis during World War II via its Geneva office cannot be ruled out," and pointed to "a significant body of evidence indicating that the Geneva office could have been aware that it was assisting these acts." (AP/San Jose Mercury News 22 Jun 2004)

Category 1D1 *Organizations, cooperation for law enforcement*

2004-10-19 **US Department of Justice DoJ hacking intellectual property rights target five units CHIP program**

DHS IAIP Daily; http://sacramento.bizjournals.com/sacramento/stories/2004/10/18/daily15.html

October 19, Sacramento Business Journal (CA) — Justice Department to target hacking, intellectual property theft with five new units.

The United States Attorney's office in five cities will be home to new Computer Hacking and Intellectual Property units, federal officials announced Tuesday, October 19. The new units, all in areas where intellectual property is a significant contributor to the economy, will be in Sacramento, CA; Washington, D.C.; Pittsburgh, PA; Nashville, TN; and Orlando, FL. The program, known as CHIP, will target copyright and trademark violations, theft of trade secrets, unauthorized access to computers, Internet fraud and theft of computers and other high-tech items. It will also train local law enforcement officers on tech issues. The new CHIP offices join 14 existing offices around the country.

Category 1D1 *Organizations, cooperation for law enforcement*

2004-11-16 **organized cybercrime Stephen Cobb Chey Cobb DHS federal**

NewsScan;

SAFE & SOUND IN THE CYBER AGE: FEDS TO THE RESCUE?
By Stephen Cobb and Chey Cobb

Feds to the Rescue? Don't Hold Your Breath. First the bad news. If you were hoping that the threat of organized cybercrime would turn out to be something that we information security experts invented to drum up business, the time has come to stop hoping. International gangs of cyber-criminals do exist, as evidenced by the arrests announced recently by the U.S. Secret Service, which hauled in 28 people for alleged involvement in a global organized cybercrime ring (see NewsScan, 29 October 2004). According to the financial institutions victimized by this criminal enterprise, it netted more than $4.3 million. The suspects, who come from six different countries in North America and Europe, are alleged to have trafficked "in at least 1.7 million stolen credit card numbers." According to Secret Service Director W. Ralph Basham, "These suspects targeted the personal and financial information of ordinary citizens, as well as the confidential and proprietary information of companies engaged in e-commerce." According to ComputerWorld, where Mr. Basham was quoted, the suspects operated Web sites that were used to buy and sell counterfeit credit cards and false identification documents, and also share information on how to commit fraud, trade in stolen information, and operate the tools needed to commit such crimes. We realize that the world today is full of big numbers, so if $4.3 million doesn't strike you as a lot of money, bear in mind that this is just one bust of a few dozen felons. There are strong indications that hundreds, if not thousands, of criminals are getting in on the cybercrime wave. And there is little doubt that banks in the U.S. and Europe have lost several billions of dollars over the last twelve months to just one form of cybercrime: phishing (see Newsscan, 1 May 2003). A few months ago Gartner put the direct losses from phishing, that is, money fraudulently removed from people's account, at over $2.4 billion, and sources in the UK cite losses of similar magnitude. So what's the good news? We don't think there is any, despite the admirable work of the Secret Service (assisted in this case by the U.K.'s National Hi-Tech Crimes Unit, the Vancouver Police Department's Financial Crimes Section, the Royal Canadian Mounted Police and Europol). Sadly, as hard as the fine officers of these agencies work, they are hardly making a dent in the problem (see the lead story in NewsScan Daily, 20 September 2004, for more on the scale of organized cybercrime). One reason for this lack of progress is undoubtedly the lack of government investment in basic cyber security research. Given the huge negative impact of cybercrimes on both U.S. citizens and U.S. financial institutions, you might expect the federal government to be pouring money into improving computer security. Sadly, according to experts in the field, the amount of federal funding for basic cyber security research is currently less than $50 million a year (by comparison, the government recently contributed $50 million to the building a rainforest in Iowa). Some say this disturbing situation was highlighted by the October resignation of Amit Yoran after just one year as director of the National Cyber Security Division of the Department of Homeland Security. This follows two previous high profile departures from the top cyber security post in less than two years (by Howard Schmidt and Richard Clarke respectively). Observers have cited a lack of funding as a major factor in all three resignations. One person who is very much in touch with this situation is Dr. Eugene Spafford, the executive director of the Center for Education and Research in Information Assurance and Security (CERIAS). Speaking at the Information Security Decisions conference in Chicago last month, Dr. Spafford surprised the audience of 500 information security practitioners with a multiple choice question: How much do you think the federal government is spending each year on basic computer security research? The responses, quickly tabulated by a very clever electronic audience feedback system, showed that most people assumed the government was spending a lot more than it really is. Always keen to give NewsScan readers the most accurate data, Stephen asked Dr. Spafford for clarification. After all, you might recall, as we did, the Cyber Security Research and Development Act of December, 2002, in which the President authorized up to $903 million in cyber security research funds and fellowship opportunities at NSF and the National Institute of Standards and Technology (NIST), from 2003 through 2007. So how could spending be less than $50 million per year? Sadly, replied Dr. Spafford, "Authorization is not appropriation... The authorization simply says that if the money is available to NSF, they can spend it. No additional money was actually appropriated." For readers interested in learning more, a report on cybersecurity research funding is due soon from PITAC, the President¹s Information Technology Advisory Committee,. It should show up here: http://www.itrd.gov/pitac/index.html. If that report does not bear good news, you might want to contact your congresspersons, whomever they now may be. [Chey Cobb, CISSP, the author of "Network Security for Dummies," is a former senior technical security advisor to the NRO. Her email address is chey at soteira dot org. Stephen Cobb, CISSP, is the author of "Privacy for Business" and the Chief Security Executive at STSN. He can be reached as scobb at cobb dot com.]

Category 1D1 *Organizations, cooperation for law enforcement*

2004-11-17 **Europe EU IT security cybercrime agency formed**

DHS IAIP Daily; http://www.computerweekly.com/articles/article.asp?liArticle ID=135123&liArticleTypeID=1&liCategoryID=6&liChannelID=22&li FlavourID=1&sSearch=&nPage=1

November 17, ComputerWeekly — Europe's IT security agency set to fight cybercrime.

The European Union's international cybercrime squad is up and running, a year after it was given the go-ahead by the European Commission. The European Network and Information Security Agency (Enisa) has a five-year budget of $44.5M and a mandate to get member states working together to combat security threats. It aims to become a pan-European "center of excellence" on security matters, collecting and analyzing data on security incidents, advising the commission and member states on security issues, standardizing security approaches and pushing for more co-operation between the private and public sectors.

Category 1D1 *Organizations, cooperation for law enforcement*

2005-01-27 **web site child abuse UK US Australia Interpol partnership**

NewsScan; http://www.usatoday.com/tech/news/techpolicy/2005-01-27-child-abuse-site_x.htm

WEB SITE TO FIGHT CHILD ABUSE

A new Web site has been created by the U.K.'s National Crime Squad (NCS) in collaboration with the technology industry and with agencies in the U.S., Canada, and Australia, and Interpol, to provide information to help and support victims of abuse. Jim Gamble of the NCS explains: "Child abuse is one of the worst crimes to affect today's society and we in the UK must break away from thinking that we can tackle this issue within our own borders. Internet users access a worldwide service and we must tackle abuse from a worldwide perspective. That is why strategic partnerships with partners across the globe are so vital to the success of this initiative. Police across the world must work as one on this." (Federal Computer Week/USA Today 27 Jan 2005)

Category 1D1 *Organizations, cooperation for law enforcement*

2005-07-01 **music movie TV software piracy international US raids FBI warez**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4640439.stm

U.S. LEADS INTERNATIONAL PIRACY RAIDS

Authorities in 11 countries, led by the FBI, conducted raids on the operators of Internet operations suspected of pirating movies, software, and computer games. The raids, which were conducted in the United States, Canada, Israel, France, Belgium, Britain, Denmark, the Netherlands, Germany, Portugal, and Australia, led to the arrests of seven individuals, the seizure of $50 million worth of pirated material, and the shutting down of eight servers used to distribute the copyrighted works. According to U.S. Attorney General Alberto Gonzales, the raids also identified more than 120 other individuals allegedly involved in Internet piracy. Targeted in the raids were 14 so-called "warez" groups, which are the source for possibly as much as 95 percent of copyrighted material that is available online. Because operators of warez groups traditionally employ extensive measures to mask their identities and hide what they are doing, the groups have proven especially difficult for authorities to penetrate. Those arrested could face fines and jail terms, including up to 10 years in prison for distributing content prior to its commercial release. BBC, 1 July 2005

1D2 Technology for law enforcement

Category 1D2 Technology for law enforcement

1997-08-12 **e-mail tracing warrant fugitive murder investigation law enforcement**

San Jose Mercury News

The badly decomposed body of a pregnant 17 year-old girl was found in the apartment of 27 year-old Troy A. Mayo in Roseville, CA. Mayo disappeared. A month later, a relative reported receiving e-mail from the fugitive and police contacted Hotmail Corp., where the e-mail came from. Responding to the police warrant, Hotmail cooperated with the investigation and police were able to locate the specific terminal used for the e-mail at the University of California library in Berkeley. Mayo sent another e-mail from the same terminal four hours later and was captured after a brief struggle.

Category 1D2 Technology for law enforcement

2000-02-03 **wiretapping Internet standards law enforcement police government regulations opposition debate discussion decision ruling**

POLITECH, Wired http://www.wired.com/news/print/0,1294,34055,00.html

The IETF rejected proposals for including support for wiretapping in Internet standards.

Category 1D2 Technology for law enforcement

2000-02-04 **technology criminal hacker evidence encryption legal law judge ruling trial case**

New York Times
http://www.nytimes.com/library/tech/00/01/cyber/cyberlaw/28law.html

During the Mitnick trial, defense lawyers were given the contents of hard disk drives seized from laptop computers belonging to the defendant — save for the roughly 1 Gb of encrypted data for which Mitnick refused to reveal the encryption key(s), as he was fully entitled to do under the prerogatives of the Fifth Amendment of the US Constitution forbidding self-incrimination. On May 20, 1998, the federal judge, Mariana R. Pfaelzer of the Los Angeles district, agreed with prosecutors that they could keep the encrypted data from the defense team. Some legal experts disagreed with the ruling, saying that in the absence of evidence to the contrary, the encrypted data should not have been sequestered by the government side. The problem would recur, they said, as disk encryption became more widespread.

Category 1D2 Technology for law enforcement

2000-04-30 **e-mail interception monitoring government law enforcement police Internet**

Sunday Times http://www.sunday-
times.co.uk/news/pages/sti/2000/04/30/stinwenws01034.html

Reports in Britain detailed government plans to build a monitoring center capable of scanning all inbound and outbound e-mail and mobile phone calls in the UK. Plans included requirements for permanent linkages between the center and ISPs. Although a warrant would be required for examination of communications to individuals, approval for interception of corporate e-mail would be easier to obtain. The proposal for the GTAC (Government Technical Assistance Centre) raised a storm of protest from civil liberties advocates.

Category 1D2 *Technology for law enforcement*

2000-07-11 **Internet service provider ISP surveillance wiretap interception monitoring law enforcement privacy protests e-mail investigation sniffer**

NewsScan, Wall Street Journal
http://interactive.wsj.com/articles/SB963264584706292829.htm, Washington Post
http://www.washingtonpost.com/wp-dyn/articles/A15206-2000Jul20.html,
Washington Post

The Federal Bureau of Investigation is using a superfast e-mail-surveillance software system called Carnivore, so named because it can quickly ferret out "the meat" among a vast quantity of data in search of criminal or terrorist content. FBI investigators say the Internet wiretapping system has been used in fewer than 100 criminal cases since its launch last year, but privacy advocates say its deployment gives government, at least theoretically, the ability to eavesdrop on all customers' digital communications, from e-mail to online banking to Web surfing. The FBI defends Carnivore as more precise than the primitive Internet wiretap systems used in the past, and credits it with the ability to target the digital traffic of just one user amidst a stream of millions of other messages. "This is just a very specialized sniffer," says Marcus Thomas, head of the FBI's Cyber Technology Section, but Republican Congressman Bob Barr (R-Ga.) counters, "Once the software is applied to the ISP, there's no check on the system. If there's one word I would use to describe this, it would be 'frightening.'" (Wall Street Journal 11 Jul 2000)

The Republican Congressional leadership . . . [opposed] Clinton Administration plans to use its "Carnivore" software system to monitor a criminal suspect's e-mail messages as they pass through an Internet service provider. The FBI says this system is not intended to extend the government's surveillance capabilities, but merely to update their methods to cope with changing technology, but House Majority Leader Dick Armey (R-Tex.) says: "Nobody can dispute the fact that this is not legal within the context of any current wiretap law... We have a Congress that is anxious to work with [the Administration] ... but in effect they have said: 'We're going to go on our own and not wait for technology or the Congress to catch up with our desires for cyber-snooping.' That's a dangerous thing for us to allow to go along unchecked." (Washington Post 21 Jul 2000)

In testimony before a House Judiciary subcommittee, FBI official Donald M. Kerr strongly defended the agency's use of the "Carnivore" system, which effectively places a wiretap on the Internet and allows law enforcement officials to identify the origin and destination of all e-mail messages related to a person under suspicion of a crime. The reaction of Rep. Spencer Bachus (R-Ala.) was skeptical: "The potential for abuse here is tremendous. What you're saying is 'Trust us.'" But Kerr insisted that Carnivore was an essential tool for fighting crime: "Criminals use computers to send child pornography to each other using anonymous, encrypted communications. Hackers break into financial service companies' systems and steal customers' home addresses and credit-card numbers, criminals use the Internet's inexpensive and easy communications to commit large-scale fraud on victims all over the world, and terrorist bombers plan their strikes using the Internet." Civil liberties groups have been consistently critical of the FBI's support of Carnivore. (Washington Post 25 Jul 2000)

Category 1D2 *Technology for law enforcement*

2000-08-03 **privacy surveillance wiretapping interception law enforcement investigation civil liberties e-mail**

NewsScan, Washington Post http://www.washingtonpost.com/wp-dyn/articles/A25897-2000Aug2.html, San Jose Mercury News
http://www.sjmercury.com/svtech/news/breaking/merc/docs/021106.htm

U.S. District Judge James Robertson . . . ordered the Justice Department to expedite its review of requests by the American Civil Liberties Union (ACLU) and the Electronic Privacy Information Center (EPIC) for background materials on "Carnivore," a software tool developed to help the FBI carry out court-approved monitoring of suspected criminal activity on the Internet. An attorney for EPIC says, "The fact that the court is going to supervise the processing of the material is very good news. If left to their own devices, it's likely the FBI would tend to drag its feet on this, and now I think that's less likely. . . . It's going to be very difficult to have a meaningful debate about the legal issues Carnivore raises if we don't really know what Carnivore is." (Washington Post 3 Aug 2000)

Attorney General Janet Reno . . . asked the Justice Department to select a U.S. university to do an objective review of the FBI's "Carnivore" e-mail surveillance system, which scans Internet data packets as they travel to and from a criminal suspect. Civil liberties groups have been demanding that they be given all the information needed to understand how the system operates. They are not happy with Reno's decision. ACLU executive Barry Steinhardt says a university-conducted review will not be "truly independent" and adds: "The fox doesn't get to choose who guards the henhouse." (AP/USA Today 10 Aug 2000)

Category 1D2 *Technology for law enforcement*

2000-08-11 **surveillance law enforcement international jurisdiction wiretaps access foreign control national security**

NewsScan, Wall Street Journal
http://interactive.wsj.com/articles/SB965952625894025409.htm

[In July,] The Federal Bureau of Investigation . . . voiced national security concerns regarding Nippon Telegraph & Telephone's planned acquisition of U.S. Internet service provider Verio. The agency has complained in recent years that its ability to maintain surveillance over U.S. telecommunications networks could be compromised by foreign ownership deals, and this latest statement indicates those concerns are now moving into the Internet arena. FBI fears are focused on the possibility of foreign companies moving network operations offshore, which could constrict the agency's ability to physically access Internet gear to conduct wiretaps. Experts say the deal probably will be approved, but have expressed concern about the precedent it will set: "I'm confident it can be worked out, but the willingness of the government to take [its inquiry] this far and get assurances they probably don't need is not a good idea," says a lawyer specializing in telecommunications and Internet regulatory matters. (Wall Street Journal 6 Jul 2000)

[In August,] The Federal Bureau of Investigation has negotiated an agreement with Nippon Telegraph & Telephone that sets conditions for the Japanese firm's $5.5 billion purchase of U.S. Internet service provider Verio. The agreement provides a number of safeguards to protect U.S. law-enforcement investigations, including a ban on Japanese government involvement in Verio's day-to-day activities (the government still owns a sizeable stake in NTT). Critics contend that the FBI overstepped its authority in laying down conditions of the sale: "If there's a lesson learned, it's get the FBI out of these transactions, because they're extracting concessions that may be beyond what the law requires," says Albert Gidari, a Seattle lawyer who specializes in regulatory issues. (Wall Street Journal 11 Aug 2000)

Category 1D2 *Technology for law enforcement*

2000-08-17 **law enforcement surveillance civil liberties monitoring surveillance interception Internet service provider ISP**

NewsScan, San Jose Mercury News
http://www.sjmercury.com/svtech/news/breaking/merc/docs/021106.htm

Civil libertarians. . . [were] unhappy with the Justice Department's response to a Freedom of Information request that it release for scrutiny all 3,000 pages of documents describing the FBI's "Carnivore" e-mail surveillance system. Their complaint is that the proposed schedule for releasing the documents "could stretch on for many months or even years." The government says that the deliberate pace is required by the fact that commercial entities that contributed to Carnivore as government contractors need the opportunity to review and express an opinion on the disclosure of information they provided. (AP/San Jose Mercury News 17 Aug 200)

Category 1D2 *Technology for law enforcement*

2000-08-26 **fingerprint registration number keyspace rollover police law enforcement technology identity confusion duplicates synonyms collisions**

RISKS 21 02

In New York State, the fingerprint ID registration field is only 7 digits long, producing a maximum of 10,000,000 values — but the population is currently 18M and there are many historical records. The decision to begin re-using the IDs alarmed security specialists despite assurances that no one would be misidentified.

Category 1D2 *Technology for law enforcement*

2000-09-07 **law enforcement surveillance civil liberties monitoring surveillance interception Internet service provider ISP**

NewsScan

Internet pioneer Vinton Cerf told a Senate committee . . . [on 6 Sep] that he is satisfied that the FBI's use of the Carnivore e-mail monitoring system won't violate the privacy of Internet users. Cerf added that the efforts by some civil liberties groups to force the FBI to reveal Carnivore's source code are misguided. "I don't want you to misunderstand that I think this is all great," he said, agreeing that the potential for abuse is there. "I don't believe what the FBI has done is abusive. Used in the fashion described, it is very constrained in its data capture." Cerf's reservations about disclosing the source code were echoed by Judiciary Committee chairman Orrin Hatch: "ISP geeks may be less familiar with the penalties and restraints than the gentlemen from the FBI." The Justice Department has agreed to an independent review of Carnivore by a panel of academic experts it will select, but some top security experts say the conditions set for the review are tyrannical: "Independent has a new meaning in DOJ parlance," said Peter G. Neumann, principal scientist at SRI International Computer Science Laboratory. "Independent means total censorship, total control over content." (Wall Street Journal 7 Sep 2000)

Category 1D2 *Technology for law enforcement*

2000-09-19 **Internet service provider ISP surveillance wiretap interception monitoring law enforcement privacy protests e-mail investigation sniffer alternative**

NewsScan, San Jose Mercury News
http://www.sjmercury.com/svtech/news/breaking/merc/docs/054462.htm

NetICE, a software security company, has developed a free and open software product called "Altivore" as "alternative to Carnivore," the e-mail surveillance system favored by the FBI but criticized by privacy advocates. The company's chief technology officer said: "We wrote Altivore to correspond exactly to what the FBI says what Carnivore does... We founded this company in order to protect peoples' privacy. By showing the source code for Altivore, we're narrowing the debate to the true issues." Altivore can be downloaded free from the company's Web site. (AP/San Jose Mercury News 19 Sep 2000)

Category 1D2 *Technology for law enforcement*

2000-10-05 **records justice judge deletion archives discard destroy invalid inadmissible evidence e-mail communications permanent**

NewsScan, New York Times
http://.nytimes.partners.com/2000/10/05/technology/06CYBERLAW.html

District Court Judge James Rosenbaum has published an article called "In Defense of the DELETE Key," in which he bemoans the eternal nature of computer communications and reminisces fondly about pre-computer days when people casually spoke "off the record": "At this earlier time, two people could easily say something — even, perhaps, something politically incorrect — simply between themselves. They might even have exchanged nasty notes between themselves. And when they had moved past this tacky, but probably innocent moment, it was truly gone." Today, however, "an idle thought jotted onto a calendar, a tasteless joke passed to a once-trusted friend, a suggestive invitation directed at an uninterested recipient, if done electronically, will last forever. Years later, it can subject its author to liability." Rosenbaum proposes a "cyber statute of limitations" — perhaps six months for an isolated e-mail message — after which "deleted" documents would be legally consigned to the electronic rubbish heap and become inadmissible as evidence of possible wrongdoing. He makes an exception for recovered "deleted" messages from someone who has exhibited a pattern of egregious behavior or communications. The article was published in the Summer issue of The Green Bag, a literary law journal. (New York Times 5 Oct 2000)

Category 1D2 *Technology for law enforcement*

2000-10-06 **fraud lawsuit prosecution criminal fraud pornography telephone cramming theft tracking software trace IP address law enforcement**

NewsScan

The Federal Trade Commission filed a complaint in federal court . . . [Oct 2] alleging that Verity International, which is registered in Dublin and is no relation to the California software company Verity Inc., improperly charged thousands of U.S. Internet users for long-distance phone calls. The porn customers were told they were being charged to view sex videos over a phone line to Madagascar at a rate of $3.99 a minute, but the FTC determined that the calls actually terminated in the U.K. and should have cost only eight cents a minute. Verity planned to pocket the difference. The scope of the scam was huge — in a single week in September, some 67,000 U.S. households received bills from Verity, with an average overcharge of $222 (although some overcharges topped $4,000). Interestingly, the agency used an off-the-shelf software program called NeoTrace to locate the alleged perpetrators. According to NeoTrace's manufacturer, NetWorx, the software is used by the FBI, the U.S. Customs Service, NATO, the Royal Canadian Mounted Police and Interpol to trace the geographic origin of Internet traffic. (Wall Street Journal 6 Oct 2000)

Category 1D2 *Technology for law enforcement*

2000-12-07 **law enforcement investigation wiretap e-mail address law ruling debate regulations**

NewsScan, Wall Street Journal
http://interactive.wsj.com/articles/SB976146889727650215.htm

Law enforcement officials have long held that a 1986 law allowing police to record phone numbers by someone tied to a criminal investigation permits them to secretly copy e-mail addresses in messages sent to people involved in criminal probes, but a newly disclosed e-mail message suggests there is internal dissension over the legality of such "pen traps": "We have agents that would like to use a pen for e-mail, but our [chief division counsel] thinks that we can only use a pen to get the telephone number dialed by the modem," one agent wrote in the Feb. 14 e-mail. "I don't think we in the field have a grasp of how the existing telecommunications laws apply to computer communications." Highlighting the depth of confusion over the issue within law-enforcement circles, the agent noted that this legal opinion came from the FBI's National Infrastructure Protection Center, which includes the bureau's top computer-crime experts in Washington. The uncertainty brings into question the legality of using Carnivore, the FBI's e-mail "sniffing" software, which has been justified under the 1986 law that covers any device that "records or decodes electronic or other impulses, which identify the numbers dialed or otherwise transmitted" and that is attached to a telephone line. "Carnivore is not attached to a telephone line and does not obtain a number dialed," says Philip L. Gordon, a lawyer with the Privacy Foundation, who notes that privacy protections for e-mail addresses should be greater than those for phone numbers. "They're clearly different." (Wall Street Journal 7 Dec 2000)

Category 1D2 *Technology for law enforcement*

2001-07-05 **e-mail archives evidence forensic investigation law enforcement**

NewsScan

IT'S A SLOW WEEK: SHOULD YOU CLEAN OUT YOUR INBOX?
One person interviewed about his e-mail usage admitted to having 2,465 messages sitting in his inbox: "I know you can put these things in files and have them organized, but it never seems worth the trouble." Ned Kock of Temple University's e-collaboration center agrees that mailbox organization places an additional burden on busy people: "In using e-mail, you have six main tasks. You open the system. You download the messages. You read the messages. You reply. You file them. You shut off the system. We as a species are optimized for face- to-face communication, so only two of these the reading and replying are vaguely associated with that. The others are just overhead. They carry no social interest at all. There is an excitement to reading and replying, but filing takes cognitive effort without an immediate reward. So despite its being important in the long run to be organized, it is human nature to avoid it." Our conclusion? The choice is yours: follow your dream... or your nature. (New York Times 5 Jul 2001)
http://partners.nytimes.com/2001/07/05/technology/05MAIL.html

---

Category 1D2 *Technology for law enforcement*

2001-07-25 **e-mail interception Carnivore ISP filtering law enforcement investigation privacy civil liberties**

NewsScan

FBI's CATCH-22 (OR CATCH-374) NAME FOR CARNIVORE [8 Feb 2001]
The FBI's plans for its Carnivore system for "wiretapping" the Internet have been under continuous criticism from privacy advocates, and House majority leader Dick Armey of Texas has said the technology raises strong concerns that the government is "infringing on Americans' basic constitutional protection against unwarranted search and seizure." Some defenders of Carnivore, have suggested that the controversy is largely because of the catchy name chosen for the system, which was called Carnivore because it could get to the "meat" of a criminal investigation. One official said ruefully: "If they called it Device 374, nobody could remember what Device 374 was." (New York Times 8 Feb 2001)
http://partners.nytimes.com/2001/02/08/technology/08CARN.html

CARNIVORE TO GET NEW PRIVACY PROTECTIONS [19 Apr 2001]
Justice Department sources are saying that Attorney General John Ashcroft, a strong defender of individual privacy rights, will heed FBI Director Louis Freeh's advice to allow the government to continue using the Carnivore e-mail surveillance system but will require various new safeguards - such as tightening the "audit trail" to make sure the system is not being abused by law enforcement officials and developing a more precise definition of what e-mail may be inspected. (Los Angeles Times 19 Apr 2001)
http://www.latimes.com/business/cutting/todays.topstory.htm

FBI JUSTIFIES ITS INTERNET SURVEILLANCE METHODS [4 May 2001]
Documents obtained by the Associated Press under the Freedom of Information Act show that the FBI used the Carnivore or Etherpeek surveillance tools 24 times from October 1999 to August 2000 to monitor Internet e-mail and other communications traffic as part of criminal investigations of such activities as network vandalism, drug probes, extortion, and intellectual property theft. One agent wrote to a superior: "We got bank accounts, where money was hidden and other information. Some of the data sent was instrumental in tying several of the conspirators to the crime." The agent's superior told the agent that the kind of information he was providing would be "very helpful in fighting the idea that we are randomly looking at everyone's e-mail." (AP/USA Today 4 May 2001)
http://www.usatoday.com/life/cyber/tech/2001-05-04-carnivore.htm

DICK ARMEY CONTINUES OPPOSITION TO CARNIVORE
In a letter to Attorney General John Ashcroft, House majority leader Dick Armey (R-Texas) is urging the Justice Department and the FBI to consider abandoning its DCS-1000 system (popularly known as "Carnivore"), which monitors large amounts of Internet traffic in search of communications to or from the target of an investigation. Armey noted that the Supreme Court has just ruled that the police must discontinue use of thermal-imaging technology to look inside a suspect's house, and argued that the same privacy principles apply to Carnivore. (New York Times 14 Jun 2001)
http://partners.nytimes.com/2001/06/14/technology/14CARN.html

CONGRESS AGAINST CARNIVORE [25 Jul 2001]
The U.S. House of Representatives has passed a bill that would require federal law-enforcement officials to provide a detailed accounting each year of how they made use of the system known as Carnivore (renamed DCS 1000), which allows criminal investigators with a search warrant to monitor the e-mail traffic to and from a suspect's computer. The FBI would be called on to reveal which officials and which courts authorized its use, which specific laws were invoked to justify its use, and what benefits were gained from that use. (Reuters/USA Today 25 Jul 2001)
http://www.usatoday.com/life/cyber/tech/2001-07-25-carnivore.htm

---

Category 1D2 *Technology for law enforcement*

2001-09-04 **computer forensics digital evidence law enforcement police investigation**

NewsScan

BITS OF EVIDENCE
A growing number of consultants now specialize in helping law firms prepare for trail by sorting through electronic documents and e-mail messages found either on a defendant's own computer or on file server systems. Computers can identify documents by date, authors, recipients and keywords, and can frequently yield information the author thought had been erased. Attorney Michael Epstein says: "You know for a paper document, it's either there or it isn't. With e-mail, it's a little different." He provides the example of a lawsuit bought by one company against its former employees, whose denials of working for themselves on company time were refuted by evidence of their personal activities obtained by restoring files erased from the computers they had used at work. (New York Times 4 Sep 2001)
http://partners.nytimes.com/2001/09/04/technology/04DISC.html

---

Category 1D2 *Technology for law enforcement*

2001-12-05 **e-mail content filtering terrorism key word search law enforcement policy technology Carnivore denial-of-service attack false positives flooding saturation useless defeat**

RISKS 21 82

Fredric L. Rice contributed a depressing analysis to RISKS about why Carnivore and similar content-based e-mail scanning will inevitably be defeated. He pointed out that it would be trivially simple to flood the system with vast numbers of messages containing machine-generated gibberish fitting the profiles used by Carnivore to spot possible involvement in terrorism. In addition, any activist who actually did get picked up the by the FBI because ofa real e-mail could simply post the suspect e-mail on the Web, thus providing a template for yet more chaff. The author concluded, "I can't see anything coming out of the struggle besides a pile of useless software running on ISP's servers fingering innocent people and failing to point at a single bad guy."

Category 1D2 *Technology for law enforcement*

2002-01-09 **biometric face recognition I&A identification authentication failure removal law enforcement police**

RISKS 21 87

Nick Brown wrote in RISKS, ". . . [A] highly-publicised facial recognition system has been quietly dropped by law enforcement officials in Tampa, Florida, following a large number of false positives (including males identified as females, and vice versa) and a total of zero matches against known criminals, leading to zero arrests. Aside from the already-discussed civil liberties RISKs of such systems, it seems we need to add the possibility that the taxpayers may not be getting value for money, with or without their knowledge (the withdrawal of this kind of thing tends to be done with rather less media coverage than its introduction). One wonders if this will have any effect on plans to introduce such systems into airports to 'detect' terrorists."
http://www.aclu.org/issues/privacy/drawing_blank.pdf

Category 1D2 *Technology for law enforcement*

2002-01-20 **content filtering analysis lying dissimulation dishonesty untruth law enforcement investigation forensic**

NewsScan

SOFTWARE UNCOVERS E-MAIL UNTRUTHS
SAS Institute has developed software that it says can sift through e-mails and other electronic text to discern falsehoods. "The patterns in people's language change when they are uncertain or lying," says Peter Dorrington, business solutions manager at SAS. "We can compare basic patterns in words and grammatical structures versus benchmarks to detect likely lies." For instance, over-use of the word "or" and too many adjectives can be giveaways, according to Aldert Vrij's book, "Detecting Lies and Deceit." SAS says its software can also be used to detect inaccuracies in resumes and job applications. (Financial Times 20 Jan 2002)
http://news.ft.com/news/industries/internet&e-commerce

Category 1D2 *Technology for law enforcement*

2002-01-20 **computer forensics accounting fraud investigation scandal financial data**

Security Wire Digest 4 5

ENRON SCANDAL PUTS FOCUS ON FORENSICS
Computer forensics will likely play a significant role in Congress' investigation into the financial collapse of Enron, since the bankrupt energy giant's accounting firm--Arthur Andersen--admitted destroying several potentially incriminating documents--including many e-mails and computer files. Authorities believe that at least some of the destroyed documents could help explain how Andersen could have approved several off-the-books partnerships--which hid billions in Enron debt--and are at the heart of the debacle. Enron has since fired Arthur Andersen. "Computer forensics is going to be very important in this investigation," says John Patzakis, president and general counsel for Guidance Software, maker of the EnCase forensics application. "There is so much that you can learn about a system, such as how it's been used. Even if these files are completely deleted, there's still a lot of information that can be gleaned, including when the deletions occurred."

Category 1D2 *Technology for law enforcement*

2002-01-20 **wireless secure network encryption police**

Security Wire Digest 4 5

At Boston's Logan Airport, MA state troopers are successfully using secure wireless gadgets for rapid background checks. The Blackberry devices, equipped with PocketBlue software, use AES for encryption.

Category 1D2 *Technology for law enforcement*

2002-01-26 **UK legal service online Web browser litigation non-US**

RISKS; Tony Ford <tony.ford@net.ntl.com>
http://www.telegraph.co.uk/news/main.jhtml
?xml=/news/2002/01/26/nsue26.xml&sSheet=/news/2002/01/26/ixhome.html
http://www.courtservice.gov.uk/mcol/ Robin.Crorie at cheshire.pnn.police.uk

NEW OFFICIAL SELF-SERVICE LITIGATION SYSTEM AVAILABLE IN ENGLAND/WALES

UK lawyer Tony Ford discusses a report in the Daily Telegraph about a new online litigation service, "Money Claim Online," in England and Wales. Through this service ordinary citizens can contest cases online, where the amount in dispute is less than 100,000 UK pounds. Legal proceedings are conducted and judgments are passed through a Web browser. Tony Ford worries about the lack of identity authentication of the parties using this service. He is also concerned about "other gross miscarriages of justice". In response, contributor Robin Crorie points out that "Money Claim Online" is service that has actually been offered for at least two years. He notes that in both "Money Claim Online" as well as its physical analogue, there are no identity checks of the parties in contest.

Category 1D2 *Technology for law enforcement*

2002-02-20 **paper snail mail conversion e-mail law enforcement surveillance investigation privacy security confidentiality vulnerability**

NewsScan

NEW SERVICE DELIVERS PAPER MAIL ELECTRONICALLY
PaperlessPOBox offers a service that delivers 100% of your mail electronically, whether it starts out that way or not. Customers who sign up have their snail mail forwarded to an outside P.O. Box address, where it is picked up by PaperlessPOBox, scanned, and transmitted to users' e-mail accounts on the same day. The user receives exact replicas of whatever mail was sent, including hand-written notes and photos. "Personal notes translate very well," says PaperlessPOBox President David Nale. "We use state-of-the-art scanners." The service is targeted toward business travelers who have difficulty keeping up with overflowing mail boxes and received a boost last fall during the anthrax scare when people were fearful of contamination via paper mail. (Reuters 20 Feb 2002)
http://story.news.yahoo.com/news?tmpl=story&cid=581&u=/nm/20020220/tc_nm/column_nettrends_dc_14

Category 1D2 *Technology for law enforcement*

2002-02-21 **consumer profiling audit trail logging tracking music video surveillance law enforcement police investigation family parental control supervision**

NewsScan

MICROSOFT TRACKS USERS' SONGS, MOVIES
The newest version of Microsoft's MediaPlayer software, which comes free with the Windows XP operating system, is designed to create a log of the songs and movies that users play. When a CD or DVD movie is played, the MediaPlayer 8 software stores that information in a file on the user's PC, in addition to transmitting an identifier number unique to each user on the computer. That function creates the possibility that information on user habits could be tracked and sold for marketing purposes. Privacy experts say the log file could be used by investigators, lawyers, snooping family members, or companies interested in finding out an individual's personal entertainment habits. Microsoft said the program creates the log so that a user does not have to repeatedly download the same track, CD or movie information, and that the ID number was created simply to enable MediaPlayer users to have a personal account on the Web site dealing with software. The company says it has no plans to share that information with others. (AP/Miami Herald 21 Feb 2002)
http://www.miami.com/mld/miamiherald/2712422.htm

Category 1D2 *Technology for law enforcement*

2002-03-28 **terrorism homeland security confidentiality anonymity surveillance**

NewsScan

HIDING ON THE INTERNET
Terrorist groups are known to be heavy users of the Internet, so why isn't it easier to trace their whereabouts? David Lang, a computer forensics expert, explains: "The Internet presents two main challenges. One is it's ubiquitous -- you can access it from just about anywhere in the world. The other thing is you can be easily hidden." Terrorists capitalize on the first of those features by using Internet cafes and anonymous public kiosks to send mail, and exploit the second feature by making good use of encryption . One interesting fact is that terrorists don't seem to need the services of sites like Anonymizer.com that specialize in helping people send messages without revealing their identities. Lance Cottrell of Anonymizer points out the tension that exists between privacy and security: "That's kind of the irony in this. For the honest good citizen, privacy is extremely endangered and tracking is ubiquitous. But I don't see a sign that we've ever been able to build a system that criminals with serious intent haven't been able to circumvent." (New York Times 28 Mar 2002)
http://partners.nytimes.com/2002/03/28/technology/circuits/28TERR.html

---

Category 1D2 *Technology for law enforcement*

2002-05-05 **suspect profiling law enforcement police surveillance cameras artificial intelligence pattern matching signatures**

RISKS 22 05

Merlyn Kline contributed this Orwellian note to RISKS:

According to the UK broadsheet *The Independent*, Dr Sergio Velastin, of Kingston University's Digital Imaging Research Centre, has developed software to analyse CCTV images for the purpose of predicting crime:

http://news.independent.co.uk/uk/crime/story.jsp?story=287307

Quote from the article:

Scientists at Kingston University in London have developed software able to anticipate if someone is about to mug an old lady or plant a bomb at an airport. It works by examining images coming in from close circuit television cameras (CCTV) and comparing them to behaviour patterns that have already programmed into its memory. The software, called Cromatica, can then mathematically work out what is likely to happen next. And if it is likely to be a crime it can send a warning signal to a security guard or police officer.

Category 1D2 *Technology for law enforcement*

2002-05-18 **profiling database errors QA quality assurance secrecy homeland security**

RISKS 22 07

Adam Shostack contributed this thoughtful note to RISKS:

>Risks of mis-identification, arrest, etc, from law enforcement databases are well documented. The new, secret terrorism databases are starting to repeat these mistakes, as documented in a New Yorker article on a 70 year old black woman (Johnnie Thomas) is in a set of FBI databases, because "John Thomas Christopher" was an alias used by Christian Michael Longo, once on the FBI top ten most wanted list. Unfortunately for Johnnie Thomas, even the fact that Mr. Longo is in jail in Oregon hasn't removed her name from the computers, and the New Yorker article documents her (so far unsuccessful) attempts to clear her name.
http://www.newyorker.com/talk/content/?020513ta_talk_mcnamer

The application of fair information practices; allowing people to know what data is stored about them, to access and correct records, etc, is often brushed aside for law enforcement claims that the data must remain secret. Does anyone know if these databases are the the Expanded Computer Assisted Passenger Screening Program, or something else?<

Category 1D2 Technology for law enforcement

2002-06-06 **ISP Internet service provider wiretaps surveillance subpoena court order compliance**

Security Wire Digest; Findlaw Download This 4 44

VERISIGN TO LAUNCH WIRETAPPING TOOL
VeriSign Inc. on Monday [in June 2002] announced a service to help telecommunications companies comply with federal wiretap regulations and orders. The company's NetDiscovery Service, scheduled to launch by the end of June, will help carriers comply with a 1994 law requiring them to have equipment that supports content-intercept orders. . . The 1994 Communications Assistance for Law Enforcement Act requires that carriers have systems in place that allow law enforcement - with a court order - to quickly intercept phone calls and data.
http://news.findlaw.com/ap/ht/1700/6-3-2002/20020603153014_08.html

Communications Assistance for Law Enforcement Act of 1994
http://caselaw.lp.findlaw.com/casecode/uscodes/18/parts/i/chapters/119/toc.html

---

Category 1D2 Technology for law enforcement

2002-06-06 **Carnivor ISP Internet service provider e-mail traffic surveillance investigation technology wiretaps flaws court order bungled**

RISKS 22 11

The Electronic Privacy Information Center (EPIC) received information under a court order that revealed that the FBI's "Carnivore" software was misconfigured during an attempt to monitor traffic relating to Osama bin Laden. The resulting tide of unwanted information, including e-mail for unauthorized targets, so upset the FBI operative that he destroyed the entire run of data. A commentary by EPIC noted, "Since its existence became public in 2000, the Carnivore system has been criticized by EPIC and other privacy groups, as well as members of Congress, because it gives the FBI unprecedented, direct access to the data networks of Internet service providers. The FBI has publicly downplayed the system's potential for over-collection of private communications, although internal documents released earlier to EPIC confirmed such a risk. An independent review of Carnivore commissioned by the Justice Department also found that the system is capable of 'broad sweeps' and recommended technical changes to address the problem. Neither DOJ nor the FBI has indicated publicly whether those recommendations were ever implemented."

Category 1D2 Technology for law enforcement

2002-06-10 **surveillance privacy terrorism homeland security audit trail**

RISKS 22 12

The New York Times (2 Apr 2002) reported that investigators trying to determine how a New York woman had contracted Anthrax during last year's bioterrorist attack had used subway computer records and her fare card to trace her movements in the city prior to her death.

Category 1D2 Technology for law enforcement

2002-08-16 **e-mail law enforcement police surveillance investigation archives fraud**

NewsScan

PEOPLE SAY THE DARNDEST THINGS IN E-MAIL
In recent investigations e-mail is playing an increasingly pivotal role in producing criminal evidence. In the kidnapping and murder case of Wall Street Journal reporter Daniel Pearl, investigators used e-mail from his abductors to track them down, and anti-American sentiments voiced in messages from Taliban convert John Walker Lindh and shoe bomb suspect Richard Reid to their mothers were gathered as evidence against them. Closer to home, Merrill Lynch analysts indiscreetly derided stocks as a "disaster" or a "dog" in e-mail while publicly touting them to investors. "It's like the gift that keeps on giving," says a California deputy attorney general. "People are so chatty in e-mail." And e-mail seems to linger forever -- or at least until the space occupied by deleted files is overwritten with new information. "The best way to get rid of computer data is to take the hard drive and pound it with a hammer and throw it in a furnace," says the head of a forensic software company. And even that might not work -- those messages may still be stored on a corporate or ISP server, or on the recipient's computer. "E-mail has become the place where everybody loves to look," says Irwin Schwartz, president of the National Association of Criminal Defense Lawyers. (AP 15 Aug 2002)
http://apnews.excite.com/article/20020815/D7LDUU4O0.htm

Category 1D2 *Technology for law enforcement*

2002-10-01 **surveillance eavedropping analysis government**

NewsScan

NSA UPGRADES SOFTWARE FOR MONITORING INTERNET CHATTER
The National Security Agency has signed a $282-million contract with Science Applications International Corp. in San Diego for new software designed to improve the Agency's abilities to sort through millions of electronic communications sent worldwide. Richard A. Best of the Congressional Research Service explains, "There's a ton more communications out there, and how to sift through that is an increasing problem for the NSA," for which it offers "profound 'needle-in-a-haystack' challenges." (AP/San Jose Mercury News 30 Sep 2002)

Category 1D2 *Technology for law enforcement*

2002-11-05 **police law enforcement investigation text messaging alerts**

NewsScan

GERMAN POLICE USE TEXT MESSAGING TO CATCH CRIMINALS
Police in Germany are taking part in a pilot project that makes use of SMS (short messaging service) technology to enlist the help of bus and taxi drivers in apprehending criminal suspects. Police send out text messages with descriptions of the person they are seeking and, if possible, a license plate number. The concept is being tested in ten cities over the next five months, and if successful, will be expanded nationwide. "It increases the likelihood of solving a crime immediately after it has been committed," says Ulrich Kersten, president of the Federal Bureau of Criminal Investigation. (Ananova 4 Nov 2002)

Category 1D2 *Technology for law enforcement*

2002-11-25 **law enforcement police databases information linking coordination**

NewsScan

LAW & ORDER DATABASES NEED BETTER LINKING
Criminologist Peter Scharf says it took too long to share information during the hunt for the snipers in the Washington area: "If these two guys could go undetected for 23 days, what about somebody with a nuclear bomb in Manhattan? The technology systems don't connect. We have an archaic patchwork of information sharing — on the fingerprint level, on the ballistics level, on the field interrogation level." Only 34 states are directly linked to the FBI's Integrated Fingerprint Identification System database; those states are the only ones that can submit prints electronically and receive a response from the FBI within two hours if any print matches one in the bureau's files. (USA Today 24 Nov 2002)

Category 1D2 *Technology for law enforcement*

2002-12-13 **law enforcement police search investigation public cooperation advertising announcements warrants**

NewsScan

A BANNER DAY FOR FBI's MOST-WANTED BAD GUYS
The FBI's "10 Most Wanted" list has been on that agency's own Web site since 1995, but now it will get new life on pop-up banner ads on Web sites owned and operated by the Terra Lycos network. The ads are being displayed as a public service by Terra Lycos. (Computer Weekly 13 Dec 2002)

Category 1D2 *Technology for law enforcement*

2003-01-06 **surveillance cameras analysis**

NewsScan

SMARTCAMS
Surveillance technology has gone from a technology that (if the power didn't fail) produced grainy black-and-white tapes to one using solar-powered digital cameras that can send color images over digital networks to databases, which can be examined by software to identify potential problems and immediately alert security guards. Bruce Finchbaugh, a Texas Instruments researcher, describes this development as "adding new intelligence to redefine security," and Hoover Institute research fellow Nick Imearato predicts that the new technology will get cheap enough for it to "migrate to millions of businesses and even homes." But Lee Tren, an attorney at the civil liberties-focused Electronic Frontier Foundation, urges caution because "this kind of continuous recording can be very dangerous, especially if coupled with technology to recognize faces. You have to always ask what is the compelling justification for such surveillance." (San Jose Mercury News 6 Jan 2003)

Category 1D2 *Technology for law enforcement*

2003-01-13 **law enforcement databases name matching foreign spellings**

NewsScan

WHAT'S IN A NAME?
Everyone from the FBI to financial firms is struggling to keep track of an increasing number of individuals with foreign (non-European) names that may be spelled in several different ways in different databases. The issue of name-matching has become particularly acute now that the U.S. government is attempting to track visitors with a Middle Eastern background — as an example, a visit to Google produces some 50 different spellings of Mohmmar Qadaffi (or is it Muammar Gaddifi?). In response software firms are racing provide effective tools for foreign-name searches. "Last year was our best ever," says the CEO of Language Analysis Systems, which provides foreign-name searching and recognition products. While 75% of the company's business comes from the U.S. government, it's also seen increased interest from banks, airline reservation systems and data-mining companies. Language Analysis recently paired up with Basis Technology to offer the government a product called Cartouche — a name-matching system for searching and retrieving names across multiple languages. Basis CEO Carl Hoffman has urged the government to adopt Unicode-compliant systems, which would make it possible to display and process foreign names, not only as they appear in the English alphabet, but also as they appear in their native scripts. (Wired.com 13 Jan 2003)
http://www.wired.com/news/conflict/0,2100,57167,00.html

Category 1D2 *Technology for law enforcement*

2003-02-12 **security camera airport scanner privacy modesty**

NewsScan

REVOLUTION SEE-THROUGH PHOTOGRAPHY
A new astronomy technique sometimes referred to as "quasi-optics" has been used to produce a so-called "T-ray image" of a human hand taken through a 15-millimeter pad of paper. The new technology —- which allows a terahertz camera to effectively see through smoke, fog, walls, a person's clothing, etc. — is likely to revolutionize imaging in astronomy, medicine, and airport security. A future version of the terahertz camera might one day be used in space to examine the early universe. (Space.com 11 Feb 2003)

Category 1D2 *Technology for law enforcement*

2003-03-05 **Web hijacking redirection law enforcement domain seizure**

NewsScan

FEDS SEIZE DOMAIN NAMES OF ALLEGED OFFENDERS
Attorney General John Ashcroft says federal agents have taken control of several Web sites allegedly selling illegal "drug paraphernalia" and have redirected them to servers at the Drug Enforcement Administration. A federal judge in Pittsburgh ruled that the takeover was permitted until a trial can take place. Meanwhile, the DOJ also reported it has seized the iSoNews.com domain, whose owner pled guilty to using his site to sell "mod" chips that enable Xbox and PlayStation owners to modify their game consoles so they can play illegally copied games. Visitors to the iSoNews.com site yesterday were greeted with a notice stating: "The domain and Web site were surrendered to U.S. law enforcement pursuant to a federal prosecution and felony plea agreement for conspiracy to violate criminal copyright laws." The seizing of Internet domain names represents a new tactic in the DoJ's arsenal against crime, with a spokesman for the Electronic Privacy Information Center observing that the practice becomes a kind of "electronic flypaper" that raises novel legal questions. (CNet News.com 26 Feb 2003)
http://news.com.com/2100-1023-986225.html

CRIMINALS LOSING THEIR DOMAIN NAMES TO THE FEDS
In recent weeks the Justice Department has been seizing the Internet domain names they allege were used in commission of a crime, and have been continuing the operation of seized Web sites to greet visitors with stern warnings from government agencies. Civil libertarians are concerned that such seizures are depriving site owners not just of their property but of their livelihoods. They're also worried that by continuing operation of confiscated sites the government would be in a position (in the words of David Sobel of the Electronic Privacy Information Center "to monitor the Web-surfing activities of unwitting individuals who believe they are going to a Web site... but possibly implicating themselves in some law enforcement investigation." (AP/San Jose Mercury News)

Category 1D2 *Technology for law enforcement*

2003-05-01 **internet wiretaps Cisco phone calls detection products surveillance**

NewsScan

INTERNET WIRETAPS FROM CISCO
In response to concerns by law enforcement officials that criminals can use Internet telephony to avoid court-approved wiretaps, Cisco Systems has developed a way for police to monitor Internet-based phone calls without detection. The company says it is building the capabilities into a limited number of its new products, though none have been sold as yet. The monitoring service includes an auditing mechanism by a third-party provider, in order to ensure that the surveillance complies with all laws governing interception of communication. (AP/USA Today 1 May 2003)

Category 1D2 *Technology for law enforcement*

2003-05-30 **log file virtual operating system replay attack digital forensics recovery computer crime**

NewsFactor Network
http://science.newsfactor.com/story.xhtml?story_title=Virtual_Time_Machine_May_Foil_Hackers&story_id=21642#story-start

Prof. Peter Chen of the University of Michigan has proposed using a virtual machine called ReVirt to log all significant events to disk, permitting not only reversion to any given point in time, but also replay of the events in a computer attack. Chen estimates that a 100GB hard disk could easily store several months worth of log files with minimal overhead. Chen and his colleagues published an article with the following abstract <
http://portal.acm.org/citation.cfm?id=844148&jmp=citings&coll=GUIDE&dl=ACM > :

Current system loggers have two problems: they depend on the integrity of the operating system being logged, and they do not save sufficient information to replay and analyze attacks that include any non-deterministic events. ReVirt removes the dependency on the target operating system by moving it into a virtual machine and logging below the virtual machine. This allows ReVirt to replay the system's execution before, during, and after an intruder compromises the system, even if the intruder replaces the target operating system. ReVirt logs enough information to replay a long-term execution of the virtual machine instruction-by-instruction. This enables it to provide arbitrarily detailed observations about what transpired on the system, even in the presence of non-deterministic attacks and executions. ReVirt adds reasonable time and space overhead. Overheads due to virtualization are imperceptible for interactive use and CPU-bound workloads, and 13—58% for kernel-intensive workloads. Logging adds 0—8% overhead, and logging traffic for our workloads can be stored on a single disk for several months.

For another summary of the system, see Kim Roth's article, "Virtual Replay" in the _Michigan Engineer_ [Fall/Winter 2003] at < http://www.engin.umich.edu/alumni/engineer/03FW/feature/ >.

Category 1D2 *Technology for law enforcement*

2003-06-04 **research NSA National Security Agency supercomputing problems computational analyze intelligence data Perntagon aircraft ships nuclear**

NIPC/DHS

June 04, National Journal — Security officials urge more research into supercomputing.

The nation's investment in supercomputing research and development has played a crucial role in national security, but more investment is needed to resolve numerous computational problems, a key National Security Agency (NSA) official said on Wednesday. George Cotter, chief of NSA's Office of Corporate Assessments, told attendees of an Army High-Performance Computing Research Center luncheon that the conclusion of a congressionally mandated study on high-end computing R&D determined a need for faster computing to enable the military to create better weapons, aircraft and ships, as well as to improve the nation's ability to monitor its nuclear-weapons stockpile. Faster computers also are needed to analyze intelligence data and build better mapping capabilities for the military, he said. The center has received $4 million in research funding annually over the past two years from the Army as the Pentagon decided to increase its focus on using supercomputing for military purposes. The program was initiated in 1990.

Category 1D2 *Technology for law enforcement*

2003-08-22 **crime fight computer database check fraud**

NewsScan

DATABASE TO FIGHT FINANCIAL CRIME

Banks throughout the Midwest U.S. can make use of a computer database called FinCrime that allows financial institutions and law enforcement to share information about crimes and provide warnings. Once check fraud or some other financial crime is committed, bankers and law enforcement personnel can enter information about the crime and the suspect into the database. FinCrime looks for matching information. "Obviously the more participants we have, the more data we can gather in this electronic database, the more valuable it's going to be for participants," said John Sorensen, president and chief executive of the Iowa Bankers Association. "We're trying to expand it widely and keep the cost of participation at either nothing or very small costs... One of the unique things about our network is that it's going to be owned by state banking associations and that it will be provided really as a service as members of these state banking associations," Sorensen said. (AP/USA Today 22 Aug 2003)

Category 1D2 *Technology for law enforcement*

2004-01-30 **electronic cyber crime evidence destruction police business practice investigation United Kingdom UK**

RISKS 23 17

UK: VITAL E-CRIME EVIDENCE OFTEN DESTROYED

Contributor Keith A. Rhodes presents an article from vnunet.com. The article states that some companies in the UK maybe destroying digital evidence on their systems while investigating cyber crimes before ringing for law enforcement help. The article reports that Len Hynds, the Detective Chief Superintendent of the National High Tech Crime Unit (NHTCU) said that there was a need to "…develop common standards in terms of dealing with high-tech crime between the private and public sectors." Michael Colao, a consultant, said: "What we see is well-meaning IT professionals going in and doing what you see on every bad crime film: they muddy the waters… You need a professional computer forensic team in there as soon as possible."

Category 1D2 *Technology for law enforcement*

2004-03-01 **forensics police lab video separation manipulation**

NewsScan

FORENSIC VIDEO

In Allegheny County, Pennsylvania, a police forensics lab is able to separate individual feeds from dozens of cameras that record on the same tape or disc and can stabilize images from shaky cameras and adjust the brightness and contrast. The techniques are similar to ones used by authorities in Florida to examine videotape from a car wash in Sarasota and help track down a man accused of abducting and killing an 11-year-old girl. But one of the officers in the Allegheny County lab cautions: "This is not a magic wand. There's a lot we can do with video and digital images, but there are still limitations." For example, although a surveillance camera outside a Pittsburgh job center captured the perpetration of a murder, police were unable to enhance the images enough to get a clear picture of the killer, causing one of the police offers to complain: "Frustrating isn't the word. You can see some facial features, his shoes, his distinct clothing, but it's just not enough." (AP/USA Today 1 Mar 2004)

Category 1D2 *Technology for law enforcement*

2004-04-01 **Massachusetts open-standards open-source IT contract**

DHS IAIP Daily; http://www.govtech.net/news/news.php?id=89839

April 01, Government Technology — Massachusetts awards first open-standards IT contract.

This week the state of Massachusetts acquired its first information technology (IT) services under its new open-standards policy. The Executive Department Legal Counsel's Virtual Law Office (VLO) will be developed using open-standards and open-source components. Similar to systems utilized by large private law firms, the VLO will deliver sophisticated content management, legal case management and new reporting tools. The contract award is expected to result in savings to the state both through more efficient management of legal services and outright ownership of the software code. Typically, state government would pay initial and ongoing licensing fees for new software. "The new open-standards policy is resulting in fair and open competition," said Administration and Finance Secretary Eric Kriss. "Out of the gate, this policy is having a positive impact on the state's bottom line."

Category 1D2 *Technology for law enforcement*

2004-05-03 **database law enforcement pharmaceutical FDA**

DHS IAIP Daily; http://www.news−medical.net/view_article.asp?id=1185

May 03, inpharma.com — Database to help identify counterfeit pharmaceuticals.

The Food and Drug Administration (FDA) is planning to create a database of the major pharmaceutical brands on the U.S. market, to make it easier to establish the authenticity of suspect products and identify counterfeit versions that enter the supply chain. The agency's Cincinnati-based Forensic Chemistry Centre (FCC) will establish a Counterfeit Analysis Work Group that will compile and maintain the database, which will contain frequently-updated information on both authentic brands and counterfeit versions of drugs. The group will put together a checklist that will be sent to all pharmaceutical companies selling products in the U.S., requiring them to provide the FCC with certain information about their brands to help ensure their authenticity. It will also create a database of authentic dosage forms for drugs. According to World Health Organization estimates, counterfeit medicines comprise six percent of the world market.

Category 1D2 *Technology for law enforcement*

2004-05-24 **wireless law enforcement automated dispatch**

DHS IAIP Daily; http://www.fcw.com/geb/articles/2004/0524/web−texwire−05 −24− 04.asp

May 24, Federal Computer Week — Wireless to help Garland police.

The Garland, TX, police department will be the first local users of a new wireless network for first responders that is able to transmit voice and data at least 20 times faster than the city's old network. The deployment of the network will start with the city's 290 police officers, including the mobile data terminals in 80 squad cars. City officials are starting with data on the new network, using it as part of the Computer Automated Dispatch system to transmit 911 calls, alarms, report management, graphics and mug shots to the mobile units, said Darrell McClanahan, Garland's telecommunications manager. "This is an important milestone in fulfilling our city's communications vision for a fully converged high-speed data, voice and video network over which police, fire, emergency medical personnel and, eventually, all city employees will be interconnected in real time," McClanahan said.

Category 1D2 *Technology for law enforcement*

2004-06-23 **law enforcement WiFi technology sting operations chat rooms pedophiles**

NewsScan

MOBILE WIRELESS USED IN STING OPERATION

Law enforcement authorities in Texas have begun using a van equipped with high-speed wireless satellite devices to catch Internet surfers using chat rooms to set up illegal liaisons with underage girls. In the first sting operation in which the van has been used, seven men were apprehended
and charged with various felonious acts. A chief investigator in the Texas attorney general's office says, "In many of our rural areas, they lack the infrastructure we need to support this kind of investigation. So we now have the technology and ability to bring it with us. It's self-contained and
we're ready to go." (AP/USA Today 23 Jun 2004)

Category 1D2 *Technology for law enforcement*

2004-07-12 **Global Positioning System GPS Tennessee paroled offender tracking surveillance privacy freedom law enforcement technology**

NewsScan

TENNESSEE GPS SYSTEM WILL TRACK PAROLED OFFENDERS

Tennessee has budgeted $2.5 million for a pilot project that will test a global positioning system (GPS) for keeping track of paroled rapists. The system would let law enforcement build maps with "zones of exclusion" for the offenders (such as playgrounds, schools, day-care centers or the homes
of victims), and would allow probation officers to determine whether the felons they are supervising are going to work during the day, going home at night, and staying away from restricted areas. (The Tennessean 12 Jul 2004)

Category 1D2 Technology for law enforcement

2004-10-18 **privacy identification printers**

NewsScan; http://news.bbc.co.uk/2/hi/technology/3753886.stm

EACH PRINTER CARRIES UNIQUE SIGNATURE

It turns out that every printer leaves a unique "intrinsic signature" on all the documents it produces, enabling law enforcement officials to track down printers used to make bogus bank notes, fake passports or other important documents. In a test, a research team from Purdue University was able to identify the correct printer more than 90% of the time. The signature derives from the way different printers lay down ink in distinct bands that can be spotted by image processing software. "We extract mathematical features, or measurements, from printed letters, then we use image analysis and pattern-recognition techniques to identify the printer," says Purdue professor Edward Delp. The research has been focused on identifying laserjet signatures, but the researchers are now turning their attention to inkjet printers as well.

Category 1D2 Technology for law enforcement

2004-11-23 **authentication artwork counterfeit law enforcement**

NewsScan;
http://www.cbc.ca/story/arts/national/2004/11/23/Arts/artcomputer041123.html

COMPUTER AUTHENTICATION OF ARTWORKS

Computer scientists at Dartmouth College have developed a new mathematical process of authenticating art using high-resolution digital photos and complex computer analyses to map out the idiosyncrasies of an artist's unique pen and brush stokes for comparison with other artworks. The process replicated the work of human authenticators when it was used to analyze works by artists Pieter Bruegel the Elder and Perugino. Dartmouth professor Hany Farid, co-director of the project, says: "What we've tried to do is capture certain mathematical properties of an artist in terms of their underlying style, properties almost certainly not visible to human eyes." But he emphasizes that the process is meant to be an additional tool, and not a replacement for the traditional means of authenticating artworks: "It's simply another tool that is contributing to the dialogue of art authenticating." (CBC News 23 Nov 2004)

Category 1D2 Technology for law enforcement

2004-12-04 **US intelligence search engine Convera homeland security data mining**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A30161-2004Dec2.html

THE SEARCH SOFTWARE USED BY THE IN-CROWD

Analysts working for U.S. intelligence and other federal agencies looking for documents and data stored on computers inside their own agencies they use software made by the Convera Corp. in Virginia, which offers specialized services and offer such features as the ability to automatically notify intelligence analysts when a new document matching a search query is added to the agency's database, and to search for patterns within data, identifying relationships buried in mountains of separate documents. Helen Mitchell, head of enterprise search for the FDA, says: "Before, people couldn't find everything if things were misfiled or they didn't have the time or resources. With the Convera software, and the technology for searching documents and patterns, they can find documents even with misspellings." Convera plans to make its Internet search engine available to regular computer users for free sometime next year. (Washington Post 4 Dec 2004)

Category 1D2 Technology for law enforcement

2004-12-05 **cyber detectives DePaul University Chicago computer scientists pattern-recognition algorithm software crime detection neural network link CSSCP**

DHS IAIP Daily; http://www.newscientist.com/news/news.jsp?id=ns99996734

December 05, New Scientist — Cyber detective links up crimes.

Computer scientists Tom Muscarello and Kamal Dahbur at DePaul University in Chicago have developed an artificial intelligence system that uses pattern-recognition software to link related crimes that may have taken place in widely separated areas whose police forces may rarely be in close contact. Called the Classification System for Serial Criminal Patterns (CSSCP), the system sifts through all the case records available to it, assigning numerical values to different aspects of each crime, such as the kind of offense, the perpetrator's sex, height and age, and the type of weapon or getaway vehicle used. From these figures it builds a crime description profile. A neural network program then uses this to seek out crimes with similar profiles. If it finds a possible link between two crimes, CSSCP compares when and where they took place to find out whether the same criminals would have had enough time to travel from one crime scene to the other. In the UK an online version of a manually searchable crime database called Crimelink was launched this week.

Category 1D2 *Technology for law enforcement*

2004-12-07 **border checkpoints screening US photos scanning finger biometrics criminal databases**

NewsScan; http://www.usatoday.com/tech/news/2004-12-07-border-print-program_x.htm

ZIPPING THROUGH BORDER CHECKPOINTS

Foreigners entering the U.S. at some border crossings are now being processed by a new digital screening program that quickly scans photos of the traveler's face and index finger and matches them against federal agencies' criminal databases. Vistor Adolfo Moroyoqui Felix, traveling between Mexico and Phoenix, says: "It's much faster this way. They had to fill out paperwork before. It's more effective this way." Other travelers seem to agree. (AP/USA Today 7 Dec 2004)

Category 1D2 *Technology for law enforcement*

2004-12-12 **data mining law enforcement research money laundering fraud financial crime**

NYT http://www.nytimes.com/2004/12/12/politics/12finance.html

DHS ICE STUDIES DATA MINING TOOL

According to Eric Lichtblau, writing for the New York Times in December 2004, DHS (Department of Homeland Security) reported that the ICE (Immigration and Customs Enforcement) is studying a British database and program for data mining in financial transactions. The database from World-Check tracks a variety of financial crimes based on open-source information including 140,000 public sources; it already has information about roughly "250,000 people and firms with suspected ties to terrorist financing, drug trafficking, money laundering and other financial crimes."

Category 1D2 *Technology for law enforcement*

2004-12-16 **law enforcement Alabama tickets**

NewsScan; http://apnews.excite.com/article/20041217/D8713ISO0.html

STATE TROOPERS ISSUING ELECTRONIC TICKETS

Well, it certainly cuts down on paperwork -- 50 Alabama state trooper vehicles are already equipped with laptops, scanners and printers that enable them to issue traffic tickets electronically and zap them directly to county courthouses rather than deliver them in person. Within two years, the state hopes to have the equipment in all 325 patrol cars, says state Public Safety Director Mike Coppage. Once e-citations are in use statewide, the next goal is to allow state troopers file accident investigation reports electronically and to enable them to access criminal records from their vehicles. (AP 16 Dec 2004)

Category 1D2 *Technology for law enforcement*

2005-01-13 **FBI failure virtual case file information sharing homeland security quality assurance features SAIC debacle fiasco**

NewsScan; http://www.latimes.com/technology/la-na-fbi13jan13

SECURITY IV: NEW FBI SOFTWARE NOT USABLE

A new FBI computer system called Virtual Case File, designed to help agents share information to ward off terrorist attacks, may have to be discarded because it doesn't work as designed. The agency will be soliciting proposals for new software from outside contractors for new software. Sen. Judd Gregg (R-N.H.), chairman of the Senate appropriations subcommittee, calls the development "a stunning reversal of progress" and adds: "If the software has failed, that sets us back a long way. This has been a fits-and-starts exercise, and a very expensive one for a very long time. There are very serious questions about whether the FBI is able to keep up with the expanding responsibility and the amount of new dollars that are flowing into it. We have fully funded it at its requested levels." Science Applications, the company that developed the system, says it "successfully completed" delivery of the initial version of the Virtual Case File software last month. (Los Angeles Times 13 Jan 2005)

Category 1D2 *Technology for law enforcement*

2005-01-14 **GPS law legal tracking privacy**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A10788-2005Jan14.html

GPS EVERYWHERE

The rules about the use of GPS devices are widely varied: whereas a federal judge in New York has ruled that police have a right to place tracking devices on vehicles without a warrant (since the drivers should have no expectation of privacy on public roads), California has restricted car rental companies' use of GPS to track customers (a law adopted after a company fined customers $3,000 because their GPS system indicated the cars had crossed the state line into Nevada in violation of the rental agreement). But the fact is that GPS is here to stay: David Gilmore, the courtappointed transportation administrator for D.C. Public Schools, says of the use of GPS to monitor school bus drivers in that jurisdiction: "As uncomfortable as this might make them, they are now being watched by satellite every minute of their workday, like it or not." (Washington Post 14 Jan 2005)

Category 1D2 *Technology for law enforcement*

2005-01-18 **FBI Carnivore eavesdrop**

NewsScan; http://apnews.excite.com/article/20050119/D87MS3CO0.html

FBI AXES CARNIVORE, EATS INVESTMENT

The FBI has abandoned its custom-built Internet surveillance technology, dubbed Carnivore, and is now using commercial software to eavesdrop on computer network traffic during investigations of suspected criminals, terrorists and spies. In addition, it's asking Internet service providers to conducting wiretaps on targeted customers, when necessary. Carnivore initially was developed because commercial tools available in 2000 were inadequate, but FBI spokesman Paul Bresson says the Bureau moved a while ago to using popular commercial wiretap software because it's less expensive and has improved in its ability to copy e-mails to and from a specific Internet account without affecting other subscribers. "We see the value in the commercially available software; we're using it more now and we're asking the Internet service providers that have the capabilities to collect data in compliance with court orders," says Bresson. The FBI didn't disclose how much it had spent on Carnivore, but outside experts estimate expenditures at somewhere between $6 million and $15 million. (AP 18 Jan 2005)

Category 1D2 *Technology for law enforcement*

2005-01-20 **Arabic language linguistics scanning OCR software terrorism antiterrorism information gathering University of Buffalo grant**

DHS IAIP Daily; http://www.usatoday.com/tech/products/software/2005−01−20−ar abic−scans_x.htm

SOFTWARE WOULD SCAN ARABIC DOCUMENTS FOR INFORMATION

Computer scientists are at work on software to scan Arabic documents, even handwritten ones, for specific words or phrases, technology its developers say could aid in intelligence gathering. Researchers at the University of Buffalo have received $240,000 in funding from the federal Director of Central Intelligence Postdocotoral Research Fellowship Program. Optical character recognition (OCR) software trains the computer to interpret the images of an alphabet based on scanned images of characters or words recorded by humans who have examined the original images. Arabic presents challenges because characters may take different forms depending on where within a word they appear, and Arabic vowels are pronounced but often not written.

Category 1D2 *Technology for law enforcement*

2005-06-02 **DHS national defense terrorism anti-terrorism University of Buffalo browser technology concepts ideas information correlation**

EDUPAGE; http://news.com.com/2100-1012_3-5730176.html

UNIVERSITY RESEARCHERS DEVELOPING BROWSER TO FIGHT TERRORISM

Researchers at the University of Buffalo (UB) are developing browser technology that endeavors to identify hidden connections in vast collections of documents. Rather than simply looking for matches to specified query terms, which is what typical search engines do, the UB technology seeks to uncover connections between ideas. According to John McCarthy, professor emeritus of computer science at Stanford University, a tool that successfully links concepts could be an important breakthrough. A number of federal agencies, including the Federal Aviation Administration (FAA), are investing in the research, which they hope can be used to find the sorts of connections that will aid efforts to fight terrorism. The project has been used to search the report from the 9/11 Commission as well as public Web pages, looking for connections regarding the hijackers. The tool searches for concepts such as names, dates, and places and maps the connections it finds, potentially resulting in trails of evidence useful to investigators or other authorities. CNET, 2 June 2005

Category 1D2 *Technology for law enforcement*

2005-07-04 **Air Force ultrawideband Sandia National Laboratories UWB radio encryption network military ultrawideband spectrum**

DHS IAIP Daily; http://www.eetimes.com/news/latest/technology/showArticle.jhtml?articleID=165600118

U.S. AIR FORCE TAPS SECURE ULTRAWIDEBAND

Sandia National Laboratories has combined ultrawideband (UWB) radio signals with advanced encryption techniques to develop a secure sensor and communications network for the U.S. military. The ultrasecure UWB communication system promises to help the government protect its troops on the battlefield by detecting the position of enemies and by making it much harder for them eavesdrop or jam military communications. "By utilizing the immense spectrum of UWB to spread the energy of communications signals from sensors over a wide frequency spectrum, the signal power falls below the noise floor of normal receivers," said Sandia National Laboratories researcher Timothy Cooley. Also known as "impulse radio," ultrawideband radio transmissions smear a wide spectrum with short, 100-picosecond pulses that are below the noise floor of conventional radio receivers. Even if enemies were equipped with a special UWB receiver, they would be unlikely to know how to reassemble the disparate data packets of each impulse into a coherent whole. And even if they should manage to reassemble the packets, they would still have to crack the 256-bit AES encryption used by Sandia's special secure military communications version. The sensor and communications networks are being developed for the U.S. Air Force Electronic Systems Center.

Category 1D2 *Technology for law enforcement*

2005-07-10 **UK police pictures e-mail records hunt phones video networks'**

DHS IAIP Daily; http://www.theregister.co.uk/2005/07/10/london_bomb_

UK POLICE REQUEST PICTURES, E-MAIL, PHONE RECORDS IN BOMBER HUNT

London police have asked the public to turn in pictures from mobile phones and video pictures as they hunt the terrorists behind the bomb attacks on the UK capital Thursday, July 7. The call came as Britain's authorities sought to secure email and mobile phone records as they continue their hunt for the bombers. Much of the media networks' coverage of the bombings came from stills and video captured on camera phones and other mobile devices. London's Metropolitan Police on Sunday asked people who captured images on Thursday, both before and after the bombings, and either in or close to the areas where the bombings happened, to forward them to images@met.police.uk. "These images may contain crucial information which could help detectives in what is a painstaking and complex inquiry," said the head of the Met's Anti-Terrorist Branch, Deputy Assistant Commissioner Peter Clarke.

Category 1D2 *Technology for law enforcement*

2005-07-22 **UK Britain terrorist Website control database**

EDUPAGE; http://news.zdnet.com/2100-1009_22-5798787.html

BRITAIN TO TRACK, CONTROL TERRORIST WEB SITES

Following recent terrorist attacks on London's public transit system, the British government announced plans to tighten oversight on people who run Web sites inciting terrorism. In speaking to Parliament on July 20, Home Secretary Charles Clarke acknowledged that the government would have to "tread carefully" around free speech in instituting changes to the national security policies. Clarke said he intends to draw up a list of unacceptable behaviors, such as preaching, running Web sites, or writing articles intended to provoke terrorism. The Foreign and Commonwealth Office and intelligence agencies will be instructed to build a database of people who provoke terrorism. Immigration officers will have access to the database, and the government is planning changes to the law to make it easier to deport religious extremists whose behaviors meet the revised policies. ZDNet, 22 July 2005

Category 1D2 *Technology for law enforcement*

2005-10-15 **software engineering quality assurance QA new system introduction training denial of service DoS interface public relations**

RISKS; http://archiv.tagesspiegel.de/archiv/13.10.2005/2112250.asp (in German) 24 08

NEW GERMAN REGISTRATION SYSTEM CAUSES CHAOS

…[T]he [German federal] registration offices bought themselves some brand-spanking-new software. All people living in Germany must register their address and the names of people who live with them with this office (which is part of the police jurisdiction) inside of a week of moving into town. The police use the data for all sorts of purposes.

They cut over to the new system October 4, and the police suddenly discovered that they were offline - their systems did not work anymore, probably because the API was different. The police had to set up emergency computers directly linked to the official system and have police officers in the field *call in* their requests. Result: the line is always busy. But of course, there is no threat to the general public, just nasty waiting for the police….

The registration office was pointing the finger at the police, saying they had known for a year that this was coming. Then people called the papers complaining that waiting times at the office - which also issues passports and ID cards and the like - had gone from an hour to FOUR hours.

The official excuse is that clerks were not sufficiently trained in the use of the 23 million Euro software called "Meso". And they insist that the waiting time is "only" doubled, not more. They request the good taxpayers who paid for the software to just stay home and not bother them until they get the kinks worked out - really, one office gave out a press release to just leave them alone!

An added problem is that many people are trying to apply for new passports because from December on people have to pay more for them because they have to have RFID chips with biometric data stored in them so that the US government is appeased and will still let Germans in without visas…..

[Report by Debora Weber-Wulff]

Category 1D2 *Technology for law enforcement*

2005-11-30 **study wiretap telephone wiretapping interception evasion security flaw privacy government agencies FBI legal ramifications**

DHS IAIP Daily; http://www.nytimes.com/2005/11/30/national/30tap.html

SECURITY FLAW ALLOWS WIRETAPS TO BE EVADED, STUDY FINDS

The technology used for decades by law enforcement agents to wiretap telephones has a security flaw that allows the person being wiretapped to stop the recorder remotely, according to research by computer security experts who studied the system. It is also possible to falsify the numbers dialed, they said. Someone being wiretapped can easily employ these countermeasures with off-the-shelf equipment, said the lead researcher, Matt Blaze, an associate professor of computer and information science at the University of Pennsylvania. "This has implications not only for the accuracy of the intelligence that can be obtained from these taps, but also for the acceptability and weight of legal evidence derived from it," Blaze and his colleagues wrote in a paper that was published Wednesday, November 30, in Security & Privacy, a journal of the Institute of Electrical and Electronics Engineers. To defeat wiretapping systems, the target need only send the same "idle signal" that the tapping equipment sends to the recorder when the telephone is not in use. The target could continue to have a conversation while sending the forged signal. Despite this, the FBI says the vulnerability exists in only about 10 percent of state and federal wiretaps today. "Signaling Vulnerabilities in Wiretapping Systems" by Blaze, et al: http://www.crypto.com/papers/wiretapping/

1D3 Litigation, legal rulings, judgements affecting law enforcement

Category 1D3 *Litigation, legal rulings, judgements affecting law enforcement*

1999-11-19 **criminal hacker attitude stance belief antivirus malicious code definitions criteria keystroke logger monitor**

HackCanada

Someone calling itself "Renderman" at HackCanada raised a legitimate question about the criteria used to define software as malicious by anti-virus product developers. This issue was the subject in early 1999 of a working group at the European Institute for Computer Anti-Virus Research (EICAR), which concluded that trying to integrate the motivation behind a program was a hopeless basis for defining malware.

Category 1D3 *Litigation, legal rulings, judgements affecting law enforcement*

2000-01-14 **privacy law evidence wiretapping**

NewsScan, New York Times
http://www.nytimes.com/library/tech/00/01/cyber/cyberlaw/14law.html

In Spokane County (Washington) Superior Court, the defense in a rape and child porn trial argued that the state's privacy laws precluded law-enforcement use of captured e-mail and chat-room messages. However, Superior Court Judge Kathleen M. O'Connor denied the motion, stating that the law does not specifically include computers as a protected medium.

Category 1D3 *Litigation, legal rulings, judgements affecting law enforcement*

2000-02-18 **wiretapping telecommunication criminal hacking phreaking**

The Times (London)

In England, the House of Lords ruled in favor of Stephen Alan Morgans, who appealed a conviction based in part on log files printed out from a device placed on the defendant's telephone line. The printouts showed that Mr Morgans had accessed phone company computers and fraudulently obtained phone services. Unfortunately, police had failed to obtain a warrant from the office of the Secretary of State. The Lords threw out the conviction on the grounds that the intercepts were illegal.

Category 1D3 *Litigation, legal rulings, judgements affecting law enforcement*

2000-07-07 **law enforcement court case judgement entrapment investigation Internet e-mail**

NewsScan, New York Times
http://partners.nytimes.com/library/tech/00/07/cyber/cyberlaw/07law.html

COURT RULES AGAINST POLICE IN INTERNET "ENTRAPMENT" CASE
A majority of a three-judge U.S. appellate court panel . . . ruled against the use of the Internet to entrap an individual into committing sex offenses. After being divorced by his wife because he could not control his compulsion to cross-dress, the individual in question began to use the Internet to search for a woman who would accommodate his sexual tastes. He entered into correspondence with someone called Sharon, who tuned out to be an undercover police investigator, who suggested the idea of having sex acts with her children. The man was arrested when he showed up at a meeting place to carry out the plan. The court ruled: "Prior to his unfortunate encounter with Sharon, [the man charged for attempting to have sex with minors] was on a quest for an adult relationship with a woman who would understand and accept his proclivities, which did not include sex with children. There is surely enough real crime in our society that it is unnecessary for our law enforcement officials to spend months luring an obviously lonely and confused individual to cross the line between fantasy and criminality." (New York Times 7 Jul 2000)

Category 1D3 *Litigation, legal rulings, judgements affecting law enforcement*

2001-02-20 **surveillance technology privacy search seizure constitution law enforcement**

NewsScan

TECHNOLOGY TESTS THE BOUNDARIES OF YOUR HOME The Constitution's Fourth Amendment protecting citizens against unwarranted search and seizure will be debated this week in the U.S. Supreme Court, which is considering a case in which police used a thermal scan of a private house to determine if excessive heat from the building suggested that it was being used to grow marijuana under high-intensity lights. An ACLU executive protests that "if the government is free to use technology inside our homes, there really won't be anything left of the right to privacy," and an attorney for the man whose house was targeted argues: "Since we don't permit police to break into people's homes, should we permit them to use technology to accomplish the same thing?" The police, however, justify the thermal scan as no different in principle from having an officer watching a house from the outside. (AP/USA Today 19 Feb 2001)
http://www.usatoday.com/life/cyber/tech/review/2001-02-19-thermal.htm

---

Category 1D3 *Litigation, legal rulings, judgements affecting law enforcement*

2001-05-03 **monitoring legal roadblocks prevention government interference auditing criminal hackers honeypot warrant**

NIPC Daily Report

A late-term change in the Clinton administration's approach to prosecuting cybercrime has made it much more difficult for NASA to track and prosecute hackers who attempt to penetrate its computer networks, a NASA network-protection office official said 30 April. "NASA lost 90% of its ability to track and pursue (suspected computer) intruders because of changes in policy" by the Justice Department, according to a director from NASA's network and advanced technologies protection office. Apparently, over the last year-and-a-half, the Justice Department's Computer Crime and Intellectual Property section began prohibiting federal agencies from electronically monitoring the actions of hackers who break into their systems. Under federal wiretapping statutes, system administrators of private computer networks may do such monitoring, but law enforcement officials are normally prohibited from doing so without a warrant. (Infosec News, 3 May)

Category 1D3 *Litigation, legal rulings, judgements affecting law enforcement*

2001-12-12 **encryption organized crime police law enforcement investigation keystroke logging surveillance data capture password wiretap virus logger Magic Lantern**

NewsScan

ENCRYPTION AND ORGANIZED CRIME [30 Jul 2001]
When Phil Zimmerman created the encryption software known as PGP ("Pretty Good Privacy") he knew that his program would be used not only by honest citizens but also by criminals, and he says "I felt bad about that," but notes that "the fact that criminals use cars doesn't mean that the rest of us shouldn't have cars." Criminal use of PGP is now being examined in a federal case against Nicodemo S. Scarfo Jr., accused of running gambling and loan sharking operations for the Gambino crime family. The defendant's lawyers are arguing that federal law enforcement officials acted unconstitutionally when they evaded the privacy protections of PGP by surreptitiously installing on Scarfo's personal computer some technology that recorded every keystroke made, including his password. Their position is that this action amounted to a wiretap, for which they should have obtained a special court order, called a "Title III" order. But assistant U.S. attorney Ronald Wigler says that "letters do not become 'electronic communications' subject to Title III merely because they happen to have been typed on a computer." (New York Times 30 Jul 2001)
http://partners.nytimes.com/2001/07/30/technology/30TAP.html

PRIVACY ADVOCATES OBJECT TO "KEY LOGGING" TECHNOLOGY [14 Aug 2001]
Privacy advocates are strenuously criticizing the use by federal law enforcement officials of "key-logging" technology to monitor the communications of "Little Nicky" Scarfo, a reputed Philadelphia mob boss. Rather than obtain a court-approved wiretap order, the officials used a simple search warrant (much easier to obtain) in order to plant on Scarfo's computer a yet-to-be-explained technology that monitors every keystroke, including e-mail. Mark Rasch of the security consulting firm Predictive Systems says: "The logical consequence of the government's argument is that the government will never need to get a wiretap order for a computer. With the technology that's available today, the government can remotely install software on a computer to capture all keystrokes and transmit that report to its agents in real time." (Washington Post 14 Aug 2001)
http://washingtonpost.com/wp-dyn/articles/A55606-2001Aug9.html

FBI TARGETS SUSPECTS' PCs WITH SPY VIRUS [21 Nov 2001]
The FBI is working on software that could insert a computer virus into a suspect's computer capable of reading encrypted data. The software, known as "Magic Lantern," installs "keylogging" software that can capture keystrokes typed on a computer. The virus can be sent via e-mail and once on the targeted PC, it waits for a suspect to launch the Pretty Good Privacy encryption program and then logs the passphrase used to start the program, essentially giving agents access to the keys needed to decrypt files. The Magic Lantern software is part of the FBI's "Enhanced Carnivore Project Plan," which operates under the umbrella project name of Cyber Knight. Electronic Privacy Information Center attorney David Sobel says privacy issues arise when keylogging results in "overly broad" searches, since it would be possible to observe every keystroke typed by the suspect, even if a court order specified only encryption keys. The FBI has already used a less-sophisticated version of the software to build the high-profile racketeering case against Nicodemo Scarfo, but had to manually turn the system on and off in order to comply with the court order. (MSNBC/Wall Street Journal 21 Nov 2001) http://interactive.wsj.com/articles/SB10062942834030720.htm (sub req'd)

FBI CONFIRMS DEVELOPMENT OF KEYSTROKE-CAPTURING EAVESDROP TECHNOLOGY [12 Dec 2001]
The FBI has confirmed that it has under development a technology that could use the Internet to plant Trojan Horse software in a criminal or terrorist suspect's PC that would capture passwords to access the suspect's e-mail and other documents. An FBI official said, "Like all technology projects or tools deployed by the FBI it would be used pursuant to the appropriate legal process." (Reuters/Yahoo 12 Dec 2001)
http://dailynews.yahoo.com/htx/nm/20011212/tc/tech_magiclantern_dc_1.html

---

Category 1D3 *Litigation, legal rulings, judgements affecting law enforcement*

2002-02-20 **law enforcement e-mail interception forensics inspection authority warrant court order lawsuit jurisprudence wiretapping**

NewsScan

DO THE POLICE NEED A COURT ORDER TO INSPECT A SUSPECT'S E-MAIL?
In a case involving the admissibility of Internet evidence used to convict he a man for solicitation of a 15-year-old girl he met in a chat room, the Pennsylvania Supreme Court will decide whether police authorities need a court order (as they would if they wanted to set up a telephone wiretap operation) before looking at a suspect's e-mail and instant messages. The lower court took the position that the wiretapping law did not apply because the police did not intercept the messages but looked at them after they had been received, and it suggested that the defendant had given implied consent to the inspection of his messages: "Any reasonably intelligent person, savvy enough to be using the Internet, would be aware that messages are received in a recorded format, by their very nature, and can be downloaded or printed." (AP/USA Today 20 Feb 2002)
http://www.usatoday.com/life/cyber/tech/2002/02/20/internet-wiretap.htm

---

Category 1D3 *Litigation, legal rulings, judgements affecting law enforcement*

2002-05-14 **ISP Internet service providers subpoenas search warrants police officers physical presence**

NewsScan

INTERNET GROUPS SAY THEY DON'T WANT POLICEMEN IN THEIR LOBBIES
Internet service providers and trade groups have gone to a federal appeals court to protest another court's requirement that police officers be physically present when search warrants are conducted to find electronic messages or files. The groups argue that the requirement creates a "chilling effect" on a company's subscribers without accomplishing anything good: "The police officer waiting in the lobby while the technician works away on the computer does not in any way safeguard anyone's Fourth Amendment rights." Besides, it would be burdensome and disruptive: "A large Internet service provider can receive literally hundreds of search warrants and other requests for information during the course of a year. It is entirely possible that at any given time a dozen or more law enforcement officers would be on the premises of given service provider." (Reuters/San Jose Mercury News 13 May 2002)
http://www.siliconvalley.com/mld/siliconvalley/3256778.htm

Category 1D3 *Litigation, legal rulings, judgements affecting law enforcement*

2002-05-28 **privacy surveillance subpoena just cause ISP telecommunications police law enforcement civil liberties homeland defense**

FindLaw Download This 87

GOVERNMENT, INTERNET BIZ FIGHT TERROR
In the seven months since the passage of a sweeping law to combat terrorism, Internet and telecommunications companies have seen a surge in law enforcement requests to snoop on subscribers. Privacy advocates fear that expanded police power under the [U.S.A.P.A.T.R.I.O.T.] Act - combined with lax oversight and increased cooperation between the government and private sector phone network and Internet gatekeepers - may be stomping on civil liberties. The new laws do not apply just to terrorism but to other crimes as well.
http://news.findlaw.com/ap/ht/1700/5-27-2002/20020527044501_18.html

Special Coverage -- War On Terrorism
http://news.findlaw.com/legalnews/us/terrorism/index.html

Category 1D3 *Litigation, legal rulings, judgements affecting law enforcement*

2002-07-09 **jurisdiction wiretaps law legal application surveillance law enforcement police investigation ISP Internet serfice provider phone cable**

NewsScan

IS BROADBAND A TELECOM SERVICE -- OR AN INFO SERVICE?
The answer to that question will make a lot of difference, especially to the FBI and the Justice Department, which rely on a law requiring "telecommunications" services to be designed in a way that would allow law enforcement officials, with a court order, to monitor activity of suspected criminals or terrorists; in contrast, there is no such requirement for "information services." So the Federal Communications Commission will be asked to determine that electronic-surveillance access rules also apply to the broadband information offerings of phone and cable companies. (USA Today 8 Jul 2002)
http://www.usatoday.com/life/cyber/tech/2002/07/09/wire

Category 1D3 *Litigation, legal rulings, judgements affecting law enforcement*

2002-07-16 **surveillance wiretaps police law enforcement warrants court order criminal hackers crackers life sentence punishment**

NewsScan

HOUSE APPROVES LIFE SENTENCES FOR CRACKERS
The U.S. House of Representatives has approved the Cyber Security Enhancement Act (CSEA) by a near-unanimous vote. Among the Act's provisions are an expansion of police ability to conduct Internet or telephone eavesdropping without first obtaining a court order, and the approval of life prison sentences for malicious computer hackers (crackers) whose acts "recklessly" put others' lives at risk. In the case of wiretaps, the Act would permit limited surveillance without a court order when there is an "ongoing attack" on an Internet-connected computer or "an immediate threat to a national security interest." The surveillance would be limited to collecting a suspect's telephone number, IP address, URLs or e-mail header information -- not the content of an e-mail message or phone conversation. In addition, the Act would permit ISPs to disclose the contents of e-mail messages and other electronic records to police in cases when "an emergency involving danger or death or serious physical injury to any person requires disclosure of the information without delay." The Act is not expected to meet any serious opposition in the Senate. (CNet News.com 15 Jul 2002)
http://news.com.com/2100-1001-944057.html?tag=fd_top

Category 1D3 *Litigation, legal rulings, judgements affecting law enforcement*

2003-03-07 **probable cause judicial ruling fourth amendment**

NewsScan

TWO JUDGES REJECT FBI TESTIMONY IN INTERNET PORN CASES
Federal district judges Denny Chin in New York and Catherine D. Perry in St. Louis have rejected evidence obtained by FBI agents who claimed falsely that anyone signing up with the child porn site "Candyman" would automatically receive child porn images from other site members. Later, the agents admitted that people signing up for the group had the ability to opt out of the member mailing list and therefore did not necessarily receive pornography through that list. Judge Chin wrote: "If the government is correct in its position that membership in the Candyman group alone was sufficient to support a finding of probable cause, then probable cause existed to intrude into the homes" of thousands of people who had merely logged onto that Web site. "Here, the intrusion is potentially enormous. Thousands of individuals would be subject to search, their homes invaded and their property seized, in one fell swoop, even though their only activity consisted of entering an e-mail address into a Web site from a computer located in the confines of their homes." (New York Times 7 Mar 2003)

Category 1D3 *Litigation, legal rulings, judgements affecting law enforcement*

2003-04-03 **wiretapping issues VoIP voice over IP**

NewsScan

ONLINE WIRETAPPING POSES LEGAL, TECHNICAL OBSTACLES
As the Internet telephony market expands, law enforcement officials are facing both legal and technical hurdles as they seek to block the emerging services from becoming a haven for criminals and terrorists. The FBI wants regulators to affirm that tapping into Voice over Internet Protocol (VoIP) networks is covered under the 1994 Communications Assistance for Law Enforcement Act, and is also pushing the industry to create technical standards that would make such wiretaps easier and cheaper. Because VoIP is so new, standards don't yet exist for setting up networks, but several groups, including the Telecommunications Industry Association, are working on them. "We're seeing major changes in the network, and we are trying to be ahead of the curve," says the FBI's unit chief for electronic surveillance. Privacy advocates, on the other hand, fear that because of the nature of the technology, tapping into the data stream for voice would also possibly retrieve more than what the court ordered, including people's e-mail and other digital communications. (AP 3 Apr 2003)

Category 1D3 *Litigation, legal rulings, judgements affecting law enforcement*

2004-01-21 **conviction underage sex solicitation email instant messaging monitoring**

NewsBits; http://pennlive.com/newsflash/pa/index.ssf?/base/news-11/1074694141293801.xml

Court upholds conviction of man arrested because of e-mail

The Pennsylvania Supreme Court upheld the conviction of a man who says police should not have monitored his e-mail and instant messages without obtaining a court order. The case involved a former police officer, Robert Proetto, who was convicted of using the Internet to solicit sex from a 15-year-old girl. Proetto, a former officer with the Colonial Regional police in Northampton County, is appealing his conviction. The Supreme Court issued an order that merely affirmed a lower court's decision without comment.

EPIC ALERT 11.02:

Category 1D3 *Litigation, legal rulings, judgements affecting law enforcement*

2005-05-28 **encryption software evidence trial court proceeding intentionality reaction response hysteria exaggeration excessive**

RISKS; 23 90
http://www.theregister.co.uk/2005/05/25/pgp_admissable_child_abuse_case/

BROUHAHA OVER ENCRYPTION AS EVIDENCE OF ILL-INTENT

An eruption of emotion resulted when a Minnesota judge ruled that the presence of encryption software on the computer of a man accused of child abuse (soliciting a minor for lewd photographs) was relevant to the prosecution's case. Although one can reasonably express skepticism about the wisdom of the court's ruling or question their understanding of the availability and acceptance of encryption software, some people responded with comically exaggerated emotion. One contributor to RISKS labeled his missive "Encryption Illegal in Minnesota" -- which was plainly nonsense. The summary from _The Register_ was as follows:

>The Minnesota State Court of Appeals has rejected an appeal from David Levie on charges of soliciting a nine-year-old girl to pose for naked pictures, ruling that the prosecution's introduction of an encryption program on his computer as evidence was admissible. During a search of his computer, police found the PGP (Pretty Good Privacy) encryption program. Levie's lawyers argued that forensic examination yielded no evidence of any encrypted files on his computer and so the presence of encryption software should not be used as evidence against Levie. One police officer testified that PGP may be included with every Apple computer on the market. The appeals court ruled that the presence of encryption software was relevant to the prosecution's case and refused to order a retrial, though the case will be sent back for re-sentencing. The case could establish a precedent in Minnesota of accepting the presence of encryption software as evidence of criminal intent.<

Category 1D3 *Litigation, legal rulings, judgements affecting law enforcement*

2005-09-10 **civil liberties privacy concerns USA PATRIOT Act FBI ACLU ruling**

EDUPAGE; http://www.nytimes.com/2005/09/10/nyregion/10library.html

FBI LOSES ROUND ONE

A federal judge has handed the FBI a preliminary defeat in its efforts to continue to suppress information about an investigation of a Connecticut institution. The institution, whose identity has been kept confidential under the terms of the USA PATRIOT Act, and the American Civil Liberties Union (ACLU) sued the FBI for the right to disclose the institution's identity. Judge Janet C. Hall agreed with the plaintiffs, saying that under the FBI's position, "the very people who might have information regarding investigative abuses and overreaching are peremptorily prevented from sharing that information with the public." Hall did grant a stay of her ruling, however, giving federal authorities until September 20 to try to persuade the Court of Appeals to overturn the ruling. If the appeals court takes no action by then, the plaintiffs are free to disclose the institution's identity.
Watching the case closely are groups critical of the PATRIOT Act, who have long argued that the law grants federal authorities excessive investigative powers at the expense of civil liberties.
New York Times, 10 September 2005 (registration req'd)

Category 1D3 *Litigation, legal rulings, judgements affecting law enforcement*

2005-09-26 **FCC VoIP wiretap decision police civil liberties privacy concerns CALEA**

EDUPAGE; http://news.zdnet.com/2100-1035_22-5883032.html

FCC ISSUES VOIP DECISION; QUESTIONS REMAIN

The Federal Communications Commission issued a decision that any voice over Internet protocol (VoIP) provider linked to the public telephone network must comply with a set of rules making it easier for police to seek and obtain wiretaps. The affected companies must meet these requirements by spring 2007. Still undecided is what the Communications Assistance for Law Enforcement Act (CALEA) ruling means for universities, nonprofits, companies, and individuals offering wireless or other forms of Internet access. The regulation is based on the argument that CALEA's definition of "telecommunications carrier" applies to broadband and VoIP providers. The FCC plans to issue another decision on the subject by the end of the year.
ZDNet, 26 September 2005

Category 1D3 *Litigation, legal rulings, judgements affecting law enforcement*

2005-10-22 **surveillance law enforcement universities academia communications Internet service providers ISPs cities municipalities counter-terrorism lawsuits**

RISKS; http://tinyurl.com/aumy4 24 08

UNIVERSITIES RESIST US GOVERNMENT DEMANDS FOR SURVEILLANCE HOOKS

The federal government, vastly extending the reach of an 11-year-old law, is requiring hundreds of universities, online communications companies and cities to overhaul their Internet computer networks to make it easier for law enforcement authorities to monitor e-mail and other online communications. The action, which the government says is intended to help catch terrorists and other criminals, has unleashed protests and the threat of lawsuits from universities, which argue that it will cost them at least $7 billion while doing little to apprehend lawbreakers. Because the government would have to win court orders before undertaking surveillance, the universities are not raising civil liberties issues.

The order, issued by the Federal Communications Commission in August and first published in the Federal Register last week, extends the provisions of a 1994 wiretap law not only to universities, but also to libraries, airports providing wireless service and commercial Internet access providers. It also applies to municipalities that provide Internet access to residents, be they rural towns or cities like Philadelphia and San Francisco, which have plans to build their own Net access networks. So far, however, universities have been most vocal in their opposition.

The 1994 law, the Communications Assistance for Law Enforcement Act, requires telephone carriers to engineer their switching systems at their own cost so that federal agents can obtain easy surveillance access.

[Abstract by Peter G. Neumann]

Category 1D3 *Litigation, legal rulings, judgements affecting law enforcement*

2005-10-23 **FCC CALEA ISP higher education libraries expense**

EDUPAGE; http://www.nytimes.com/2005/10/23/technology/23college.html

HIGHER EDUCATION RESPONDS TO CALEA ORDER

The higher education community is preparing several responses to an order by the Federal Communications Commission to extend the provisions of the Communications Assistance for Law Enforcement Act (CALEA) to Internet service providers, including institutions of higher education, libraries, and municipalities that provide Internet access. The order would require covered entities to configure their networks to allow law enforcement officials--with the authority of a court order--to tap into data streams remotely. Currently, such taps typically require the assistance of network personnel. Making networks compliant with the new regulations would in most cases require significant investment in new switches and routers, and higher education officials contend that the expense would not be justified by the number of taps placed on their networks. By some accounts, U.S. colleges and universities would incur costs of at least $7 billion to redesign their networks. Those seeking an exception from CALEA for education noted that in 2003, just 12 of nearly 1,500 wiretap orders were issued for computer networks. Representatives of higher education are working on responses including appeals, possible lawsuits, and negotiations with federal officials. Higher education officials said that the objection is not with providing appropriate assistance to law enforcement but that lower-cost solutions would provide the needed capability without placing a large financial burden on colleges and universities and their students. New York Times, 23 October 2005 (registration req'd)

Category 1D3 *Litigation, legal rulings, judgements affecting law enforcement*

2006-02-06 **wiretapping racketeering federal grand jury private investigator indictment**

DHS IAIP Daily; http://www.securityfocus.com/brief/129 23

THREE CHARGED WITH WIRETAPPING, RACKETEERING.

A federal grand jury indicted private investigator Anthony Pellicano and two associates for the alleged illegal use of law enforcement data and wiretapping using a custom software program, prosecutors announced on Monday, February 6. The 110-count indictment charges Pellicano and his associates with creating a criminal enterprise in which the private detective allegedly paid tens of thousands of dollars to police officers to provide him with confidential law enforcement information on numerous individuals. In addition, the indictment charges Pellicano and the two associates -- a software developer and a telecommunications engineer -- with creating a program known as Telesleuth in 1995 and using it as early as 1997 to wiretap such people as Herbalife co-founder Mark Hughes, actor Sylvester Stallone and journalist Anita Busch. Monday's indictment was originally issued under seal on Wednesday, February 1. Among the other charges are 31 counts of wire fraud and five counts of identity theft. Four other defendants were charged wiretapping and wire fraud.

1D4 Government funding for law enforcement

Category 1D4 *Government funding for law enforcement*

2000-02-07 **budget proposal administration wiretapping law enforcement military telco telephone company**

Wired http://www.wired.com/news/politics/0,1283,34164,00.html, NewsScan, Washington Post http://www.washingtonpost.com/wp-dyn/articles/A32193-2000Aug15.html

In February, the Clinton administration proposed a $1.84T budget fiscal 2001 that would include major increases in spending on law enforcement capabilities such as wiretapping. The government would reimburse telcos to the tune of $240M (up from $15M) under the controversial CALEA (Communications Assistance to Law Enforcement Act) for rewiring their networks to make wiretapping easier.

[However, in August (wrote the NewsScan editors), A three-judge panel of the U.S. Court of Appeals for the District of Columbia . . . ruled that the Federal Communication Commission's attempts to implement a 1994 electronic wiretap law have been too accommodating to law enforcement agencies and not sufficiently protective of the right of citizens to individual privacy or of the financial requirements of companies. The wiretap law (the Communications Assistance for Law Enforcement, or CALEA) was passed by Congress because the FBI had insisted it was losing ground against criminals because wireless phone companies were not designing wiretapping capabilities into their networks. An executive of the Center for Democracy and Technology, which had opposed the FBI's request to Congress, . . . [said] the appellate court's decision means that "government cannot get its hands on what it's not authorized to get just by promising it won't read what it's not supposed to read." (Washington Post 16 Aug 2000)

Category 1D4 *Government funding for law enforcement*

2002-05-21 **cybercrime research funding law legislation**

FindLaw Download This 86

SENATE PANEL OKS MORE CYBERCRIME DOLLARS
The U.S. Senate Commerce Committee today voted to increase funding for anti-cybercrime programs, despite claims from software and high-tech groups that last-minute changes to the bill could stifle innovation. The "Cyber Security Research and Development Act," sponsored by Sen. Ron Wyden, D-Ore., would give $970 million over five years to the National Science Foundation and National Institute of Standards and Technology to improve government computer and network security.
http://www.newsbytes.com/news/02/176661.html

Category 1D4 *Government funding for law enforcement*

2002-10-09 **federal funding grant institute cyberterrorism research**

NewsScan

CARNEGIE MELLON GETS GRANT TO FIGHT CYBERTERRORISM
Carnegie Mellon's new Center for Computer and Communications Security has received $35.5 million in funding from the U.S. Defense Department to further its goal of developing tools and tactics for fighting cyberterrorism. The Center is already researching ways to integrate artificial intelligence into computer hardware so that components such as hard drives could automatically shut down in event of hacker attack and even report such attacks to network administrators. Researchers are also investigating how to use biometric technology, such as fingerprints, iris and voice scans, and face recognition, to confirm the identity of computer system users. (AP 8 Oct 2002)
http://apnews.excite.com/article/20021008/D7MHJA6G0.htm

Category 1D4 *Government funding for law enforcement*

2003-04-30 **Tom Ridge DHS Northern Virginia Technology Y2K 9/11 terrorist attacks ideas security**

NIPC/DHS

April 30, IDG News Service — DHS asks for tech help.

Tom Ridge, secretary of the Department of Homeland Security (DHS), highlighted his department's need for technological innovations during a speech for members of the Northern Virginia Technology Council in Virginia, Tuesday. Ridge also called for the technology industry to do more to protect the U.S. technology infrastructure, noting that private companies control 85 percent of the nation's cyber resources. "We think that the lessons learned from Y2K and 9/11 should be applied and not forgotten. Ridge said he fears that some U.S. residents may be "lapsing into complacency" about the possibility of terrorist attacks. "You need to be just as worried, maybe even more worried, about somebody hacking into your system as somebody pulling up with explosives," Ridge said. Ridge asked the crowd for "good ideas and cost-effective solutions" for domestic security that can be copied across the U.S.

Category 1D4 *Government funding for law enforcement*

2003-08-08 **NSA National Security Agency backdoor detection center information assurance director Daniel Wolf Software logic bombs**

NIPC/DHS

August 08, SecurityFocus — NSA proposes backdoor detection center.

The information assurance director for the National Security Agency's (NSA) is calling on Congress to fund a new National Software Assurance Center dedicated to developing advanced techniques for detecting backdoors and logic bombs in large software applications. In testimony before the House Select Committee on Homeland Security's cybersecurity subcommittee last month, Daniel Wolf bemoaned an absence of tools capable of scouring program source code and executables for evidence of tampering. The proposed solution: a federally funded think-tank that would include representatives from academia, industry, government, national laboratories and "the national security community," said Wolf, "all working together and sharing techniques."

Category 1D4 *Government funding for law enforcement*

2003-10-23 **internet Security Ads Government TV radio firewall virus alerts national cyber security Alliance worms FTC**

NIPC/DHS

October 23, Washington Post — U.S. Government plans Internet security ads.

An advertising campaign designed to educate home and small business computer users about the importance of using firewalls and anti-virus software, as well as defending against online fraud, is expected to debut next year. The $1.8 million program is the brainchild of officials at the Department of Homeland Security (DHS) and the National Cyber Security Alliance, a group of more than 50 technology companies. The campaign will air on television and radio spots and in magazines, newspapers and movie theaters throughout the country. The alliance in a June study found that roughly 67 percent of high-speed Internet users do not use firewalls. More than 60 percent of those surveyed said they did not keep their anti-virus software updated against the most current viruses and worms. Orson Swindle, a commissioner on the Federal Trade Commission, said the large number of people affected by online fraud and the recent spate of viruses and worms show just how much education needs to be done.

Category 1D4 *Government funding for law enforcement*

2004-01-16 **Department Commerce IT security INFOSEC fund funding**

NIPC/DHS; http://www.fcw.com/fcw/articles/2004/0112/web−sade−01−14−04. asp

January 14, Federal Computer Week — Commerce to fund IT security.

A senior Commerce Department official said funding will be poured into information technology security this year. Michael Sade, director for acquisition management and procurement executive, said the real impact of IT security isn't going to be on the technology side, but on the personnel side — such as ensuring vendors have security clearances. Sade generally spoke about how Commerce officials will better partner on projects with vendors and other government agencies through dialogue. Significant projects underway include modernization of the Patent and Trademark Office and National Weather Service. Commerce has begun making significant IT investment in preparation for the 2010 Census — possibly including the capability of doing surveys through the Web, Sade said. Another growing trend will entail better review of satellite programs in which the department funds projects that are overseen by other departments and agencies.

Category 1D4 *Government funding for law enforcement*

2004-02-26 **security trade group cybersecurity advocacy Homeland Security Council**

DHS IAIP Daily; http://www.fcw.com/fcw/articles/2004/0223/web−security−02 −26 −04.asp

February 26, Federal Computer Week — Security trade group formed.

Eleven computer security companies announced the formation of an advocacy group, the Cyber Security Industry Alliance, to influence public policy and spending on cybersecurity. The members, which include well-known computer security firms, said they want to promote generally accepted information security principles, exchange cybersecurity threat information with government agencies, and eventually expand education and research to improve cybersecurity. Paul Kurtz was named executive director of the new organization. He is a former special assistant to the president and senior director of the Critical Infrastructure Protection Directorate under the White House's Homeland Security Council. Companies in the alliance are also interested in and supportive of the federal government's information technology product and systems certification program known as the National Information Assurance Partnership, said Ron Moritz, senior vice president and chief security strategist at Computer Associates International Inc.

Category 1D4 *Government funding for law enforcement*

2004-05-18 **cybercrime law enforcement importance of skills**

DHS IAIP Daily; http://news.zdnet.co.uk/internet/security/0,39020375,3915513 8,00.htm

May 18, ZDNet UK — Skills not money needed to fight cybercrime.

Law enforcement agencies require a bigger pool of skilled investigators and digital forensic experts, not more money or legislation, according to a study by The European Information Society Group (EURIM) that was presented at the House of Commons on Tuesday, May 18. According to the third phase of EURIM's e-crime study, around half the UK population and 10 percent of the world's population has access to the Internet. This means that a large number of criminals also connect to the Internet, which has led to the transfer of traditional crimes to the online world. The problem, said EURIM, is that although cybercrimes are becoming more common, members of the police force and specialist computer crime units lack many of the basic skills required to trace and analyze computer-based crimes. EURIM 's study makes a number of recommendations, one of which is to create specialist academic courses that focus on areas that are currently neglected by schools and colleges.

Category 1D4 *Government funding for law enforcement*

2004-11-30 **Federal Bureau Investigation FBI cybercrime security information technology student specialist recruitment challenge Internet Crime Complain Center I3C**

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1734035,00.asp?kc=ewnws120104dtx1k000 0599

November 30, eWeek — FBI's cyber-crime chief relates struggle for top talent.

The FBI's inability to recruit and keep the best available IT talent has proven to be one of the biggest challenges facing the government's Internet Crime Complaint Center (I3C), a senior official said Tuesday, November 30. Delivering the keynote address on the opening day of Ziff Davis Media's Security Virtual Tradeshow, I3C chief Daniel Larkin said the center's staffing problems underline the need for deeper cooperation between the FBI and the IT industry to win the battle against sophisticated cyber-criminals. "We can't recruit and keep the best available minds in the IT world. They come, stay a few years and move on because, ultimately, we can't pay what the industry pays for talent," Larkin said, adding that the bureau also has experienced difficulties with keeping pace with employees' training needs. Because of those shortcomings, Larkin said, the I3C spent the past four years forging partnerships with the biggest names in the tech industry to share expertise, coordinate on intelligence and develop best practices and protocols for fighting cyber-crime.

Category 1D4 *Government funding for law enforcement*

2006-01-08 **computer crime New Jersey law enforcement effort FBI child pornography incident response outreach fraud identity theft**

DHS IAIP Daily; 23
http://www.nj.com/news/gloucester/local/index.ssf?/base/news − 2/1136625344302990.xml&coll=8

NEW JERSEY LAW ENFORCEMENT UNITS COMBINE TO FIGHT COMPUTER CRIME

Three state law enforcement units in New Jersey will combine to fight computer crime. The new Computer Crime Task Force, formed by New Jersey state Attorney General Peter C. Harvey, will include personnel from the Division of Criminal Justice's (DCJ) Computer Analysis and Technology Unit (CATU), the New Jersey State Police Digital Technology Investigations Unit, and the state police Cyber Crimes Unit. The new task force will include three investigative units staffed with state troopers, DCJ investigators, and FBI special agents and will focus on computer hacking and viruses, Internet fraud, and the creation and distribution of child pornography. The Incident Response Unit investigations will focus on computers, computer networks, telecommunication devices, and other devices used in the commission of crimes. It will also provide cyber crime awareness outreach services to the public and train law enforcement regarding network intrusion crimes. The Cyber Crime Unit will investigate the use of computers in fraud and identity theft. A training committee will coordinate community outreach programs. The task force will aim to increase the reporting of cyber crime and computer intrusions. A Computer Crimes Task Force hotline is available at 1-888-648-6007, in addition to an online incident reporting form at http://www.cctf.nj.gov.

21.1 General QA failures

Category 21.1 *General QA failures*

1997-01-08 **QA quality assurance**

PA News

A major stock brokerage in England faced million-pound claims for compensations after its new computer software generated a tide of errors. The errors sparked so many queries that the staff began falling behind in providing responses, leading to an avalanche of customer complaints. The company even had to stop taking on new business.

Category 21.1 *General QA failures*

1997-01-10 **QA**

RISKS 18 75

In Finland, a software error caused the automobile registration system to send out 11,000 erroneous letters threatening to de-register cars because they were supposedly out of use. The embarrassed agency had to send out 11,000 letters of apology.

Category 21.1 *General QA failures*

1997-01-13 **QA quality assurance ticket verification operator error**

RISKS 18 76

You might want to hang on to those "old-fashioned" paper tickets for a while. In a case posted to RISKS in January 1997, Robin Burke reports that his wife was informed that her electronic ticket had been used the week before her confirming phone call. It took several phone calls to prove that she was not trying to defraud the airline. It appears that a data entry operator had incorrectly brought up the wife's record and marked it "used" without noticing the mismatch.

Category 21.1 *General QA failures*

1998-01-06 **QA quality assurance Trojan unauthorized liability tort**

RISKS 19 53

Larry Werring wrote in RISKS FORUM DIGEST that major software manufacturers are permitting appalling lapses of quality assurance by letting their programmers insert unauthorized code into production versions of software. Microsoft EXCEL 97, for example has a flight simulator of sorts that pops up if you press a particular sequence of keys. How much memory and disk space are these Trojans taking up, he asks. [BTW, I tested the EXCEL Easter Egg; it worked but it crashed EXCEL when I pressed the ESC key.]

Category 21.1 *General QA failures*

1998-01-06 **authenticity quality assurance QA design identification**

RISKS 19 53

An anonymous correspondent reported to RISKS that a CVS pharmacy computer program keyed on first and last name as a (falsely) unique identifier. As a result, his prescription would have been assigned to a stranger's record — and in some circumstances (e.g., treatment for HIV infection) such prescriptions would damage insurability.

Category 21.1 *General QA failures*

1998-01-10 **confidentiality reliability personnel hiring background**

RISKS 19 54

ICL, the big high-tech UK company, proposed to hire prison inmates to work on the Y2K problem. Security experts politely pointed to security risks in having such people become intimately acquainted with and even modify internal details of production applications.

Category 21.1 *General QA failures*

1998-03-23 **QA**

Wired

Al Gore's staff used their computer system to send Sen. Daniel Moynihan birthday greetings on 16 March. However, what they actually sent was congratulations on the birth of twins.

Category 21.1 *General QA failures*

1998-03-26 **QA dimension capacity software failure**

EDUPAGE

As if the Y2K problem weren't enough, some analysts were concerned about the likely failure of some financial software incapable of handling a Dow-Jones Industrial Average of 10,000 or more. Seems many programmers limited that field to four digits.

Category 21.1 *General QA failures*

1998-04-09 **QA quality assurance pension fund underpayment blooper bug**

RISKS 19 66

Over the last 20 years, Los Angeles County in California underpaid its employee pension fund because of a programming error. The bill: $1.2B in missing capital.

Category 21.1 *General QA failures*

1998-04-14 **QA quality assurance nuclear facility fissionable uranium**

RISKS 19 67

At Los Alamos National Laboratory, a problem in the software linking a joy-stick to a stepper motor caused a servomechanism to almost slam together two masses of fissionable uranium-235 [these particular U-235 masses would have remained subcritical even if they had slammed together]. The report on the DoE Web site (see <http://tis.eh.doe.gov/web/oeaf/oe_weekly/oe_weekly_98/oe98-12.html>) said, "Engineers troubleshot the control circuitry and discovered problems with the software and flaws in the communication between the joystick controls and the central processing unit. They determined that when the joystick interface did not respond, a subroutine returned an ASCII (American Standard Code for Information Interchange) character "?" to the main program for the potentiometer settings that controlled the stepping motor speed. The main program was never developed to deal with a question mark and translated this value to the number equivalent of an ASCII "?" (the number 63). The number 63 corresponded to a large negative position (beyond closure of the stacks) that caused the stepping motor to drive in at full speed when it was selected for movement." [Moral: design your QA tests to prevent nuclear explosions wherever possible.]

Category 21.1 *General QA failures*

1998-04-21 **QA privacy phones**

EDUPAGE

Southern California customers of GTE who paid to have unlisted numbers were not pleased when 50,000 unlisted accounts were published in detail and sold to telemarketers. The company, facing fines of up to $30,000 per name, blamed the problem on the notorious "computer glitch" which is (judging from its curiously frequent occurrence in critical systems) presumed to be a cybercontruct, possibly extraterrestrial, completely independent of quality assurance procedures. X-files staff members should look into this, as should tort lawyers.

Category 21.1 *General QA failures*

1998-05-10 **QA data corruption quality assurance database codes publish**

RISKS 19 73

Pity Mr Cody Johnston, a commercial trucker in Bozeman, MT. He admittedly broke speeding laws and paid a fine. Unfortunately, the court computer system printed out a list of convictions using erroneous labels for the internal codes and the local newspaper reported his misdemeanor as a sexual deviation charge, which potentially includes homosexuality and bestiality. Mr Johnston sued the court and the newspaper for libel.

Category 21.1 *General QA failures*

1998-05-14 **QA quality assurance software engineering reliability**

EDUPAGE

Salon Magazine, the online source for intellectual discussions of social issues, published an interesting essay by Ellen Ullman, author of _Close to the Machine_ (City Lights Press), describing the poor quality of current software engineering. See <http://www.salonmagazine.com/21st/>.

Category 21.1 *General QA failures*

1998-06-18 **obscenity QA quality assurance program language cursing**

EDUPAGE

Matsushita Panasonic Interactive media sold a program for children called "Secret Writer's Society." The program helps kids by reading their writing back to them; it includes an extensive list of prohibited words — curses, obscenities and so on. Unfortunately, poor QA allowed the program to generate strings of the prohibited words instead of suppressing them. Children and parents were startled by the streams of foul language erupting from their computers. The company's response was to deny that it was a significant problem.

Category 21.1 *General QA failures*

1998-06-23 **QA quality assurance lottery random numbers**

RISKS 19 83

Nobody who chose the digit "9" ever won the Arizona Lottery's new Pick 3 game — because the algorithm never generated a 9 in the winning three-digit numbers. Great embarrassment, possible legal liability. . . .

Category 21.1 *General QA failures*

1998-06-28 **QA quality assurance chip bug problem**

EDUPAGE

The new Xeon microprocessor from Intel, a component of workstation computers, was admitted to be flawed. Intel lamely tried to make a virtue of necessity; a spokesperson said, "The good news is that this (chip) isn't in the market yet."

Category 21.1 *General QA failures*

1998-07-22 **e-mail Eudora bug file corruption QA quality assurance**

EDUPAGE

In July, reports surfaced of a peculiar and disruptive bug affecting the popular Eudora Pro versions 3.0 and 4.0 e-mail programs. Bruce Adelsman of New Brighton, MN discovered that when the outbox was heavily loaded with messages that had already been sent, the e-mail program behaved erratically in sending new e-mail. Some new messages were marked as sent even though they weren't and some old messages we re-sent.

A few weeks later, another problem in Eudora came to light when independent testers found that it would be possible to interpret a mouse click on a URL embedded in a mail message to execute programmatic instructions instead of linking to a Web site. This flaw would allow a user to execute a malicious Trojan Horse program that could do anything the programmer wanted on the target machine. Qualcomm, makers of Eudora, immediately issued a patch to fix the problem.

In mid-August Sendmail, Inc., the company that has taken over commercial distribution of the formerly free sendmail program, announced server-level patches that would apply filters to e-mail to prevent delivery of hostile attachments.

Category 21.1 *General QA failures*

1998-07-26 **software engineering quality assurance QA fraud corruption**

EDUPAGE

In Mexico City, the change of government has reduced the level of endemic corruption that permeates Mexican business and politics. As a result, IBM de Mexico has agreed to pay the city administration $37.5M in damages for a failed database system project that they won without competitive bidding in 1996.

Category 21.1 *General QA failures*

1998-08-13 **QA quality assurance software backup Web site support**

RISKS 19 91

McAfee's PC Medic 97 Deluxe package included QuickBackup v2.04 for Windows; it failed to perform a total backup because it could not backup files from directories whose names contain a blank space. Solution from Network Associates Technical Support: download version 2.05 from the Web site. Problem: impossible, as the file was not on their Web site. Result: I returned the product for refund. Moral: Quality Assurance really does matter.

Category 21.1 *General QA failures*

1998-09-23 **QA quality assurance testing operations management**

RISKS 19 97

After technicians finished testing new programs at the National Australia bank, a major Sydney (Australia) clearing center, they unfortunately forgot to restore the payroll program. The NAB then failed to authorize payments from more than 50 major companies. "Tens of thousands of people missed payday" as a result.

Category 21.1 *General QA failures*

1998-10-01 **QA quality assurance testing operations availability**

RISKS 20 1

The Department of Social Security in the UK lost its National Insurance Registry when errors in the installation of new software developed by Andersen Consulting destroyed the database. Payments were forcibly being made manually and without normal checks on eligibility. The outage was expected to last at least a month, with untold hardship for government staff and unknown losses due to fraud.

Category 21.1 *General QA failures*

1998-10-01 **QA quality assurance testing operations availability banking**

RISKS 20 1

The Bank of Montreal installed a new version of its electronic-card transaction-processing software and promptly crashed its system. All MasterCard and debit-card authorizations were denied and the Bank's ATMs shut down. The system came back up again 10 hours later.

Category 21.1 *General QA failures*

1998-10-03 **QA quality assurance operations oversight banking**

RISKS 20 2

The Royal Bank of Canada prepared a file of checks destined for direct deposit in the Toronto Dominion Bank accounts of 50,000 welfare recipients in Ontario. When a Royal Bank technician noticed an error in dates on the file they had transmitted, they warned the Toronto Dominion to expect a new file and that file was duly transmitted. Unfortunately, the Toronto Dominion operations crew forgot to set a parameter to read the new file — and so 50,000 poor people got no checks at all that day.

Category 21.1 *General QA failures*

1998-10-21 **quality assurance QA design constraints real-world**

RISKS 20 4

M. Ruth Milner of New Mexico ran into a textbook case of poor software design. Several departments of the state government implemented a new database structure that attempts to comply with federal regulations requiring data interchange among states. Some bonehead analyst decided that the only name formats allowed would be
1. Initial(s) and last name.
2. First name, last name.
3. First name, middle initial, last name.

Poor M. Ruth was labelled MRUTH by both the DMV and the taxation department. Officials told her that the new systems had been implemented without real-world testing.

Category 21.1 *General QA failures*

1998-11-06 **euro conversion Europe commerce interoperability**

Reuters

At Gartner Group's European IT Conference in Cannes, France, industry analysts worried that European organizations have failed to cope with the monetary conversion to the Euro. The date for implementation was 1 December 1999, but many companies have failed to prepare for the new currency. Another problem was that many firms had already assigned their IT staff to the millennium conversion and were therefore understaffed to deal with the additional requirements of the new money. The Euro conversion experience could be a dry-run for the Y2K problem.

Category 21.1 *General QA failures*

1998-11-11 **quality assurance QS pornography TV satellite channels**

Reuters

For a few hours, subscribers to European satellite TV services were startled to see pornography from the Eros Channel on the channels normally assigned to BBC News. The mixup was apparently an accidental technical error at the satellite distribution center in Switzerland.

Category 21.1 *General QA failures*

1999-01-03 **QA quality assurance bug spreadsheet data export import**

RISKS 20 14

A RISKS correspondent noted that exporting numbers with 12 significant figures from Excel to a comma-delimited CSV file and back causes loss of the last 5 significant digits — and it doesn't even roundoff, merely truncates.

Category 21.1 *General QA failures*

1999-01-15 **QA**

RISKS 20 15

Craig Raskin reported in RISKS that several Y2K testing tools missed obvious errors in test programs he devised for quality assurance of his own Y2K tools. He wondered how many errors such commercial tools are missing in the production environments where they are being used trustingly by Y2K-compliance teams.

Category 21.1 *General QA failures*

1999-01-15 **Y2K QA quality assurance**

RISKS 20 15

James S. Vera wrote in RISKS 20.16: Intuit's Quicken'99 fails with a "divide by zero" message when a transaction dated in January 1999 is recorded in the Auto category and its "Home and Car Center" is opened.

Category 21.1 *General QA failures*

1999-01-29 **QA Y2K quality assurance**

RISKS 20 18

In the southern Swedish city of Malmö, a new version of the municipal accounting package caused consternation by losing transactions every night when the system would crash. As a result, some bills were not being paid, causing embarrassment for the city and cash-flow problems for the unpaid vendors.

Category 21.1 *General QA failures*

1999-02-01 **QA quality assurance failure bug underpayment contract**

RISKS 20 19

In England, the government's expensive (£140M) new NIRS 2 social benefits computer system installed by the UK Government Department of Social Security (DSS) was more than a year late in delivery. As a result, thousands of widows were underpaid for up to two years; missing amounts ranged from £1 to £100 a week. The government was therefore sitting on (and earning interest on) a windfall of £1B in unpaid benefits.

Category 21.1 *General QA failures*

1999-02-03 **QA Internet Explorer Microsoft antitrust trial embarrassment**

Wired via PointCast

A huge gefuffle over a small error erupted in the marathon Microsoft antitrust trial. A videotape of how slowly Windows 98 would access the Web when modified as instructed by government attorneys and experts. Turns out the videotape was made correctly but installation and uninstallation of the software for access to the Prodigy value-added network damaged the system registry.

Category 21.1 *General QA failures*

1999-02-04 **programming error bug array dimension limit rollover**

Investor's Daily, USA Today

As the Dow Jones industrial average approached 10,000 there were warnings that older software might rollover their interpretation of the index to 1000, causing a wave of automated selling and a potential dip in the stock market. In the event, nothing bad happened.

Category 21.1 *General QA failures*

1999-02-10 **QA quality assurance misplaced faith technology records**

RISKS 20 20

At Carnegie Mellon University, Professor Philip Koopman lost his photocopier privileges for one of his graduate courses because the administrators reported, straight-faced, that he and his students had made 4,294,967,026 copies in two weeks. They knew this because a computer told them so. Prof. Koopman didn't even bother doing the page/minute calculations but commented that the number was "suspiciously close to 2**32 and that it [was] far more likely the number -272 printed with an unsigned print format, but that argument didn't do [him]any good." He should have stuck to the page per minute calculation ((it works out to ~3551 copies per _second_ continuously for the entire 14 days).

Category 21.1 *General QA failures*

1999-02-12 **quality assurance Web site correction privacy**

San Jose Mercury News

Hallmark Cards deserves kudos for fixing a security hole on its Web site within 5 minutes of the first alert. [Would that everyone were so responsive.]

Category 21.1 *General QA failures*

1999-03-01 **QA quality assurance automated phone**

RISKS 20 23

Keith Rhodes wrote in to RISKS, "A police computer in Fort Worth TX made 1,300 phone calls to invite residents to a police community forum — beginning at 3 a.m. Sunday morning, instead of during the day."

Category 21.1 *General QA failures*

1999-03-11 **availability crash rollover design quality assurance QA time**

RISKS, http://support.microsoft.com/support/kb/articles/q216/6/41.asp 20 24

Because of what appears to be a 32-bit millisecond counter in the Windows95 and Windows98 Vtdapi.vxd module, all Windows 9x computers hang after 49.7 days of continuous operation. [See <http://support.microsoft.com/support/kb/articles/q216/6/41.asp>]

Category 21.1 *General QA failures*

1999-03-11 **date quality assurance QA**

RISKS 20 24

Kenneth Dyke reported in RISKS that several improperly-dated e-mail messages caused confusion and disorder in his MS-Outlook in-basket. For example, a message dated "Sun, 4 Jan 2099 18:28:02 -0200" was listed by Outlook as being dated "Fri, Aug 1, 1919, 12:28 PM." This and other errors did not increase Mr Dyke's confidence in Microsoft's Y2K remediation programs.

Category 21.1 *General QA failures*

1999-03-11 **prison jail doors locks open**

RISKS 20 24

ICSA.net's Director of Research Services, David Kennedy, wrote in RISKS, ". . . cell doors on the ninth floor of the Kenton County Detention Center in Covington KY opened spuriously and remained open for 9.5 hours, although the convicts were still confined within a larger area.

Category 21.1 *General QA failures*

1999-04-15 **privacy confidentiality e-mail addresses prospects blunder error bug snafu QA quality assurance failure**

CNET News.com http://www.news.com/News/Item/0,4,35168,00.html

Strike another blow for better quality assurance: registrants on the Xterra Web site run by Nissan were surprised to receive e-mail containing the entire list of 24,000 e-mail addresses of all those who had registered — a gold mine for unscrupulous scumbag junk mailers — or to competitors engaged in competitive intelligence. A Nissan spokesperson lamely explained that a "technical error" had done the deed. Yeeeessss, we had already deduced that the e-mail was unlikely to have been sent deliberately. . . .

Category 21.1 *General QA failures*

1999-04-15 **privacy confidentiality e-mail addresses prospects blunder error bug snafu QA quality assurance failure**

CNET news.com http://www.news.com/News/Item/0,4,35225,00.html

In April 1999, AT&T sent 1,800 e-mail messages containing all 1,800 addressees in the visible TO: field. Some recipients expressed concern about having their e-mail address distributed to junk e-mailers. A company spokesperson blamed human error for the blunder. In a story for CNET news.com, Troy Wolverston reported that, "Online privacy activist Jason Catlett, president of Junkbusters, said the Nissan and AT&T incidents show that companies are still trying to figure out how to use the Internet to target customers. He said that companies are starting to consider email to be an important marketing tool, but they lack the expertise to use it properly."

Category 21.1 *General QA failures*

1999-04-21 **QA quality assurance browser bugs correction patches**

CNET News.com http://www.news.com/News/Item/0,4,35492,00.html

Microsoft responded quickly to serious vulnerabilities in its Internet Explorer browser versions 4 and 5 by issuing patches within a couple of weeks after revelations that malicious Web sites could bypass IE security mechanisms using misleading URLs. The weaknesses allowed access to user files and a simple mechanism for hijacking Web connections, putting up spoofs in place of authentic pages and thereby tricking users into revealing confidential information such as user IDs, passwords, credit-card numbers and so on. Another peculiar feature was corrected in IE 5, where it was possible for a Web page to force an executable ActiveX control into a user's clipboard.

Category 21.1 *General QA failures*

1999-07-19 **Y2K programming quality assurance embedded code rollover time limits dates UNIX**

New York Times

A New York Times article reported on many date-related problems that will persist beyond the Y2K transition. For example, a well-known counter in UNIX systems rolls over to zero in 2038. Microsoft programs have counters that will break at various times; for instance, MS-Visual C++ will break in 2036 unless there are significant changes to the compiler and existing programs are recompiled before the limit. [In addition, many programmers have decided to use arbitrary windows of time rather than fixing the fundamental problem; thus they have defined two-digit ranges that fall into the 20th century and others that fall into the 21st. Unfortunately, no one agrees on precisely where the windows should lie so it is quite possible that an old product (or one based on an old product) will have serious problems in, say, 2025 whereas another one will break in 2030.]

Category 21.1 *General QA failures*

1999-07-21 **liability tort Y2K protection law consumers**

Reuters

In July, the Clinton Administration approved a law to delay lawsuits against companies providing software or other products that are not Y2K compliant. The 90-day cooling-off period should allow repairs, according to supporters of the bill. However, opponents claimed that the delay would limit consumer rights. [Strike another blow for allowing companies to get away with making users serve as unpaid quality-assurance staff — and doing testing on production systems.]

Category 21.1 *General QA failures*

1999-07-21 **financial fraud Y2K quality assurance outside consultants foreign study report**

Journal of Commerce

GartnerGroup issued a report on _Year 2000 and the Expanded Risk of Financial Fraud_ and warned that the huge effort to pry into production software worldwide has greatly increased the possibility that dishonest programmers will try to take advantage of the systems they have learned about — and modified, sometimes with minimal supervision.

Category 21.1 *General QA failures*

1999-07-30 **Y2K quality assurance critical infrastructure protection government**

Reuters

The Y2K Information Coordination Center (ICC) was established by the US government with plans to go operational by 31 October 1999 and close down by June 2000. The Y2K-ICC would help coordinate government efforts in Y2K remediation and response and would also work with critical infrastructure to log and counter Y2K problems and possibly even cyberattacks. However, John Koskinen, chair of the President's Council on Year 2000 Conversion, told Newsbytes that the ICC would definitely not morph into the dreaded FIDNET (Federal Intrusion Detection Network).

Category 21.1 *General QA failures*

1999-08-21 **GPS global positioning system rollover**

New York Times

The GPS time counter rolled over at midnight GMT on Friday Aug 20, 1999, with Saturday the 21st expressed as 0 instead of 1024 weeks since Jan 6, 1980. Although some people in Japan were inconvenienced by failure of their automobile GPS receivers, the event caused little disruption.

Category 21.1 *General QA failures*

1999-09-09 **date problem glitch bug legacy code programs**

Philadelphia Inquirer

Some Y2K specialists were concerned about the possibility of legacy-code failures on 9-9-99 because that date used to be commonplace as a marker meaning "End of input data." However, almost no reports of trouble were publicized. Many observers hoped that this non-event presaged similarly mild problems over the Y2K transition.

Category 21.1 *General QA failures*

1999-10-01 **malware backdoor Trojan logic bomb Y2K consultants sabotage infowar**

Newsbytes

Michael Vatis of the FBI's computer crime section and head of the National Infrastructure Protection Center warned that he expects to see significant sabotage and fraud carried out by consultants who have worked on Y2K fixes. The pressure and lack of quality assurance on outsourced program fixes makes his prediction reasonable.

Category 21.1 *General QA failures*

1999-10-28 **quality assurance computer hardware bug flaw tort liability class action lawsuit settlement**

OTC

Toshiba announced in late October that it had settled a class-action lawsuit resulting from a bug in some of its laptops that allowed data corruption on diskettes when writing to the last byte on any sector. The company agreed to pay $2.1B in damages.

Category 21.1 *General QA failures*

1999-11-04 **Web e-commerce sales preparation quality assurance load errors volume availability**

Wired

Handspring announced its new Visor palm-top computers and went online to sell them. Unfortunately, the company failed to apply adequate quality assurance to its site and encountered so many problems that even its President couldn't get the units he ordered. Chris Oakes, writing for Wired magazine, described the debacle. Key points:
* The unexpected surge in Web and telephone orders caught the company unprepared.
* Few customers have received their handhelds.
* Some customers have received duplicate orders or been billed twice the right amount.
* The company has made errors in calculating the sales taxes.
* Their Web site crashed immediately upon opening for business because of the heavy demand.
* In response, the company hired 40 operators to deal with phone orders — and still had customers waiting two hours for service.
The author commented, ". . . Handspring has become a virtual case study in how not to conduct e-commerce."

Category 21.1 *General QA failures*

1999-11-29 **Y2K QA quality assurance software testing bug glitch date**

Computerworld Online
http://www.computerworld.com/home/news.nsf/CWFlash/9911291jury

Sami Lais, writing for Computerworld Online on 1999-11-29, described a Y2K glitch with wider import. In Philadelphia, Jury Commissioner Michael J. McAllister was surprised to find potential jurors reporting that they had received instructions to appear for jury duty on Jan 3, 1900. The Y2K-compliant jury-roster software had been cleared of date bugs during acceptance tests. Investigation showed that subsequent changes linked the program to a module in a non-compliant library.

Moral: all quality assurance tests must be repeated after any program modification before putting the new version into production.

Category 21.1 *General QA failures*

1999-12-03 **quality assurance QA contingency planning glitches bugs errors failures**

http://www.idg.net/go.cgi?id=203718

Sean M. Dugan, senior research editor in the InfoWorld Test Center, published a thoughtful article in December about the implications of quality assurance for e-business. He pointed out that failing to have contingency plans in place to solve inevitable glitches is embarrassing and potentially disastrous for organizations trying to do business on the Web.

Category 21.1 *General QA failures*

2000-01-03 **Y2K quality assurance success**

Edupage, Washington Post, Wall Street Journal

On the whole, the IT world was delighted to see that Y2K fixes worked. As the New Year opened, few major problems were reported worldwide. Skeptics began murmuring that the entire exercise had been futile and that warnings of Y2K difficulties had been exaggerated. [Presumably these same people were prepared to burn fire stations for their annoying insistence on fire prevention techniques in the absence of worldwide conflagration.]

Category 21.1 *General QA failures*

2000-01-04 **Web site quality control QA assurance checking erotic inappropriate books videos advertising merchandising**

NewsScan, Los Angeles Times
http://www.latimes.com/business/20000104/t0000010000.html

Wal-Mart Stores, Inc. discovered guidebooks to erotic videos being advertised on its new Web site. A spokeswoman apologized for the failure of quality control in checking a third-party supplier's lists and promised to expunge references to "The Best of Gay Adult Videos" and "The Couple's Guide to the Best Erotic Videos."

Category 21.1 *General QA failures*

2000-01-09 **Y2K failures screen shots Web sites archive**

RISKS 20 74

The site < http://y2kmistakes.com > published an extensive list of screen shots from Web sites with Y2K problems.

Category 21.1 *General QA failures*

2000-01-19 **DNS WHOIS quality assurance QA**

NewsScan, Wired http://www.wired.com/news/technology/0,1282,33753,00.html

BulkRegister, a recently approved Internet domain name registrar, apparently has goofed. It allegedly sold several domain names to customers and then released them for sale again a day or two later, at which point they were resold by other registrars. The more recent buyers are the ones that show up in the master Whois.com database, which controls who can set up a site using that URL. "We are not allowed physically to access these domains," says one frustrated BulkRegister purchaser. "We couldn't put up a site, even though BulkRegister claims we own them." Some of the names sold twice include kids.com, welcome.com and eDiscount.com. (Wired.com 19 Jan 2000)

Category 21.1 *General QA failures*

2000-01-23 **QA quality assurance e-mail**

RISKS 20 75

E-mail program MS-Outlook automatically interprets the string "begin" followed by two spaces as an instruction to interpret all remaining text as an attachment (and thus rendering it invisible). There is no option with which to turn this helpful feature off.

Category 21.1 *General QA failures*

2000-01-26 **privacy violations error quality assurance Web embarrassing**

NewsScan, New York Times http://www.nytimes.com/aponline/f/AP-Internet-Privacy.html

Two companies escaped prosecution by settling with the New York State Attorney General in January. Both companies (Chase Manhattan Bank and InfoBeat) had erroneously revealed private customer data on their Web sites due to bad programming. The Bank compromised data for 18 M credit-card and mortgage holders; the Internet company gave customer e-mail addresses to advertisers by mistake.

Category 21.1 *General QA failures*

2000-02-07 **design boundary conditions quality assurance QA stress testing overload denial of service**

NewsScan;St Petersburg Times (FL) http://www.sptimes.com/, MSNBC http://www.msnbc.com/news/365664.asp

A new Web site promising to give away $10,000 a day in scholarship money to the lucky visitor who wins the luck of the draw [was launched on 3 Feb]. The Cambridge, Mass.-based company FreeScholarships.com is financing its giveaways through marketing groups and advertisers eager to access the teenage and 20-something population. The money is available for college, graduate school, or private school for children, and winners need only be U.S. citizens over the age of 13. Applicants must divulge some amount of demographic data to qualify, and winners are chosen by computer-generated random drawing. The odds of winning depend on how many log on. And for those who don't win? FreeScholarships.com also offers tips on financial aid. (AP/St. Petersburg Times 3 Feb 2000)

FreeScholarships.com found out that handing out money can be harder than it looks sometimes. On [the first day of operation] the site was overwhelmed with visitors trying to register for the tuition giveaway, causing the servers to crash. Technicians were still working on the problem [the next day]. The site, described by its founder as "a low-energy path for people to get a shot at helping them pay for school," plans to give away $10,000 a day to students seeking funds for college, graduate programs, private or parochial school. Additional drawings will give away $25,000 every month and $50,000 each quarter. (MSNBC 4 Feb 2000)

[This case illustrates the critical importance of appropriate design and of stress testing as part of quality assurance.]

Category 21.1 *General QA failures*

2000-02-15 **quality assurance QA bug design**

NewsScan, Los Angeles Times
http://www.latimes.com/business/2000215/t000014636

A computer glitch at the Internal Revenue Service is responsible for rejecting about 40,000 electronically filed returns before the error was discovered and fixed last week. An "error reject code" was triggered when taxpayers sent returns that included a child-care credit or dependent-care benefits. The IRS suggests that the rejected returns be refiled. Congressional guidelines call for 80% of all returns to be filed electronically by 2007. (Los Angeles Times 15 Feb 2000)

Category 21.1 *General QA failures*

2000-02-16 **quality assurance, QA bug government**

NewsScan

Tax preparer H&R Block, which [expected] to use the Internet this season to file the tax returns of 650,000 of its customers, . . . temporarily discontinue[d] online filings until it [determined] how information from a small group of returns was commingled (a mix-up that apparently affected 50 or fewer of a total of 300,000). The company expects to be able to have the problem solved by next week. (AP/USA Today 16 Feb 2000)

Category 21.1 *General QA failures*

2000-02-20 **QA quality assurance browser patch wrong message**

RISKS 20 80

A patch for a security hole in Microsoft's Internet Explorer that would allow a server with an exact filename to retrieve that file without permission from a client's hard disk itself contained a quality assurance flaw. If one attempted to install the patch on IE 4.01 with SP1 (Service Pack 1), the installer stated that the patch was not needed — when in fact it was needed.

Category 21.1 *General QA failures*

2000-02-21 **source code untrusted authors espionage**

RISKS 20 81

According to a 17 Feb 2000 AP item (18 Feb 2000 article in *The Washington Post* by David Ignatius, the US State Department has its shorts in a knot because they have just realized that a software package called the Mission Performance Plan that is running on embassy computers around the world was written by programmers from the former Soviet Union. On 2 Feb 2000, the Department of State sent an urgent cable to 170 embassies ordering them to remove the package by the 7th while security specialists examine the code for trap doors, logic bombs and other cybernasties.

[Comment by MK: this incident reinforces the view that the trustability of software writers is even more important than quality assurance where security is concerned. As many commentators have noted, it may be impossible in practice to apply adequate quality assurance to untrusted code. I have frequently urged QA specialists to ensure that they use code-coverage logging to ensure that every line of code is actually executed during the SQA process; however, even total coverage does not necessarily mean that a program is guaranteed safe, since variable sequence of execution could result in different outcomes for the same subroutines because of data dependencies.]

Category 21.1 *General QA failures*

2000-02-23 **QA quality assurance operating system performance software feature bloat**

RISKS 20 82

RA Downes of Radsoft Laboratories published a blistering denunciation of Microsoft's continuing pattern of making its operating systems less and less efficient. Windows 2000 is even slower than Windows NT, requiring massive upgrades in processor speed, disk space and RAM to achieve equivalent throughput — and this without significant improvements in functionality, according to Downes. Current estimates of error rates at Microsoft are 4 bugs/KLoC (1024 lines of code) — and Windows 2000 is estimated to have around 60M lines of code (implying perhaps 60,000 unidentified errors).

Category 21.1 *General QA failures*

2000-02-28 **quality assurance glitch bug QA broadcast channel pornography**

Reuters

Canadian purveyor of professional wrestling to theaters across Canada mixed up the feed and piped in graphic pornography at the end of a WWF Entertainment show, just as families were leaving. Apparently the action was even tougher than in the ring; "It was very graphic," said Colleen Allen to a Vancouver Province reporter. "My 11-year-old was devastated. . . . Little girls were coming out crying." The company apologized and said they were rewiring their entire switching facility. [Rewiring the facility??]

Category 21.1 *General QA failures*

2000-03-01 **QA quality assurance testing critical systems**

RISKS 20 84

Peter Ladkin of the University of Bielefeld (Germany) analyzed a report on the Wide Area Augmentation System, an adjunct to the Geographical Positioning System that should permit identification of airliners to within 3 meters (instead of today's 100 m) over the continental USA. However, one of the requirements struck experts as grounds for concern: "The probability that a pilot would *not* get a positive warning when WAAS guidance is erroneous for longer than 6.2 seconds must be less than 1 in 10exp7 (units - I presume approaches). This evaluates to one in 47.5 years, apparently. *AvWeek* points out what most safety-critical-system professionals know and others can figure out in a second or two, that confidence to this level can only be achieved by analysis and not by testing."

Category 21.1 *General QA failures*

2000-03-03 **quality assurance QA software bug incompatibility denial of service**

NewsScan

National Discount Brokers, and online brokerage, says the outages it experienced recently were the result of "hacker-like" attacks by an unnamed Web software maker. The company had originally said its problems "had the earmarks of a hacker attack." Apparently, the periodic disruptions were the result of software incompatibility with products made by the outside company that resulted in denial-of-service-type outages. NDB says it's considering whether to pursue "appropriate judicial relief" through legal action against the company. The outages meant that NDB customers had to wait an average of 43.9 seconds to reach its site, twice as slow as the next slowest online trading site, and prevented 200,000 customers from placing stock orders online, although they could still relay orders over the phone. (Reuters/TechWeb 3 Mar 2000)

Category 21.1 *General QA failures*

2000-03-13 **user interface design error judgement QA quality assurance technical support data loss error message**

RISKS 20 84

Dick Karpinski noted in RISKS that some voice-mail systems require the user to press the pound (#) key to save a voice-mail message. Most users assume that hanging up saves the message. Karpinksi correctly noted in an exasperated letter to a manager at Lucent Technologies, "The problem is not even that such messages are unceremoniously dumped. The problem is that the message is lost AND NO ERROR IS INDICATED. A guy can go for months telling people he DID return their voice mail while they tell him they never got it. It wouldn't take a big change to fix the problem, but all the experts chalk up the failures to inadequate training. I chalk it up to a BROKEN user interface that allows slightly forgetful users to go on making mistakes for a long time. This makes the whole organization seem stupid or irresponsible. It may die the death of a thousand cuts. This is not a trivial matter. They are your customers and they deserve better. "

Category 21.1 *General QA failures*

2000-03-21 **vulnerability e-commerce passwords**

RISKS; http://cs.nyu.edu/rubin/passport.html 20 85

Avi Rubin and Dave Kormann published a paper about security holes in Microsoft's Passport protocol; their abstract follows verbatim: Passport is a protocol that enables users to sign onto many different merchants' web pages by authenticating themselves only once to a common server. This is important because users tend to pick poor (guessable) user names and passwords and to repeat them at different sites. Passport is notable as it is being very widely deployed by Microsoft. At the time of this writing [March 2000], Passport boasts 40 million consumers and more than 400 authentications per second on average. We examine the Passport single signon protocol, and identify several risks and attacks. We discuss a flaw that we discovered in the interaction of Passport and Netscape browsers that leaves a user logged in while informing him that he has successfully logged out. Finally, we suggest several areas of improvement.

Category 21.1 *General QA failures*

2000-04-06 **QA quality assurance telephone failure**

RISKS 20

The Australian Telstra company announced on 2000-04-06 that a software failure in its switches was preventing 76,000 subscribers from receiving incoming calls; outbound calls were functioning.

Category 21.1 *General QA failures*

2000-04-18 **QA quality assurance applet**

RISKS 20

Microsoft's Explorapedia v 1.0 shows the Earth rotating the wrong way. [There was no truth to the rumor that Bill Gates had suggested that the planet's rotation be reversed to match his software's description.]

Category 21.1 *General QA failures*

2000-05-26 **elections delay software QA quality assurance**

RISKS 20 89

In Caracas, Venezuela, the High Court delayed general elections at the end of May because of major problems with election software.

Category 21.1 *General QA failures*

2000-06-05 **software bloat QA quality assurance professionalism**

RISKS http://radsoft.net/bloatbusters/sw_dns.htm 20 91

R. A. Downes examined the source code for an old Microsoft registry cleaner called RegMaid. He trimmed the executable from 153,600 bytes down to 83,968 bytes in ten minutes. "Not to beat the dead horse but - just think about it. Ten minutes, 55% savings of 83,968 - and I had never seen this code before in my life." In another bloatware analysis, his team reduced a piece of commercial software from 3.5MB to 7KB (yes, that's seven _kilo_bytes) in a single hour. As Downes wrote, "Avoiding bloat has never been an effort, despite what the defenders of latter-day commercial software like to claim. Things can be done right from the beginning, or even if not, corrected in a negligible envelope of time. . . . It's professional pride on the one side — and `who cares?' on the other."

In a follow-on submission to RISKS, Martin Ward complained about the default handling of inserted images in MS-Word documents: there is no compression unless one takes special measures. As a result, the document ended up at 26 Mb — when simple compression converted it to a mere 180 Kb. Ward summarized two specific design flaws as follows:
* Their image file format doesn't compress images;
* MS Word doesn't compress files when it stores them.

Category 21.1 *General QA failures*

2000-07-28 **QA quality assurance design outsourcing consultants failure delay costs**

RISKS 20 98

Peter G. Neumann summarized a software development disaster: "San Mateo County has spent $35 million thus far on a new Health Services computer system (now two-years old) that was expected to integrate 40 different stovepipe entities that previously were unable to communicate with one another. Over the past few months, the system has been so unreliable that it could not even send out medical bills. The backlog of account receivables is now more than $40 million. Blame is being distributed among poor initial outside advice, a sudden cut in anticipated money, and damaging turnover in consultants. The costs are about double what had been budgeted." Dr Neumann added, "As an aside that seems relevant to many other situations if not to this one, outsourcing of responsibilities (from requirements to design to implementation to operation and maintenance) is increasingly popular, but doomed if you don't have serious in-house competence to understand what is being outsourced."

Category 21.1 *General QA failures*

2000-08-10 **QA quality assurance**

RISKS 21 01

Peter G. Neumann wrote, "After problems with its new computer system, Northeastern University unintentionally admitted 25 percent too many freshmen — 600 extra students — for this fall. Earlier, the names of hundreds of potential applicants had been lost when the system was first installed, which resulted in an aggressive campaign to enroll the students who had been accepted."

Category 21.1 *General QA failures*

2000-08-11 **quality assurance software bugs**

NewsScan, Los Angeles Times
http://www.latimes.com/business/cutting/techwr/20000811/tCB00V0452.html

A project at eBay to improve the online auction company's computer system is being blamed for at least two system problems in the last few days. Unhappy eBay customers have been expressing their frustration on various online message boards. (Los Angeles Times 11 Aug 2000)

Category 21.1 *General QA failures*

2000-08-29 **quality assurance hardware chip design fabrication**

NewsScan, Washington Post http://www.washingtonpost.com/wp-dyn/articles/A40772-2000Aug29.html

Intel is recalling its 1.3 gigahertz Pentium III chip, which it has sold only to "a handful" of "power users" running advanced applications, because a certain combination of data, voltage, and temperature conditions may cause the chip to fail. The chip is expected to be back on the market in a couple of months. (Reuters/Washington Post 29 Aug 2000)

Category 21.1 *General QA failures*

2000-09-20 **QA quality assurance boundary condition inequality operator disjunction design testing Web**

RISKS 21 05

Andrew Koenig reported an interesting boundary-condition problem with some ordering software at an e-commerce site. An Amazon.com e-mail announced a $50 discount on any order of $100 or more from the site in question. However, it was impossible to persuade the order software to accept the special discount for a $100 watch. Solution: a customer-service rep added one penny to the price and succeeded in getting a discounted price of $50.01. The most likely explanation: someone programmed ">$100" for the discount instead of ">=$100." [Moral: follow QA guidelines and test boundary conditions!]

Category 21.1 *General QA failures*

2000-10-19 **QA quality assurance vulnerabilities alerts correction patch**

NewsScan, USA Today http://www.usatoday.com/life/cyber/zd/zd5.htm

The Swedish security firm Defcom is saying that some large companies have been slow in correcting security vulnerabilities they've been warned about. Defcom's chief technology officer says: "We have found vulnerabilities in major operating systems. More than one company hasn't responded with anything... It is quite irresponsible." Recently, the U.S. government's Computer Emergency Response Team (CERT) decided that in future it will give companies no more than 45 days to fix security problems before it publicizes them. (ZDNet/USA Today 19 Oct 2000)

Category 21.1 *General QA failures*

2001-01-02 **Y2K quality assurance bug denial of service**

NewsScan; RISKS 21 18

Y2K BUG BELATEDLY BEDEVILS NORWAY'S TRAINS

The Y2K glitch hit Norway's national railroad company a year later than expected, when none of the company's 16 new airport express trains or 13 high-speed long-distance Signatur trains would start on the morning of Dec. 31. The company performed a quick work-around by resetting the computers to Dec. 1, 2000, and the trains were able to start up on ignition. "We didn't think of trying out the date 31/12/00," says a spokesman for Adtranz, the German producer of the new trains. "Now we have one month to find out what went wrong so we can fix the problem for good." (AP/San Jose Mercury News 1 Jan 2001) http://www0.mercurycenter.com/svtech/news/breaking/ap/docs/797241l.htm

---

Category 21.1 *General QA failures*

2001-01-03 **QA quality assurance Y2K+1 credit card availability**

RISKS 21 18

The national chain of 7-Eleven convenience stores were hit by a belated Y2K bug ("Y2K+1!) when all their credit-card processing software failed on the 1st of January 2001.

Category 21.1 *General QA failures*

2001-01-03 **Y2K+1 QA quality assurance palm computerorganizer**

RISKS 21 18

Philip Berman reported in RISKS that his Sharp YO-550 Electronic Organizer was unable to function correctly with any system date of 2001 or later.

Category 21.1 *General QA failures*

2001-04-16 **quality assurance bug flaw software**

NewsScan

ULTIMATETV USERS ARE BUGGED BY GLITCH
Users of Microsoft's UltimateTV are complaining about a glitch in the system that severely restricts their useable recording time. Subscribers are entitled to as many as 35 hours of digital recording time, but the bug can reduce that time to as little as five hours. Other functions -- including the interactive features and Internet access -- are not affected. Microsoft WebTV Networks acknowledged that a "small number of subscribers" had lost storage space on their systems, and warned users not to press "erase" before pressing "stop" first. "We believe it is a software bug that is exacerbated by some fairly obscure pattern of usage by the subscriber." Meanwhile, the company says a software correction will be distributed directly to the hardware via satellite in the next few months. (Hollywood Reporter 15 Apr 2001)
http://hollywoodreporter.com/hollywoodreporter/convergence/

Category 21.1 *General QA failures*

2001-04-17 **automated loo toilet WC QA quality assurance**

RISKS 21 35

Article by Lester Haines, 17 Apr 2001, quoted in RISKS by Gareth Randell:
<From < http://www.theregister.co.uk/content/28/18312.html >]

A 51-year-old woman was subjected to a harrowing two-hour ordeal [on 16 Apr 2001] when she was imprisoned in a hi-tech public convenience. Maureen Shotton, from Whitley Bay, was captured by the maverick cyberloo during a shopping trip to Newcastle-upon-Tyne. The toilet, which boasts state-of-the-art electronic auto-flush and door sensors, steadfastly refused to release Maureen, and further resisted attempts by passers-by to force the door. Maureen was finally liberated when the fire brigade ripped the roof off the cantankerous crapper. Maureen's terrifying experience confirms that it is a short step from belligerent bogs to Terminator-style cyborgs hunting down and exterminating mankind.

Category 21.1 *General QA failures*

2001-04-25 **QA quality assurance availability real-time process control failure bug design flaw testing**

RISKS 21 36

Peter G. Neumann, moderator of RISKS, reported on quality assurance failures in the Washington Metro: "Washington D.C. Metro's $20 million central computer system crashed at 5:15 p.m. during the evening rush hour on 24 Apr 2001. The central system provides real-time graphics to the downtown control center. Similar malfunctions occurred in 1998 and 1999 (e.g., RISKS-20.60). In the 15 months following its installation, this BDM system crashed 50 times, according to the Metro. Coincidentally, a six-car train that had broken down 8 minutes earlier was stuck in the tunnel between Friendship Heights and Bethesda, and had to be towed out."

Category 21.1 *General QA failures*

2001-08-12 **system failure crash availability communications network phone software error bug flaw QA quality assurance notification**

RISKS 21 60

Andre Oppermann reported from Switzerland on a massive mobile telephone network failure. Writing in RISKS, he summarized the events as follows:

On Friday, July 27th 2001, the whole Swisscom Mobile GSM network, serving 3.3 million customers (70% market share in Switzerland), broke down for 10 hours from approx. 12:30 until 22:30 GMT+0200.

Two independent software errors in the primary and backup network signaling processors (the SS7 network) caused a halt for the processing of all signaling in a GSM network. This includes call setup, call receiving, SMS (short message service), logging onto network and basically everything else. The central GSM systems (HLR, VLR, NMC and so on) stayed up but were unable to communicate with the base stations in the field.

The primary system suffered a complete failure (software error) and as designed the backup system took over. While it was working fine first the backup system got loaded more and more, judging from the description something like a missing free() call, and eventually broke down too half an hour later.

The newspaper "Le Monde" was reporting insider information last week saying that these signaling processors are made by Alcatel and that Alcatel found out about the software errors two weeks before (and probably also had a fix) but "forgot" to inform Swisscom Mobile about it. Alcatel is now facing a Swiss Franc 30 million liability case. This is the loss Swisscom Mobile has because of lost revenues, not including public image damages.

In one thing I have respect for Swisscom; They did a pretty good job with public relations and informed the media and public very openly about their technical problem(s). Now, two weeks later, Swisscom Mobile also issued a, thought written for the non technician but pretty detailed, press release of the cause and events of this network failure.

. . . .

Category 21.1 *General QA failures*

2001-11-06 **QA quality assurance installation format data destruction disk drive underlying assumptions**

RISKS 21 74

A minor programming bug (missing quotation marks) in the new version of the iTunes media player for Macintosh computers resulted in total deletion of all the data on the unfortunate victims' disk drives.

In a later issue of RISKS, a commentator made the point that actually, it wasn't a minor programming bug that caused the error, it was bad quality assurance. Another writer explained the underlying problem: on the Mac, spaces can be used within file names. However, writes the contributor, "With the new Unix-based OSX, long-time mac users are discovering the hard way that spaces are used as delimiters in scripts and in parsing, so filenames containing spaces can have unintended results. Most Unix code samples and docs assume that no one ever puts spaces in their file names, so the samples never show quotes being used, and some docs don't mention this need either. Just about every programmer making the Mac switch from OS 9 to 10 finds this out the hard way, just not as publicly and catastrophically. The risk-- changing the underlying behavior of familiar software, and not being aware of all the assumptions behind that underlying behavior."

Another followup explained that "According to a well-placed friend within Apple, the failure was a bit more complex than described. He says that the bug in the script was actually discovered prior to the software being posted, but that the corrected version somehow did not end up being posted (classic version management issue.) Furthermore, the fact that broken script had been posted was discovered in the middle of the night, but the folks responsible for the server did not pull it down until hours later, thus increasing the collateral damage (classic people management issue.)"

Category 21.1 *General QA failures*

2001-12-04 **data entry keystroke error QA quality assurance bounds checking limits reasonableness check losses stock market trading share price fall**

RISKS 21 81

According to the _Wall Street Journal_, "Dentsu Inc., one of the world's biggest advertising companies, was making its trading debut Friday on the Tokyo Stock Exchange after completing one of the year's biggest initial public offerings -- a deal arranged by UBS Warburg, a unit of Switzerland's UBS AG. . . . Before the Tokyo market opened Friday, a UBS Warburg trader entered what was intended to be an order to sell 16 Dentsu shares at 610,000 yen ($4,924.53) each or above. Instead, the trader keyed in an order to sell 610,000 Dentsu shares at 16 yen apiece. . . . The order was canceled by 9:02 AM, but not before 64,915 shares, almost half of the 135,000 shares in the IPO, had been sold. The price of Dentsu shares, which had been bid up to 600,00 yen before the market opened, fell to 405,000 yen. Now, UBS Warburg is obligated to deliver the shares it sold, and will have to buy them on the open market."

George C. Kaplan, who contributed this item to RISKS, cogently pointed out, "The article doesn't say anything about sanity checks in UBS's trading software. These have their own risks, of course, but you'd think that an error of 4 orders of magnitude in the selling price would at least merit an "Are you sure?" before the order went through. Once again, we see how computers let people make really big mistakes quickly."

Category 21.1 *General QA failures*

2001-12-21 **buffer overflow vulnerability quality assurance remote control penetration**

NewsScan

SECURITY PROBLEMS IN MICROSOFT AND ORACLE SOFTWARE [21 Dec 2001]
Two top companies have issued new statements acknowledging security flaws in their products: Microsoft (Windows XP) and Oracle (the 9i application server, which the company had insisted was "unbreakable." Resulting from a vulnerability called "buffer overflow," both problems could have allowed network vandals to take over a user's computer from a remote location. Microsoft and Oracle have released software patches to close the security holes, and a Microsoft executive says: "Although we've made significant strides in the quality of the software, the software is still being written by people and it's imperfect. There are mistakes. This is a mistake." (San Jose Mercury News 21 Dec 2001)
http://www.siliconvalley.com/docs/news/svfront/secur122101.htm

---

Category 21.1 *General QA failures*

2001-12-26 **QA quality assurance buffer overflow programming flaws language design compiler**

RISKS 21 84

Henry Baker and Peter G. Neumann began a discussion of buffer overflows as a root cause of quality assurance problems world wide. Some highlights from Baker's essay:

* I'm no fan of lawyers or litigation, but it's high time that someone defined "buffer overflow" as being equal to "gross criminal negligence".

* If buffer overflows are ever controlled, it won't be due to mere crashes, but due to their making systems vulnerable to hackers. Software crashes due to mere incompetence apparently don't raise any eyebrows, because no one wants to fault the incompetent programmer (and his incompetent boss). So we have to conjure up "bad guys" as "boogie men" in (hopefully) far-distant lands who "hack our systems", rather than noticing that in pointing one finger at the hacker, we still have three fingers pointed at ourselves.

Highlights from Dr Neumann's response:

* . . . [A]n expressive programming language that prevents you from doing bad things would with very high probability be misused even by very good programmers and especially by programmers who eschew discipline; and use of a badly designed programming language can result in excellent programs if done wisely and carefully.

* . . . [I]t would be very helpful if designers of modern programming languages, operating systems, and application software would more judiciously observe the principles that we have known and loved lo these many years (and that some of us have even practiced!). Take a look at my most recent report, on principles and their potential misapplication, for DARPA's Composable High-Assurance Trustworthy Systems (CHATS) program, now on my Web site:
http://www.csl.sri.com/neumann/chats2.html

[This discussion went on for weeks and can be followed in subsequent issues of RISKS.]

Category 21.1 *General QA failures*

2002-01-04 **QA quality assurance automated teller machines ATM bank data corruption error bug**

RISKS 21 84, 87

Paul van Keep reported to RISKS on a drastic programming error in the Netherlands just as the currency switched to the Euro:

"About 51,000 customers who withdrew money from their ING Bank account on 1 & 2 Jan 2002 (through an ATM) have had the wrong amount debited from their account. The bank hasn't yet given an explanation for the error other than to suspect that it was related to the high stress their systems were under during the first few days of the new year. The amounts debited from customer accounts was a hundred times what they withdrew from the ATMs. This got some people into trouble when their balance went negative and they could no longer use their bank PIN card to pay with in shops. ING Bank corrected the error yesterday."

Category 21.1 *General QA failures*

2002-01-06 **QA quality assurance Euro conversion**

RISKS 21 86

Clive Page told RISKS readers of a serious quality assurance problem in England: "Although the UK is one of the three European Union countries not to have adopted the Euro, many large retailers in the UK announced that they would accept them, but would give change in pounds sterling. Among these was the Debenhams chain of department stores. . . . Robert Sheilds, a 15-year old Luton schoolboy, decided he would like experience of using Euro, so he changed 10 pounds to Euro at a bank, and went on to his local branch of Debenhams to spend them. He found that they had programmed their tills as if there were 1.6 pounds to the Euro rather than 1.6 Euro to the pound, but none of the sales assistants was experienced enough to notice the error. So after his initial purchase, he still had more than 10 pounds in change. He tried to tell the store staff of their mistake, but they said the rate was programmed into the computer, and nobody had the authority to change it. So he carried on spending, and after two hours, ended up with 130 pounds of goods, and 20 pounds in cash. At this point the store manager asked him to leave, saying «I think you've had your fun». Richard then took a train to Bedford (about 20 miles away) to try his luck at another branch, but by this time staff had been alerted, and refused all Euro transactions."

Category 21.1 *General QA failures*

2002-01-10 **QA quality assurance design support flaws features failures incompetence stupidity foolishness crash data corruption**

RISKS 21 86

Rex Black wrote in to RISKS with an off-the-top-of-his-head list of obvious quality assurance and design failures and bloopers from his recent experience. Some key points summarized (not literal quotes) from his list:

* Too many programs are written with no consideration of the possibility of data corruption in their data files. They ought to have recovery capabilities.

* Products are designed so that there are sometimes no error or diagnostic messages at all when they fail.

* Automatic updates of software can sometimes wipe out laboriously constructed configurations, making the updated version useless.

* Long-established problems that are known to technical support fail to make into even the electronic read-me files for their products.

* "The daily (or more often) crash that my Windows Me laptop computer subjects me to, generally without warning, usually losing a good fifteen minutes worth of work. I guess I should learn to save every thirty seconds?"

Mr Black ends with, "If experienced people like me have problems like this, imagine the average computer user who has no idea whatsoever about what is going on when her system screws up. And why should they have to understand a computer to use them? (Don Norman, in his book *The Invisible Computer*, discusses this situation at length.) Ultimately, a computer is a tool, nothing more, nothing less. I think we have a long way to go before we can claim levels of quality consistent with what the makers of almost any other tool could claim."

Category 21.1 *General QA failures*

2002-01-10 **bank interest calculations changes information warfare QA quality assurance design customer relations technical support failure incompetence stupidity obfuscation dolts publicity audit**

RISKS; http://www.mit.edu/people/jik/pfsb_problem/ 21 86

Jonathan Kamens noticed a discrepancy in the interest calculations on his bank account one month as a result of a software upgrade (he was slightly overpaid). It took five months for the bank to explain the difference. In the meantime, Kamens put up a Web site that provided a great deal of embarrassing publicity and even humiliation for the bank officials who had been unable to deal with his simple request. [Moral: in the age of the Web, horrible customer service can cost you much more than the loss of one client's business.]

Category 21.1 *General QA failures*

2002-01-16 **QA quality assurance data input bounds checking limits edits output verification**

RISKS 21 87

Carl Fink contributed this gem to RISKS: "A Georgetown, TX man who had arranged for his water bill to be automatically debited from his bank account alertly noticed that his monthly bill was for over $21,000. (If he hadn't noticed, the debit would have happened, causing him to bounce multiple checks before the error was corrected.) When he told the city of the problem, «They said there was absolutely nothing they could do to stop the automated debit, and it was out of their hands.» Their solution was to send a city employee with a check for $21,000 to reimburse their customer!
http://www.austin360.com/statesman/editions/tuesday/metro_state_1.html

Risks? Lack of sanity checking on a new billing system springs to mind. Lack of any way to correct errors is also quite prominent.

Category 21.1 *General QA failures*

2002-01-19 **QA quality assurance design human error**

RISKS 21 87

Arthur Goldstein reported, "The Chesterfield and North Derbyshire Royal Hospital admitted on 10 Jan that it had mistakenly sent computer generated letters to 30 patients, including six elderly men, telling them they were pregnant. The system operator was blamed for choosing the wrong option (instead of informing them that their operations had been postponed)."

[MK comments: Of course it isn't the operator's fault that there was a glitch; program designers are supposed to take input errors into account and to compensate for them. The designers should have included gender-specificity, age constraints, and so on in their design; e.g., {IF gender = male AND condition = female-specific THEN error}.

MORAL: Use table-driven checks to validate human inputs.]

Category 21.1 General QA failures

2002-02-01 **quality assurance security reliability development Microsoft oxymoron**

NewsScan

GATES REFLECTS ON FUTURE HOPES AND PAST SINS [12 Nov 2001]
Microsoft Chairman Bill Gates says his two top priorities now are improving the reliability of his company's software and conquering the market for "tablet" computers, the laptop-size computers that can be used like a clipboard. The tablets can be written on with a special stylus, and the writing is then treated by Microsoft software as though the words had been typed. Gates says tablet PCs will overtake laptops by 2005. As for software reliability, Gates is repentant: "We're doing a little bit of mea culpa on this. These are areas where Microsoft needs to improve. It affects the way we develop code." (USA Today 12 Nov 2001)
http://www.usatoday.com/life/cyber/tech/review/2001-11-12-comdex-gates.htm

MICROSOFT MAKES SECURITY A TOP PRIORITY [16 Jan 2002]
Microsoft Chairman Bill Gates says it's time to shift away from focusing on features to ensuring more security and privacy. Calling the new initiative "Trustworthy Computing," Gates wrote in an e-mail to employees, "When we face a choice between adding features and resolving security issues, we need to choose security. Our products should emphasize security right out of the box." Gates also emphasized that privacy should be a concern: "Users should be in control of how their data is used. It should be easy for users to specify appropriate use of their information, including controlling the use of e-mail they send." The new focus comes on the heels of a widely publicized security flaw in its flagship Windows XP program. (CNet News.com 16 Jan 2002)
http://news.cnet.com/news/0-1003-200-8509737.html?tag=mn_hd

MICROSOFT HIRES SECURITY SPECIALIST [1 Feb 2002]
Microsoft has hired a top security expert who will oversee the development of company strategies to enhance the security of Microsoft's products, services and infrastructure. Scott Charney, a principal for PricewaterhouseCoopers' Cybercrime Prevention and Response Practice, called his new job "in a word, irresistible." Microsoft CTO Craig Mundie said Charney would be a valuable addition to the company: "As one of the industry's top computer security experts, Scott has wide-ranging experience in cybercrime and computer forensics, which will make him an essential member of Microsoft's Trustworthy Computing leadership team." (AP 1 Feb 2002)
http://apnews.excite.com/article/20020201/D7HD1SFO0.html

Category 21.1 General QA failures

2002-03-11 **real time control system version upgrade failsafe QA quality assurance management**

RISKS 21 94

RISKS moderator Peter G. Neumann summarized a case of inappropriate use of control software coupled with lack of management concern over safety issues in a railway accident in Michigan:

Operating with a less-than-a-year-old remote-controlled system, a runaway train plowed through NIPSCO's Michigan City Generating Station on the morning of 7 Mar 2002, hitting another locomotive before the second locomotive's engineer narrowly jumped to safety. The unmanned eastbound diesel-electric engine, known as Big Blue, was pushing six coal cars when it approached the coal drop-off area at about 30 m.p.h. at 7:15 a.m. However, the train (in excess of 1.5 million pounds, including the coal) did not respond to radio controls and smashed through the enclosed thaw shed and coal rotary dumper, before smashing into the other train, Old No. 12. (Big Blue should have been going only about 1 mph for the last 100 yards entering the dumper.) The impact sent the other train through a fence, uprooted a bumper post, and ripped up track. A spokesman blamed it on a switch malfunction. But the system was supposedly designed so that if the remote-controlled engine receives no signal, its brakes should automatically engage. Employees reportedly said that the system was not designed for the engines currently in use. Two other accidents occurred in the past month. Also noted was what sounds like a serious lack of receptivity from NIPSCO in responding to safety complaints from the workers' union over the past four or five years.

Category 21.1 General QA failures

2002-04-22 **Y2K QA quality assurance repayments accounting errors**

RISKS 22 04

In Brevard County, FL, several city administrations were reeling in shock when they were informed that due to problems during the run-up to the year 2000, they had been significantly overpaid by the County. Some small towns were facing repayments of up to 10% of their annual budget.

Category 21.1 *General QA failures*

2002-05-05 **automated inventory control model overshoot exception QA quality assurance statistical quality control**

RISKS 22 05

Paul Breed told a cute story in RISKS:

>I've been working on an old car, in the process of removing the spot welds I needed a specific sized bullet tipped drill bit. The bit would only last about 5 welds and I had hundreds to do. The only place I could find locally to buy the bits was in a pack of 15 various size bits at the local home center.

So, over the period of three months, I purchased all of their drill sets, every weekend (usually 3 sets). Now I have disassembled the old car and don't need more bits. The last time I was in the home center they had so many of these drill bit sets that they were overflowing on to the floor.

From my experience the computerized inventory system has a delay of about 3 months. It determined that this item sold out for 12 weeks straight, plugged this into it's inventory tracking prediction S/W and ordered hundreds and hundreds of sets.....<

[MK comments: The spike in demand was so unusual it should have triggered a request for a human being to check on whether the automated system really should order so many replacements. Designers of automated systems should program statistical quality-control features into their software.]

Category 21.1 *General QA failures*

2002-05-05 **QA quality assurance billing utility electricity meter computer court disaster response public relations failure**

RISKS 22 05

Some customers of Seattle City Light have been billed up to 10 times the correct amount for their electricity. Although the municipal administration claimed it would adopt the "Nordstrom way" by dealing with billing disputes quickly and in favor of the customers, a spokesperson also said that electric meters don't lie, and thus at least one customer who had protested his bill had to prove that he did not use the power. [MK notes: hellooo? Computers often lie when they are programmed wrong. Claiming that a computer-generated result must be true because the computer says it is reminds one of the touching faith some children have in the Tooth Fairy.]

Category 21.1 *General QA failures*

2002-05-22 **Web design QA quality assurance public relations breach contract fraud misrepresentation bait-and-switch class action lawsuit**

RISKS 22 08

Tudor Bosman reported in RISKS: >Despite its initial denials, Compaq Australia now admits that it did in fact process the payments of customers who bought Presario laptops for just one cent as a result of an online pricing hiccup. [...] Compaq is still adamant, however, that it is not obligated to honor the accidental one-cent pricing, despite mounting industry criticism and ongoing threats of a customer-initiated class action law suit. [...] "As this was a genuine error, Compaq canceled all orders from the system. In instances where 1 cent was debited from customers accounts it will be refunded." <

Category 21.1 *General QA failures*

2002-05-22 **program design QA quality assurance automated dispenser bounds checking violation array initialization price error**

RISKS 22 08ff

Several RISKS correspondents had a feast recounting stories of badly programmed vending machines. In one case, a user could lose money by punching in a choice too quickly after giving the no-armed bandit his dollar; slower-witted customers did fine [MK notes: this is an example of a "race condition" in programming, in which the programmer assumes that certain independ actions will necessarily occur in a strict sequence. The appropriate design is to serialize the components of the transaction; e.g., by using manually-coded semaphores or existing lock routines.] Another case involved unprogrammed values in the selection codes for chocolates; even though the machine typically had only 10 types of candies numbered from 1 to 10, nothing prevented entry of higher values (e.g, 80), and some of these numbers dispensed candybars with very low prices. [MK notes: any bets on the reasons for these bugs? Sure look like omission of bounds-checking (shouldn't accept position numbers higher than what's been filled) coupled with failure to initialize elements of an array (perhaps random values left over from quality assurance testing – if you can call it that in these circumstances).]

Category 21.1 *General QA failures*

2002-05-23 **user interface design failure confusion ergonomics**

RISKS 22 09

Chris Brady continued his analysis of the trouble at Swanwick airport in Britain:

Confusing screens at Swanwick's new air-traffic control centre near Heathrow have resulted in aircraft being directed towards the wrong airports. Controllers have also misread the altitude of aircraft because letters and numbers are difficult to distinguish on the screens, according to the *Daily Mail*, 23 May 2002. For example, the numbers 0, 8 and 6 are confused, leading to mistakes of thousands of feet in the height of flightpaths (noted in a report in *Computer Weekly* magazine).

Controllers and their supervisors at the privatised NATS (National Air Traffic Services) centre at Swanwick have detailed the errors in a health and safety report, which revealed that one controller has repeatedly misread requested flight levels, and mixed up FL360 (36,000 ft) with FL300 (30,000ft).

Others reported difficulties of seeing some letters clearly, particularly the Glasgow code EGPF and the Cardiff code EGFF.

NATS and the CAA (Civil Aviation Authority, U.K.) have said that difficulties in reading screens has been experienced only by a small number of controllers, and that it is not a safety matter. NATS also said that an improved display had been developed and a prototype was shortly to undergo testing.

The risks are many and unfortunately obvious. But what happened to the principles of good HCI design (human-computer interface) and user acceptance testing? Obviously no-one thought to ask the controllers if they could actually read the screens clearly as they play three-dimensional chess with the aircraft and passengers flying into, out of, and past one of the busiest airports in the world.

Category 21.1 *General QA failures*

2002-05-23 **air-traffic control system failure crash availability upgrade maintenance disruption real-time**

RISKS 22 09

Chris Brady reported in RISKS:

Yet again the new multi-million-pound air-traffic computer system at Swanwick near Heathrow crashed last Friday (May 17, 2002) shortly after 6.30 am.

This is a time of maximum inbound flights from the Middle and Far East -- with full 747's arriving at one a minute. Also too it is just when the morning rush hour for domestic and European departures and arrivals begins to build up.

The crash was the result of a 'routine upgrade' which made half the air traffic controllers' computer screens inoperable. This meant that only half the normal flights could be handled. This meant that airlines had to cancel most of their flights into and out of Heathrow - a situation which lasted for most of the day. Imagine one flight being canceled and all the disruption that can cause, then multiply that by many hundreds. And the knock on effect of the wrong planes and crews in the wrong places at the wrong times lasted for most of the following weekend. The consequent loss of revenue to the struggling airline industry is inestimable, to say nothing of the increased loss of confidence in the safety of flying amongst the traveling public.

The risks are obvious. The new computer system at Swanwick is a disaster waiting to happen. A 'routine upgrade' should not result in a major loss of service. The upgrade was obviously made to the primary system before testing on any back up system (is there one?), and if a routine upgrade can cause such a system loss then what would happen to a major upgrade?

Confidence in the safety of the ATC system at Heathrow is not increased with the U.K. Government's refusal to financially bale out - yet again - to the tune of millions of pounds - the owners of the new system, the privatised NATS (National Air Traffic Services).

Category 21.1 *General QA failures*

2002-06-27 **documentation assumption error training awareness error**

RISKS 22 13

Steve Bellovin summarized an unfortunate case of dependence on the wrong assumption when operating a computer-controlled military device:

According to a U.S. Army report, a software problem contributed to the deaths of two soldiers in a training accident at Fort Drum. They were firing artillery shells, and were relying on the output of the Advanced Field Artillery Tactical Data System. But if you forget to enter the target's altitude, the system assumes a default of 0. (A Web site I found indicates that (part of) Ft. Drum is at 679 feet above sea level.) The report goes on to warn that soldiers should not depend exclusively on this one system, and should use other computers or manual calculations.

Other factors in the incident include the state of training of some of the personnel doing the firing. [Source: AP]

Category 21.1 *General QA failures*

2003-02-21 **Oracle server new vulnerabilities exploit software CERT CC advisory**

NIPC/DHS

February 19, CERT/CC — CERT Advisory CA-2003-05 Multiple Vulnerabilities in Oracle Servers.

Multiple vulnerabilities exist in Oracle software. Depending on the vulnerability being exploited, an attacker may be able to execute arbitrary code; read, modify, or delete information stored in underlying Oracle databases; or cause a denial of service. Systems running the following software are affected: Oracle9i Database (Release 1 and 2); Oracle8i Database v 8.1.7; Oracle8 Database v 8.0.6; and Oracle9i Application Server (Release 9.0.2 and 9.0.3). Solutions for specific vulnerabilities can be found in Oracle Security Alerts published here:
http://otn.oracle.com/deploy/security/alerts.htm. Systems administrators should review the Oracle Security Alerts and apply patches as appropriate. Until a patch can be applied, the CERT/CC recommends that vulnerable sites disable unnecessary Oracle services, run Oracle services with the least privilege, and restrict network access to Oracle services.

Category 21.1 *General QA failures*

2003-02-28 **QA quality assurance blooper**

NewsScan

WELCOME TO CORNELL. (NO, WAIT — NOT SO FAST THERE!)
Because of a "systems coding error," Cornell University sent welcoming e-mail letters to hundreds of high school students who'd already been rejected. A few hours after the university congratulated the students on their acceptance, it had to send them letters confessing its mistake and apologizing. One high school counselor said, "I know mistakes can happen, but this kind is devastating to the student and family. The apologies of the university don't quite cover the disappointment of my senior." (New York Times 28 Feb 2003)

Category 21.1 *General QA failures*

2003-03-12 **new vulnerability PeopleSoft business software flaw exploit Web server compromise**

NIPC/DHS

March 10, CNET News — Security alert posted for PeopleSoft.

A serious security flaw has been found in business management software from PeopleSoft. The flaw, known as a remote command execution vulnerability, gives outsiders the ability to install malicious computer code on PeopleSoft customers' Web servers, potentially leading to a "complete compromise" of their PeopleSoft business systems, according to Internet Security Systems (ISS), the Atlanta-based computer security company that issued the warning on Monday. PeopleSoft supplies software designed to streamline accounting, human resources, sales and manufacturing activities to more than 5,000 companies around the world. The flaw affects only certain releases of PeopleSoft version 8, which the company began shipping in 2000. Nearly 2,000 companies have installed version 8, according to PeopleSoft spokesman Steve Swasey. The patches and details about the vulnerability are available on the company's private Web site for PeopleSoft customers: www.peoplesoft.com. PeopleSoft has yet to hear of any problems related to the security flaw, Swasey added.

Category 21.1 *General QA failures*

2003-03-20 **new advisory CERT CC integer overflow Sun RPC XDR**

NIPC/DHS

March 19, CERT/CC — CERT Advisory CA-2003-10: Integer overflow in Sun RPC XDR library routines.

XDR (external data representation) libraries are used to provide platform-independent methods for sending data from one system process to another, typically over a network connection. The xdrmem_getbytes() function in the XDR library provided by Sun Microsystems contains an integer overflow that can lead to improperly sized dynamic memory allocation. Depending on how and where the vulnerable xdrmem_getbytes() function is used, subsequent problems like buffer overflows may result. Exploiting this vulnerability will lead to denial of service, execution of arbitrary code, or the disclosure of sensitive information. Specific impacts reported include the ability to crash the rpcbind service and possibly execute arbitrary code with root privileges. In addition, intruders may be able to crash the MIT KRB5 kadmind or cause it to leak sensitive information, such as secret keys. CERT recommends the application of a vendor specified patch or upgrade as specified by vendor.

Category 21.1 *General QA failures*

2003-03-24 **Yahoo security obscurity obfuscation Website open access**

NIPC/DHS

March 19, SecurityFocus — Point, click, get root on Yahoo.

A simple scan for unpublished websites within Yahoo's Internet address space gave an unemployed IT worker access to several of the portal company's internal systems, including root access inside the company firewall, the worker says. Yahoo URLs provided by the man routed to what appeared to be two unprotected Web-based remote administration consoles for company disk and file storage systems. In a written statement, Yahoo spokesperson Mary Osako acknowledged that the servers shouldn't have been exposed to the Internet, and said the company closed off access on Wednesday. "No user data was compromised," Osako wrote. The IT worker, who asked to remain anonymous, confirmed Yahoo's statement.

Category 21.1 *General QA failures*

2003-03-26 **CERT CC advisory vulnerabilities Lotus Notes Domino software servers**

NIPC/DHS

March 26, CERT/CC — CERT Advisory CA-2003-11: Multiple Vulnerabilities in Lotus Notes and Domino.

In February 2003, NGS Software released several advisories detailing vulnerabilities affecting Lotus Notes clients and Domino servers. Multiple reporters, the close timing, and some ambiguity caused confusion about what releases are vulnerable. The impact of these vulnerabilities range from denial of service to data corruption and the potential to execute arbitrary code. The CERT/CC has issued an advisory to help clarify the details of the vulnerabilities, the versions affected, and the patches that resolve these issues. Please refer to the CERT website for additional information.

Category 21.1 *General QA failures*

2003-04-17 **quality assurance failure flaw bug Microsoft MS Office 200 register software**

NIPC/DHS

April 17, CNET News.com — Flaw bugs Office 2000 customers.

A software slipup in Microsoft's latest update to Office 2000 results in the application repeatedly asking some customers to register the program. The glitch apparently affects only Office 2000 users who don't have administrative rights on their computer, a Microsoft representative said Thursday. "They are experiencing unexpected registration prompts, but it doesn't interfere with product functionality," he said. Administrative rights allow a PC user to exercise total control over the computer's data. Giving such rights to nontechnical employees is considered by many security experts to be an unacceptable risk for companies. Microsoft's representative didn't know if the cause of the problem had been determined but said that the software company is working on fixing the issue.

Category 21.1 *General QA failures*

2003-04-22 **bug patch flaw fix Microsoft MS Office 2000 quality assurance failure**

NIPC/DHS

April 22, The Register — Microsoft issues Office 2000 registration bug patch.

Microsoft has posted a patch to remedy the registration bug that has plagued Office 2000 users in some of the world's biggest organizations since April 15. The bug invokes Office's Registration Wizard, even if the user has already registered the product, typically through the purchase of a Select Customer volume license. In many cases, the bug is merely annoying, forcing the user to get rid of an unwanted window. In some cases, dismiss the window too often and Office ceases to function, or enters what Microsoft calls "Reduced Functionality Mode". The only way to get it back is to register the software with Microsoft. The patch may be found on the Microsoft Website:
http://support.microsoft.com/?id=818798

Category 21.1 *General QA failures*

2003-04-27 **quality assurance failure bug software flaw expenses software engineering SEI**

NIPC/DHS

April 27, The Associated Press — Spread of buggy software raises questions.

Last year, a study commissioned by the National Institute of Standards and Technology found that software errors cost the U.S. economy about $59.5 billion annually. Developers say defects stem from several sources: software complexity, commercial pressure to bring products out quickly, the industry's lack of liability for defects, and poor work methods. Programmers typically spend half their time writing code and the other half looking for errors and fixing them. That approach may have worked in the infancy of computers, when programs were small, says Watts Humphrey, of Carnegie Mellon University's Software Engineering Institute. Now, most programs in testing have five to 10 defects per 1,000 lines of code, or up to 10,000 bugs in a million-line program. It would take 50 people a year to find all those bugs, Humphrey says.

Category 21.1 *General QA failures*

2003-04-29 **Oracle9i vulnerability operating system compromise buffer overflow patch databases link**

NIPC/DHS

April 29, eWEEK — Vulnerability puts Oracle9i at risk.

A new vulnerability in Oracle Corp.'s database software puts not only the information in the database at risk, but in some cases, also can lead to a compromise of the operating system. The vulnerability is in the service that enables users to create links between two Oracle databases. In order to exploit the flaw, an attacker would need to send an overly long parameter with the connect string with a query to create a database link. This would trigger the stack buffer overflow, which would in turn overwrite the saved return address on the stack. This would give the attacker the ability to run any code he chose on the vulnerable server. The vulnerability affects Oracle 9i Release 1 and 2; all releases of 8i; all releases of 8; and 7.3.x. A patch is available at the Oracle website:
http://otn.oracle.com/deploy/security/pdf/2003alert54.pdf.

Category 21.1 *General QA failures*

2003-05-02 **Outlook 2003 microsoft beta version bug 21 steps offline folder Government Computer News**

NIPC/DHS

May 02, Government Computer News — Bug delays Outlook 2003's release.

A bug lives on in the latest beta version of Microsoft Outlook 2003 despite two widely publicized fixes. The Inbox bug systematically deletes e-mail messages throughout networked systems that still have Outlook 2002 installed. One workaround proposed by Microsoft involves 21 steps to redirect the location of the cache and change the location of the default profile's Offline Folder File. That didn't work in tests conducted by Government Computer News. Another workaround, which also didn't fix the Outlook bug, is to back up all user data on the server running Microsoft Exchange Server and then delete and recreate the Outlook Profiles. Backup is necessary because this procedure deletes calendar data, e-mails and so on. Microsoft has delayed final product release from early summer to late summer or early fall.

Category 21.1 *General QA failures*

2003-05-05 **Connectiva vulnerabilities Linux arbitrary code DoS denial of service Apache Web Server GNU C**

NIPC/DHS

May 05, Information Security — Multiple vulnerabilities in Conectiva implementations.

Conectiva, a vendor of Portuguese, Spanish and English versions of Linux, has released updates to correct several vulnerabilities in its implementations. These could allow an attacker to run arbitrary code, cause denial of service or crash applications. A vulnerability in glibc, a GNU C Library could be used by an attacker to create an overflow problem in the xdrmem family of functions to run arbitrary code or crash applications. Another pair of vulnerabilities involves the Apache Web server. A memory leak could allow an attacker to deplete memory and cause a denial of service. There are also file descriptor leaks that could give privileges to untrusted CGI scripts. Updated versions are available from the Conectiva website:
http://distro.conectiva.com.br/atualizacoes

Category 21.1 *General QA failures*

2003-06-25 **MS03-021 windows media player library access 9 ActiveX control script flaw**

NIPC/DHS

June 25, Microsoft — Microsoft Security Bulletin MS03-021: Flaw In Windows Media Player May Allow Media Library Access.

A flaw exists in the way in which the ActiveX control included with Windows Media Player 9 Series provides access to information on the user's computer. An attacker could invoke the ActiveX control from script code, which would allow the attacker to view and manipulate metadata contained in the media library on the user's computer. An attacker could also embed a link to a malicious site in an HTML e-mail and send it to the user. After opening the e-mail, the site could be visited automatically without further user interaction. The attacker might also be able to determine the user name of the logged-on user by examining the directory paths to media files. Microsoft has assigned a risk rating of "Moderate" to this issue and recommends that system administrators install the patch on a schedule consistent with their practices.

Category 21.1 *General QA failures*

2003-08-21 **Orcale9iM XDB flaw open door hackers XML Database denial service DoS vulnerability insider FTP HTTP server buffer overflow**

NIPC/DHS

August 21, eWEEK — Oracle XDB flaws open door for hackers.

The XDB (XML Database) in Oracle Corp.'s Oracle9i Database Release 2 has a set of potential buffer overflows that a smart attacker could exploit to cause a denial-of-service (DoS) attack or to capture an active user session on Oracle9iM. To exploit the weaknesses, an authenticated database user is required, or the FTP and HTTP servers must be enabled in the XML database. The vulnerabilities are "highly susceptible" to an insider attack that originates on a corporate intranet if users ignore best practices for secure database configuration. To minimize risk, Oracle recommends disabling the FTP and HTTP servers in the XML database. Those are both installed and enabled by default and can't be turned on or off individually. A patch is available on the Oracle Website:
http://metalink.oracle.com/

Category 21.1 *General QA failures*

2003-09-03 **MS03-037 flaw Visual Basic Applications Arbitrary Code Execution VBA documents e-mail attachemnt forward**

NIPC/DHS

September 03, Microsoft — Microsoft Security Bulletin MS03-037: Flaw in Visual Basic for Applications Could Allow Arbitrary Code Execution.

A flaw exists in the way Microsoft VBA checks document properties passed to it when a document is opened by the host application. A buffer overrun exists which if exploited successfully could allow an attacker to execute code of their choice in the context of the logged on user. In order for an attack to be successful, a user would have to open a specially crafted document sent to them by an attacker. This document could be any type of document that supports VBA, such as a Word document, Excel spreadsheet, PowerPoint presentation. In the case where Microsoft Word is being used as the HTML e-mail editor for Microsoft Outlook, this document could be an e-mail, however the user would need to reply to, or forward the mail message in order for the vulnerability to be exploited. Microsoft has assigned a rating of "Critical" to this vulnerability and recommends that system administrators install the patch at the earliest available opportunity.

Category 21.1 *General QA failures*

2003-09-03 **MS03-036 code execution execute wordperfect converter corel malicious code buffer overrun**

NIPC/DHS

September 03, Microsoft — Microsoft Security Bulletin MS03-036: Buffer Overrun in WordPerfect Converter Could Allow Code Execution.

There is a flaw in the way that the Microsoft WordPerfect converter handles Corel WordPerfect documents. A security vulnerability results because the converter does not correctly validate certain parameters when it opens a WordPerfect document, which results in an unchecked buffer. As a result, an attacker could craft a malicious WordPerfect document that could allow code of their choice to be executed if an application that used the WordPerfect converter opened the document. Microsoft Word and Microsoft PowerPoint, FrontPage, Publisher, and Microsoft Works Suite can all use the Microsoft Office WordPerfect converter. The vulnerability could only be exploited by an attacker who persuaded a user to open a malicious WordPerfect document-there is no way for an attacker to force a malicious document to be opened or to trigger an attack automatically by sending an e-mail message. Microsoft has assigned a risk rating of "Important" to this vulnerability and recommends that system administrators install the patch at their earliest opportunity.

Category 21.1 *General QA failures*

2003-09-03 **MS03-035 Microsoft Word Macros Automatically Run malicious document e-mail attachment**

NIPC/DHS

September 03, Microsoft — Microsoft Security Bulletin MS03-035: Flaw in Microsoft Word Could Enable Macros to Run Automatically.

A vulnerability exists because it is possible for an attacker to craft a malicious document that will bypass the macro security model. If the document was opened, this flaw could allow a malicious macro embedded in the document to be executed automatically, regardless of the level at which macro security is set. The malicious macro could take the same actions that the user had permissions to carry out, such as adding, changing or deleting data or files, communicating with a web site or formatting the hard drive. The vulnerability could only be exploited by an attacker who persuaded a user to open a malicious document -there is no way for an attacker to force a malicious document to be opened. The vulnerability cannot be exploited automatically through e-mail. A user must open an attachment sent in e-mail for an e-mail borne attack to be successful. The vulnerability only affects Microsoft Word—other members of the Office product family are not affected. Microsoft has assigned a risk rating of "Important" to this vulnerability and recommends that system administrators install the patch immediately.

Category 21.1 *General QA failures*

2003-09-03 **MS03-038 Microsoft Access Snapshot Viewer Code Execution Execute malicious website visit Office**

NIPC/DHS

September 03, Microsoft — Microsoft Security Bulletin MS03-038: Unchecked buffer in Microsoft Access Snapshot Viewer Could Allow Code Execution.

A vulnerability exists because of a flaw in the way that Microsoft Access Snapshot Viewer validates parameters. Because the parameters are not correctly checked, a buffer overrun can occur, which could allow an attacker to execute the code of their choice in the security context of the logged-on user. For an attack to be successful, an attacker would have to persuade a user to visit a malicious Web site that is under the attacker's control. The Microsoft Access Snapshot Viewer is not installed with Microsoft Office by default. Microsoft has assigned a rating of "Moderate" to this vulnerability and recommends that system administrators install the patch at the earliest available opportunity.

Category 21.1 *General QA failures*

2003-11-06 **critical fix patch update Microsoft MS Office 2003**

NIPC/DHS

November 05, eSecurity Planet — 'Critical' Office 2003 patch released.

Microsoft has issued a 'critical' update to fix problems in the Powerpoint, Word and Excel products in Microsoft Office 2003, which was released on October 21. Microsoft said the errors occur when a user tries to open or save files that includes an OfficeArt shape that was previously modified or saved in an earlier version of Microsoft Office. The errors mean that documents may not open completely or may be corrupted. In some cases, the documents may open but with missing content. There is no word on whether the 'critical' patch will be shipped with all new sales of the Office 2003 suite going forward. The update is available on the Microsoft Website:
http://support.microsoft.com/?kbid=828041

Category 21.1 *General QA failures*

2003-11-07 **software error medical tests wrong treament computer always right**

RISKS 23 19

CANADIAN MEDICAL EQUIPMENT GIVES REVERSED DIAGNOSTIC RESULTS

[Peter Neumann summarized a report from Danny Burstein on a medical testing equipment failure that illustrates a common failing among computer users: not using common sense.]

About 3,000 people got opposite results when they were tested for gonorrhea and chlamydia over an 18-month period. Because of a faulty diagnostic machine in Cranbrook (southeastern British Columbia), positive and negative test results for the two sexually transmitted diseases were reversed.

About 3,000 people were tested. The 83 that were positive were incorrectly told they were clean. The 2,900 or so that were negative were told they were positive and were given the standard treatments. From a health standpoint the 83 sick folks come out the worst, because their treatment was delayed for months or years. But even the folk who were well went through the drug protocols and other exams and treatments -- which have their own secondary effects, plus, of course, the social/inter-personal problems which being (mis)diagnosed with an STD will cause, especially with regard to patient partner tracking.

One Would Have Thought that someone in the medical office or the lab or the insurance or the pharmacy or somewhere…, looking at 3,000 test results, would have quickly noticed that instead of finding a positive rate of 3% these tests were coming back at 97%. One would Also Have Thought that enough of these people would have gotten a second set of tests so as to raise eyebrows a lot earlier.

Category 21.1 *General QA failures*

2003-11-13 **new critical vulnerability Microsoft security bulletin buffer overflow overrun patch fix exploit**

NIPC/DHS

November 13, Microsoft — Microsoft Security Bulletin MS03-051: Buffer Overrun in Microsoft FrontPage Server Extensions Could Allow Code Execution.

There are two vulnerabilities in Microsoft FrontPage Server Extensions. The first vulnerability exists because of a buffer overrun in the remote debug functionality of FrontPage Server Extensions. This functionality enables users to remotely connect to a server running FrontPage Server Extensions and remotely debug content using, for example, Visual Interdev. An attacker who successfully exploited this vulnerability could be able to run code with Local System privileges on an affected system, or could cause FrontPage Server Extensions to fail. The attacker could then take any action on the system. The second vulnerability is a Denial of Service vulnerability that exists in the SmartHTML interpreter. This functionality is made up of a variety of dynamic link library files, and exists to support certain types of dynamic web content. An attacker who successfully exploited this vulnerability could cause a server running Front Page Server Extensions to temporarily stop responding to requests. Microsoft has assigned a risk rating of "Critical" to this issue and recommends that system administrators install the patch immediately.

Category 21.1 *General QA failures*

2003-11-13 **new critical vulnerability Microsoft security bulletin Word Excel arbitrary code execution patch fix exploit**

NIPC/DHS

November 11, Microsoft — Microsoft Security Bulletin MS03-050: Vulnerability in Microsoft Word and Microsoft Excel Could Allow Arbitrary Code to Run.

A vulnerability exists in Microsoft Excel that could allow malicious code execution. If successfully exploited, an attacker could craft a malicious file that could bypass the macro security model. If an affected spreadsheet was opened, this vulnerability could allow a malicious macro embedded in the file to be executed automatically, regardless of the level at which the macro security is set. The malicious macro could then take the same actions that the user had permissions to carry out. A vulnerability exists in Microsoft Word that could allow malicious code execution. If a specially crafted document were to be opened it could overflow a data value in Word and allow arbitrary code to be executed. If successfully exploited, an attacker could then take the same actions as the user had permissions to carry out. Microsoft has assigned a risk rating of "Important" to this issue and recommends that system administrators install this patch immediately.

Category 21.1 *General QA failures*

2003-12-09 **Oracle new critical vulnerability warning OpenSSL denial-of-service**

NIPC/DHS

December 05, eWEEK — Oracle issues high-severity vulnerability warning.

Oracle issued a high severity security alert warning Thursday, December 4, confirming that a variety of its server products could be tampered with through vulnerabilities via the OpenSSL protocol. The flaws could potentially open the door for a remote hacker to cause a denial-of-service (DoS) attack, execute arbitrary code, and gain access privileges. The notification addresses SSL vulnerabilities detailed in CERT Advisory CA-2003-26 and SSL vulnerabilities detailed in several older Common Vulnerabilities and Exposures (CVE) Candidates. Products concerned with the vulnerability include certain releases of Oracle9i Database Server, Oracle8i Database Server, Oracle9i Application Server, and Oracle HTTP Server. Additional information is available on Oracle's Website:
http://otn.oracle.com/deploy/security/pdf/2003alert62.pdf

Category 21.1 *General QA failures*

2003-12-24 **MySQL release bug fix patch open-source database software**

NIPC/DHS

December 22, eWEEK — MySQL Quashes Defects in Database Release. MySQL AB on Monday, December 22, released Version 4.0.17 of its MySQL open-source database software. The update features a number of cleaned up code defects. Available in source code and binary form, the MySQL 4.0.17 maintenance release for the current MySQL production version corrects all valid bugs discovered during an October poll conducted within the development community via an independent study. According to the study, 21 software defects in 235,667 lines of MySQL source code were found. The report's Defect Summary noted 15 defect instances of NULL Pointer Deference, three defect instances of an allocated memory leak, and three defect instances of an uninitialized variable prior to usage. Additional information is available on the MySQL Website:
http://www.mysql.com/downloads/mysql-4.0.html

Category 21.1 *General QA failures*

2004-01-05 **QA quality assurance failure car registration computer always right**

RISKS 23 11

INPUT DATA ERROR ON TAG TRANSFER CAUSES DRIVER'S ARREST

Stanley Klein reported in risks that a data entry error in processing a Maryland driver's car registration resulted in her arrest when computer systems deleted her records instead of transferring her registration to her new car.

Category 21.1 *General QA failures*

2004-01-05 **time_t 32-bit time software programs computers**

RISKS 23 12

HAPPY 2**30'TH BIRTHDAY, TIME_T!

Contributor Paul Eggert writes about the POSIX time counter time_t reaching half its positive range on January 9, 2004. The 32-bit counter counts seconds elapsed since 1970. Some products by Parametric Technology Corp. which were using time_t for keeping time needed patching because of the time_t half-time milestone. Eggert wonders how many applications will break when time_t finally overflows in January 2038. Contributor Paul E. Black reports an overflow bug in Moscow ML, a higher order logic system, caused by time_t's birthday. The maintainers of Moscow ML issued patches within a few days of the bug being discovered. In another follow-up article, Ed Ravin reports failure of the Heimdal implementation of Kerberos because of the time_t birthday. Ravin's company was able to work around this failure by upgrading to a newer version of Heimdal, which had the bug fixed.

Category 21.1 *General QA failures*

2004-01-14 **Microsoft security bulletin patch flaw vulnerability fix buffer overflow overrun**

NIPC/DHS;
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS04−003.asp

January 13, Microsoft — Microsoft Security Bulletin MS04-003: Buffer Overrun in MDAC Function Could Allow Code Execution (832483).

Microsoft Data Access Components (MDAC) is a collection of components that provides the underlying functionality for a number of database operations. When a client system on a network tries to see a list of computers that are running SQL Server and that reside on the network, it sends a broadcast request to all the devices that are on the network. Because of a vulnerability in a specific MDAC component, an attacker could respond to this request with a specially-crafted packet that could cause a buffer overflow. An attacker who successfully exploited this vulnerability could gain the same level of privileges over the system as the program that initiated the broadcast request. For an attack to be successful an attacker would have to simulate a SQL server that is on the same IP subnet as the target system. A target system must initiate such a broadcast request to be vulnerable to an attack. An attacker would have no way of launching this first step but would have to wait for anyone to enumerate computers that are running SQL Server on the same subnet. Also, a system is not vulnerable by having these SQL management tools installed. Code executed on the client system would only run under the privileges of the client program that made the broadcast request. Microsoft has assigned a severity rating of "Important" to this issue.

Category 21.1 *General QA failures*

2004-02-08 **design flaw data overrun field short digits quality assurance failure QA**

RISKS; http://www.haaretzdaily.com/hasen/spages/392009.html 23 21

FIXED-LENGTH FIELDS STRIKE AGAIN

Robert Israel reports on a design failure: >…the Israel Defense Forces will have to pay tens of millions of shekels to fix a two-year-old automated system for calling up reservists: the system allocates 9 digits for a reservist's cell-phone number, but in a few months all Israeli cell phones will have 10 digits. According to the article, "The army will also look into expanding the fields for personal and other telephone numbers to prevent future problems."<

Category 21.1 *General QA failures*

2004-02-11 **power outage software flaw vulnerability General Electric GE software energy management US blackout**

RISKS 23 18

SOFTWARE BUG CONTRIBUTED TO BLACKOUT

Contributor Kevin L. Poulsen writes that a bug in General Electric (GE) energy management system XA/21 might have contributed to the August 14, 2003 northeastern US power blackout. The flaw was discovered from an in-depth software audit following the blackout. A spokesman for Ohio-based FirstEnergy Corp., where the investigation into the blackout began, said: "It [the software flaw] had never evidenced itself until that day…" The North American Electric Reliability Council (NERC)--the organization responsible for preventing blackouts in the US and Canada--asked FirstEnergy to thoroughly patch its XA/21 by June 30, 2004. NERC would start asking all electric companies in North America to patch their XA/21s in March 2004.

Category 21.1 *General QA failures*

2004-02-25 **quality assurance QA failure design problems toll system highway German autobahn**

RISKS 23 21

TOLL COLLECT CONSORTIUM FAILS TO DELIVER

Peter Ladkin provided a detailed report on the failure of a major industrial consortium to furnish the toll collection system for the German Autobahn network. Part of the problem may be traced to the unrealistic development schedule foisted on the winners of the Call for Proposals by government agencies. There were apparently also major design flaws such as inadequate interfacing with debit cards or the accounting systems used by major trucking firms. Losses are estimated in the billions of Euros.

Category 21.1 *General QA failures*

2004-02-27 **heart monitor scanner physical reconfiguration design flaw**

RISKS 23 22

PACEMAKER REQUIRES OPERATION FOR RECONFIGURATION

Nigel Metheringham noted in RISKS that a child was at risk of having an operation to replace a cardiac pacemaker so that a new monitor could be used after his original monitor was stolen. "The idea of an implantable medical device apparently requiring physical reconfiguration (at least) to talk to an external monitor implies a level of trust in the reliability of the external device which is seriously scary."

However, Dave Brunberg retorted in RISKS 23.24, "I think the RISKS of allowing unauthenticated remote reprogrammability of an implanted medical device may be just as scary. One way of reducing that RISK may be to have some sort of an "emergency broadcast" safe mode in which a new external monitor could identify itself to the implant and authorize through a highly secure key which would require knowledge of a passphrase to transmit. Of course, you'd really have to remember to change the default password…."

Category 21.1 *General QA failures*

2004-03-02 **security vulnerability flaw hole patch fix WinZip MIME**

DHS IAIP Daily; http://www.eweek.com/article2/0,4149,1540280,00.asp

February 27, eWEEK — Vulnerability in WinZip could compromise security.

Security analysts on Friday, February 27, reported that versions of the popular ZIP file management program WinZip have a serious security flaw. According to iDefense Inc., an error in the parameter parsing code in these versions "allows remote attackers to execute arbitrary code." The attacker would have to construct a specially designed MIME archive (with one of .mim, .uue, .uu, .b64, .bhx, .hqx and .xxe extensions) and distribute the file to users. Once opened, the attack would trick WinZip into executing code contained in the attacking file. iDefense said it had a functioning proof-of-concept attack demonstrating the problem. The malicious file could be distributed by e-mail, on a Web page, or through peer-to-peer networks. According to iDefense, versions 7 and 8, as well as the latest beta of WinZip 9 are vulnerable to this attack. However, the released Version 9 of WinZip is not vulnerable. In addition to upgrading, users can prevent an attack by turning off automatic handling of these file types by WinZip in Windows Explorer.

Category 21.1 *General QA failures*

2004-03-31 **new security vulnerability flaw hole buffer overflow exploit patch fix RealNetworks**

DHS IAIP Daily; http://service.real.com/help/faq/security/security022604.html

March 26, eSecurity Planet — RealNetworks confirms buffer overflow problem.

Digital media delivery firm RealNetworks confirmed a buffer overflow vulnerability in its Helix Universal Server product, warning that a root exploit could give an attacker "inappropriate access" to compromised system. RealNetworks first warned of the flaw in January, describing it as a simple denial-of-service issue, but on Friday, March 26, the company released an updated advisory Friday to confirm the existence of a "potential root exploit." A root exploit could give an attacker complete control over a susceptible machine to execute malicious code. On Windows platforms where the Helix Server is run as an NT Service, the bug could allow arbitrary code execution under the context of the NT SYSTEM account. Vulnerable products includes Real's Helix Universal Mobile Server & Gateway 10, version 10.1.1.120 and prior and the Helix Universal Server and Gateway 9, version 9.0.2.881 and prior. RealNetworks has released an updated version of the Helix Universal Server or Gateway: http://service.real.com/help/faq/security/security022604.htm l

---

Category 21.1 General QA failures

2004-05-19 **open source code repository flaw vulnerability**

DHS IAIP Daily; http://news.com.com/Flaws+found+in+manager+apps/2100−1002_3− 5216353.html?tag=nefd.lede

May 19, CNET News.com — Flaws drill holes in open-source repository.

Flaws in two popular source code repository applications could allow attackers to access and corrupt open-source software projects, a security researcher said Wednesday, May 19. One vulnerability affects the Concurrent Versions System (CVS), an application used by many developers to store program code. The other flaw affects a system known as Subversion, said Stefan Esser, the researcher who discovered the security holes. The flaw in CVS, which is used more widely than Subversion, affects all versions of the software released before May 19, according to Esser. The vulnerability, technically known as a "heap overflow," occurs because data from the system's users is not vetted carefully enough. The CVS Project and major Linux and BSD distributions have posted advisories on the issue. The hole in Subversion is caused by an error in the way the code parses dates. It could be exploited to allow "remote code execution on Subversion servers and therefore could lead to a repository compromise," according to Esser's advisory.

Category 21.1 General QA failures

2004-05-26 **vulnerability CVS buffer overflow concurrent version system**

DHS IAIP Daily; http://www.us−cert.gov/cas/techalerts/TA04−147A.html

May 26, US-CERT — Technical Cyber Security Alert TA04-147A: CVS Heap Overflow Vulnerability.

There is a heap memory overflow vulnerability in the way CVS handles the insertion of modified and unchanged flags within entry lines. When processing an entry line, an additional byte of memory is allocated to flag the entry as modified or unchanged. There is a failure to check if a byte has been previously allocated for the flag, which creates an off-by-one buffer overflow. By calling a vulnerable function several times and inserting specific characters into the entry lines, a remote attacker could overwrite multiple blocks of memory. In some environments, the CVS server process is started by the Internet services daemon (inetd) and may run with root privileges. An authenticated client could exploit this vulnerability to execute arbitrary code, execute commands, modify sensitive information, or cause a denial of service. Note that if a CVS server is configured to permit anonymous read-only access, then this provides sufficient access to exploit a vulnerable server, as anonymous users are authenticated through the cvspserver process. Users should apply the appropriate patch or upgrade as specified by vendor. This issue has been resolved in Stable CVS Version 1.11.16 and CVS Feature Version 1.12.8.

Category 21.1 General QA failures

2004-08-12 **Adobe Acrobat Reader 5.0 UNIX Linux vulnerability command execution backtick character patch issued**

DHS IAIP Daily; http://www.idefense.com/application/poi/display?id=124&type=vulnerabilities&flashstatus=true

August 12, iDEFENSE — Adobe Acrobat Reader (Unix) shell metacharacter code execution vulnerability.

Remote exploitation of an input validation error in the uudecoding feature of Adobe Acrobat Reader (Unix) 5.0 allows an attacker to execute arbitrary code. The Unix and Linux versions of Adobe Acrobat Reader 5.0 automatically attempt to convert uuencoded documents back into their original format. The vulnerability specifically exists in the failure of Acrobat Reader to check for the backtick shell metacharacter in the filename before executing a command with a shell. Successful exploitation allows attackers to execute arbitrary code under the privileges of the user who opened the malicious document with a vulnerable version of Adobe Acrobat Reader. PDF documents are frequently exchanged via e-mail and in combination with a social engineering attack allows attackers to remotely exploit this vulnerability. Adobe Acrobat Reader (UNIX) 5.0.9 appears to be patched against this vulnerability.

Category 21.1 *General QA failures*

2004-08-17 **concurrent versioning system CVS history comand information disclosure vulnerability**

DHS IAIP Daily; http://www.kb.cert.org/vuls/id/579225

August 17, US-CERT — Vulnerability Note VU#579225: CVS "history" command may disclose sensitive information.

Concurrent Versions System (CVS) is a source code maintenance system that is widely used by open-source software development projects. It provides a history command that displays reports on cvs commands that have been executed on files or directories in the source repository. When using the history command, it supports a -X command line switch, which is designed to allow a user to specify the name of the history file to be used. There is an information disclosure vulnerability in this command line switch. When specifying a directory or filename to the -X command line switch, the error message that is returned could allow an attacker to determine the existence and accessibility of arbitrary files or directories on an affected system. A remote, authenticated CVS user could determine if arbitrary files or directories exist on an affected system and whether the CVS daemon has 9 privileges to access them. This issue has been resolved in Stable CVS Version 1.11.17 and CVS Feature Version 1.12.9: https://www.cvshome.org/

Category 21.1 *General QA failures*

2004-08-18 **Qt3 C++ programming library heap-based vulnerability**

DHS IAIP Daily;
http://www.mandrakesoft.com/security/advisories?name=MDKSA−2 004:085

August 18, Mandrakesoft — Updated qt3 packages fix multiple vulnerabilities.

A heap-based overflow has been discovered in the QT library when handling 8-bit RLE encoded BMP files. This vulnerability could allow for the compromise of the account used to view or browse malicious BMP files. On subsequent investigation, it was also found that the handlers for XPM, GIF, and JPEG image types were also faulty. These problems affect all applications that use QT to handle image files, such as QT-based image viewers, the Konqueror web browser, and others. The updated packages have been patched to correct these problems.

Category 21.1 *General QA failures*

2004-08-21 **buffer heap overflow vulnerabilities XV file viewer**

DHS IAIP Daily; http://www.zone−h.org/advisories/read/id=5372

August 21, Zone-H.org — XV multiple buffer overflows.

XV contains at least five exploitable buffer and heap overflow vulnerabilities in the image handling code. This could allow an attacker to craft a malicious image, trick a user into viewing the file in xv, and upon viewing that image execute arbitrary code under privileges of the user viewing image. All versions may be affected. No workaround or solution is known at this time. Original Advisory: http://seclists.org/lists/bugtraq/2004/Aug/0275.html

---

Category 21.1 *General QA failures*

2004-08-26 **Common Desktop Environment buffer overflow vulnerability information disclosure**

DHS IAIP Daily;
http://www.idefense.com/application/poi/display?id=134&type=
vulnerabilities&flashstatus=true

August 26, iDEFENSE — CDE libDtHelp LOGNAME buffer overflow vulnerability.

A buffer overflow vulnerability exists in the CDE libDtHelp LOGNAME variable that can allow local attackers to gain root privileges. CDE is a widely deployed default desktop environment for UNIX operating systems. Depending on the function of the machine, this vulnerability could lead to exposure of highly sensitive data. The vulnerability exists due to a lack of bounds checking on the LOGNAME environment variable. Patches addressing this issue are available from the various CDE vendors.

Category 21.1 *General QA failures*

2004-08-26 **Winamp multimedia software skin file vulnerability code execution attack**

DHS IAIP Daily; http://secunia.com/advisories/12381/

August 26, Secunia — Winamp skin file arbitrary code execution vulnerability.

A vulnerability exists in Winamp 5.04 which can be exploited by malicious people using a specially crafted Winamp skin to place and execute arbitrary programs. With Internet Explorer this can be done without user interaction. The problem is caused due to insufficient restrictions on Winamp skin zip files. The vulnerability has been confirmed on a fully patched system with Winamp 5.04 using Internet Explorer 6.0 on Microsoft Windows XP SP1. No solution is currently available.

Category 21.1 *General QA failures*

2004-09-01 **Oracle Database Application Server Enterprise Manager vulnerabilities**

DHS IAIP Daily; http://www.uscert.gov/cas/techalerts/TA04−245A.html

September 01, US-CERT — Technical Cyber Security Alert TA04-245A: Multiple Vulnerabilities in Oracle Products.

Several vulnerabilities exist in the Oracle Database Server, Application Server, and Enterprise Manager software. The most serious vulnerabilities could allow a remote attacker to execute arbitrary code on an affected system. Oracle's Collaboration Suite and E-Business Suite 11i contain the vulnerable software and are affected as well. The impacts of these vulnerabilities range from the remote unauthenticated execution arbitrary code to data corruption or leakage. Vendor patches and updates are available: http://otn.oracle.com/deploy/security/pdf/2004alert68.pdf

---

Category 21.1 *General QA failures*

2004-09-02 **DB2 Universal Database software buffer overflow vulnerabilities fixpacs updates issued**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Sep/1011140.html

September 02, SecurityTracker — DB2 multiple unspecified vulnerabilities.

Multiple unspecified vulnerabilities exist in DB2 Universal Database, allowing malicious people to compromise a vulnerable system. Two of the vulnerabilities are caused due to boundary errors, which can be exploited by a remote user to execute arbitrary code. There are also some other unspecified errors with an unknown impact. The vendor has issued fixpaks, which address the two buffer overflow vulnerabilities: DB2 8.1: http://www-306.ibm.com/software/data/db2/udb/support/downloa dv8.html and DB2 7.x: http://www-306.ibm.com/software/data/db2/udb/support/downloa dv7.html

---

Category 21.1 *General QA failures*

2004-09-02 **Winzip ZIP file buffer overflow vulnerabilities exploit code execution attack**

DHS IAIP Daily; http://secunia.com/advisories/12430/

September 02, Secunia — Winzip unspecified multiple buffer overflow vulnerabilities.

Multiple buffer overflow and input validation vulnerabilities exist in Winzip 9.0, which potentially can be exploited by a remote user to compromise a user's system. Successful exploitation can potentially lead to execution of arbitrary code. Update to 9.0 SR-1: http://www.winzip.com/upgrade.htm

---

Category 21.1 *General QA failures*

2004-09-08 **mpg123 MPEG layer-2 audio decoder buffer overflow vulnerability no update issued**

DHS IAIP Daily; http://secunia.com/advisories/12478/

September 08, Secunia — mpg123 Mpeg Layer-2 audio decoder buffer overflow vulnerability.

A buffer overflow vulnerability exists in mpg123 version 0.59r. Successful exploitation may allow execution of arbitrary code with the privileges of the user executing mpg123. No vendor solution is currently available.

Category 21.1 General QA failures

2004-09-08 **Usermin vulnerabilities open source command execution**

DHS IAIP Daily; http://secunia.com/advisories/12488/

September 08, Secunia — Usermin shell command injection and insecure installation vulnerabilities.

Two vulnerabilities have been reported in Usermin, where the most critical can be exploited to permit malicious people to execute arbitrary commands with the privileges of the Usermin user. Update to version 1.090: http://www.webmin.com/index6.html

---

Category 21.1 General QA failures

2004-09-30 **Samba input validation vulnerability file access attack**

DHS IAIP Daily; http://www.idefense.com/application/poi/display?id=146&type=vulnerabilities&flashstatus=true

September 30, iDEFENSE — Samba arbitrary file access vulnerability.

An input validation vulnerability has been reported in Samba 3.0.2 and 2.2.9 which allows attackers to remotely access files and directories outside of the specified share path. An attacker does not need exploit code to exploit this vulnerability. Vendor upgrades available at: http://us4.samba.org/samba

---

Category 21.1 General QA failures

2004-10-06 **DB2 database vulnerabilities denial of service DoS**

DHS IAIP Daily; http://secunia.com/advisories/12733/

October 06, Secunia — DB2 Universal Database multiple vulnerabilities.

Multiple vulnerabilities have been reported in DB2 Universal Database, where some of the vulnerabilities can be exploited to cause a Denial of Service, system access, or execution of arbitrary code. Apply DB2 FixPak 6a or 7a: http://www-306.ibm.com/software/data/db2/udb/support/downloa dv8.html. Fixes for DB2 7.2 will be included in FixPak 13.

Category 21.1 General QA failures

2004-10-08 **SANS top 20 Internet security vulnerabilities list**

DHS IAIP Daily; http://security.itworld.com/4341/041008sanstop20/page_1.html

October 08, IDG News Service — SANS unveils top 20 security vulnerabilities.

IT security and research organization The SANS Institute released its annual Top 20 list of Internet security vulnerabilities on Friday, October 8, with the intention of offering organizations at least a starting point for addressing critical issues. The SANS list is compiled from recommendations by leading security researchers, companies, and government organizations around the world. The list is divided into the top 10 Windows and top 10 Unix vulnerabilities. Topping the Windows list is Web servers and services, while the Unix list leads with BIND domain name systems. Vulnerabilities in file sharing applications and instant messaging (IM), which ranked seven and 10 on the Windows list, respectively, represent fairly new categories of risk, said Ross Patel, director of the Top 20 list. Report: http://www.sans.org/top20/

Category 21.1 General QA failures

2004-10-13 **Adobe Acrobat Reader information disclosure vulnerability no update issued**

DHS IAIP Daily; http://secunia.com/advisories/12809/

October 13, Secunia — Adobe Acrobat / Adobe Reader disclosure of sensitive information.

A vulnerability has been discovered in Adobe Acrobat and Adobe Reader, which can be exploited by malicious people to disclose sensitive information. The problem is that embedded Macromedia flash files can be executed in a local context. There is no vendor solution at this time.

Category 21.1 General QA failures

2004-10-15 **Oracle database vulnerability exploits software patches available**

DHS IAIP Daily; http://www.nwfusion.com/news/2004/1015oraclwarns.html

October 15, IDG News Service — Oracle warns of exploits for latest database flaws.

Oracle is warning customers to apply software patches it released in August 2004, citing the availability of malicious code that can exploit unpatched vulnerabilities in its software. The security holes affect a number of Oracle products, including Versions of its 8i, 9i and 10g Database, Application Server and Enterprise Manager software. Oracle strongly recommends affected customers apply the software patches "without delay."

Category 21.1 General QA failures

2004-10-19 **Lotus Notes Domino cross site scripting attack vulnerability no update issued**

DHS IAIP Daily; http://securitytracker.com/alerts/2004/Oct/1011779.html

October 19, SecurityTracker — Lotus Notes/Domino square bracket encoding failure lets remote users conduct cross-site scripting attacks.

A remote user can access the target user's cookies (including authentication cookies), if any, associated with the site running the Notes/Domino software, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user. It is reported that the Lotus Notes HTML encoding function fails to encode square brackets ('[' and ']'). No solution is currently available.

Category 21.1 General QA failures

2004-10-26 **Novell ZENworks privilege escalation vulnerability Remote Management Agent**

DHS IAIP Daily; http://secunia.com/advisories/12969/

October 26, Secunia — Novell ZENworks for Desktops privilege escalation vulnerability.

A vulnerability exists in Novell ZENworks for Desktops, which can be exploited by malicious, local users to gain escalated privileges. The vulnerability is caused due to the Remote Management Agent invoking the ZENworks Remote Control Help functionality with SYSTEM privileges. This can be exploited to execute arbitrary programs with escalated privileges. The vulnerability has been fixed in version 4 SP1b/4.0.1 Interim Release 5:
http://support.novell.com/servlet/filedownload/sec/pub/zfd40 1_ir5.exe

---

Category 21.1 General QA failures

2004-10-27 **RealPlayer skin buffer overflow vulnerability code execution attack**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Oct/1011944.html

October 27, SecurityTracker — RealPlayer skin file buffer overflow may let remote users run arbitrary code.

RealNetworks reported that a remote user can create a malicious skin file that, when loaded by the target user, will trigger a buffer overflow in DUNZIP32.DLL and potentially execute arbitrary code. A fixed version (10.5 (6.0.12.1056)) is available: www.service.real.com/help/faq/security/041026_player/

Category 21.1 General QA failures

2004-10-28 **QuickTime software heap based buffer overflow vulnerabilities HTML BMP**

DHS IAIP Daily; http://secunia.com/advisories/13005/l

October 28, Secunia — Two Quicktime vulnerabilities.

An unspecified integer overflow can be exploited in Quicktime to cause a buffer overflow and execute arbitrary code on a user's system via a specially crafted HTML document. Also, a boundary error within the decoding of BMP images can be exploited to cause a heap-based buffer overflow and execute arbitrary code on a user's system. The integer overflow only effects Windows systems. Update to version 6.5.2: http://www.apple.com/support/downloads/quicktime.html

---

Category 21.1 *General QA failures*

2004-11-04 **Google local service cross site scripting vulnerability no update issued**

DHS IAIP Daily; http://www.zone−h.org/advisories/read/id=6180

November 04, Zone-H.org — Cross Site Scripting vulnerability in Google Local service.

An input validation vulnerability has been reported in Google Local service. A remote user can access the target user's cookies (including authentication cookies), if any, associated with the Google Local site, access data recently submitted by the target user via Web form to the site, or take actions on the site acting as the target user. There is no solution at this time.

Category 21.1 *General QA failures*

2004-11-23 **Winamp stack based buffer overflow vulnerability code execution**

DHS IAIP Daily; http://secunia.com/advisories/13269/

November 23, Secunia — Winamp "IN_CDDA.dll" buffer overflow vulnerability.

A vulnerability in Winamp 5.05 has been reported which can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to a boundary error in the "IN_CDDA.dll" file. This can be exploited in various ways to cause a stack-based buffer overflow, e.g., by tricking a user into visiting a malicious web site containing a specially crafted ".m3u" playlist. Successful exploitation allows execution of arbitrary code. Update to version 5.0.6: http://www.winamp.com/player/

Category 21.1 *General QA failures*

2004-12-16 **Veritas backup software registration stack based buffer overflow vulnerability code execution attack update issued**

DHS IAIP Daily; http://secunia.com/advisories/13495/

December 16, Secunia — Veritas Backup Exec registration request buffer overflow.

A vulnerability has been reported in VERITAS Backup Exec, which can be exploited by malicious people to compromise a vulnerable system. The vulnerability is caused due to a boundary error in the Agent Browser service when processing received registration requests and can be exploited to cause a stack-based buffer overflow. Successful exploitation allows execution of arbitrary code. Original advisory and hotfixes available at: http://seer.support.veritas.com/docs/273419.htm

---

Category 21.1 *General QA failures*

2004-12-21 **libtiff TIFF integer overflow vulnerability code execution attack update issued**

DHS IAIP Daily;
http://www.idefense.com/application/poi/display?id=174&type= vulnerabilities

December 21, iDEFENSE — Libtiff directory entry count integer overflow vulnerability.

Remote attackers may be able to execute arbitrary code with permissions of the user opening the malformed TIFF file. The exposure to this vulnerability is mitigated by the fact that user interaction is required and that the user must view the malicious TIFF file in an application that is linked to a vulnerable version of libtiff. Update to version 3.7.1.
ftp://ftp.remotesensing.org/pub/libtiff/

Category 21.1 *General QA failures*

2004-12-22 **Xpdf buffer overflow vulnerability code execution attack update issued**

DHS IAIP Daily; http://secunia.com/advisories/13602/

December 22, Secunia — Xpdf "doImage()" Buffer Overflow Vulnerability.

A vulnerability has been reported in xpdf, which can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to a boundary error in the "doImage()" function in "Gfx.cc". This can be exploited to cause a buffer overflow by tricking a user into opening a malicious PDF file.Successful exploitation may allow execution of arbitrary code. Apply patch for version 3.00: ftp://ftp.foolabs.com/pub/xpdf/xpdf-3.00pl2.patch Update to version 3.00pl2.
http://www.foolabs.com/xpdf/download.html

Category 21.1 *General QA failures*

2004-12-30 **WHM application software AutoPilot multiple vulnerabilities cross site scripting attack update issued**

DHS IAIP Daily; http://secunia.com/advisories/13673/

December 30, Secunia — WHM AutoPilot multiple vulnerabilities.

WHM AutoPilot has some vulnerabilities that can be exploited by malicious people to conduct cross-site scripting, this allows hackers to compromise a vulnerable system and disclose system information. Input passed to the "site_title" and "http_images" parameter in "header.php" isn't properly sanitized before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of a vulnerable site. Update to version 2.5.0: http://www.whmautopilot.com/

Category 21.1 *General QA failures*

2005-01-01 **quality assurance QA failure credit card payments overcharge reimbursement drug store**

RISKS; http://www.latimes.com/business/la-fi-rup1.4jan01,1,4107985.story 23 65

SPECIAL DEAL AT WALGREEN -- DOUBLE YOUR CHARGES

Monty Solomon reported in RISKS on a software glitch:

Walgreen Co., the largest U.S. drugstore chain, accidentally overcharged as many as 4 million customers buying gifts and decorations the two days before Christmas because its payment-processing system malfunctioned from overuse. Walgreen discovered the error on Christmas Day and electronically reimbursed customers whose credit or debit cards had been incorrectly double- and triple-charged, said company spokesman Michael Polzin. Some credits may not post on customers' accounts until early next week, he said.

Category 21.1 *General QA failures*

2005-01-04 **quality assurance QA failure rate vehicle toll system satellite GPS**

RISKS; http://www.spiegel.de/wirtschaft/0,1518,335367,00.html 23 65

BUGGY GERMAN TOLL-COLLECTION SYSTEM FOR BUGGIES

On 1 Jan 2005, the German government introduced an automated toll-collection system for truckers. Dr Debora Weber-Wulff, Professor of Media and Computing at the Fachhochschule für Technik und Wirtschaft (University of Applied Sciences) in Berlin relayed a report to RISKS from Der Spiegel that there were significant errors: "10 % of all attempts to use the system ended in failure or in people just not paying the toll. The system started with just 320.000 'On-Board Units' (OBU) installed that calculate the tolls using a complicated, satellite-based scheme. If a trucker does not have an OBU they must either purchase a ticket by mobile phone (costly) or at a toll booth in a rest stop. The problems here are that many truckers do not know exactly what exit they will be getting off at. In addition, if there is a traffic jam or other problems and they have to take a detour, they must change their toll ticket."

Category 21.1 *General QA failures*

2005-01-04 **quality assurance QA design flaw automated welfare payment banking direct deposit**

RISKS; http://www.heise.de/newsticker/meldung/54690 23 65

GERMAN DIRECT DEPOSIT DOESN'T

On 1 Jan 2005, the German government introduced a new system for direct deposit of social welfare payments. Dr Debora Weber-Wulff, Professor of Media and Computing at the Fachhochschule für Technik und Wirtschaft (University of Applied Sciences) in Berlin reported in RISKS that about 5% of the recipients received no payments because their older account numbers had fewer than the expected 10 digits. Apparently "The program was of course supposed to put in *leading* zeros, for example <0012345678>. Instead, the zeros were added at the end (1234567800) causing the payments to be unassignable to the recipient." The search for the guilty began immediately, with the software company involved, T-Systems, immediately blaming the government for supplying bad data.

Category 21.1 General QA failures

2005-01-06 **quality assurance QA design flaw procedures employees fail-safe fall-back**

RISKS; http://www.boingboing.net/2005/01/05/a_kafka_day_at_the_l.html 23 66

YOU CAN'T GET THERE FROM HERE

Mark Frauenfelder reported on a Kafkaesque response to a software design flaw in Los Angeles, CA. When a police officer forgot to enter the date on a moving traffic violation ticket, the city computer system was unable to register the ticket. A bureaucrat at the ticket office informed the driver that she would have to call the office _every single workday_ to find out when the ticket finally did get registered, then drive down immediately to pay the fine -- which would include penalties for late payment. Paying the ticket before the computer system registered it was impossible. Paying the ticket "late" would result in an increase in car insurance premiums.

In a follow-up posting, Paul Robinson suggested contacting city attorneys to "ask them to agree to dismiss the charge and not prosecute this particular ticket because the case office is not posting the ticket and you can't be put in a position where you are 'twisting, turning in the wind,' waiting for an unknown and unknowable filing to be made which places you in jeopardy of even more serious criminal penalties when you can't get the current one resolved." Failing that, Mr Robinson advised suing the District Attorney's office "for a writ of mandamus prohibiting them from prosecuting the original ticket. You may even be able to sue for damages but I think all you're interested in is to get rid of the matter, either by converting it off of a moving violation or getting it dismissed. I don't think it would be that difficult to file for an order even without a lawyer since you're only trying to solve the problem and the government, by its incompetence or misconduct is placing you in a position in which you are being denied the right to a constitutionally guaranteed speedy trial and quite possibly to equal.protection and possibly other issues. Even if you don't get the order you've got grounds to have any potential penalty for not paying the ticket and not appearing canceled."

Category 21.1 General QA failures

2005-01-06 **WinAce GZIP ZIP vulnerability directory traversal attack**

DHS IAIP Daily; http://secunia.com/advisories/13734/

WINACE GZIP AND ZIP DIRECTORY TRAVERSAL VULNERABILITY.

A vulnerability has been reported in WinAce 2.5, which potentially can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to an input validation error when extracting files compressed with GZIP (.gz) or ZIP (.zip). This makes it possible to have files extracted to arbitrary locations outside the specified directory using the "../" directory traversal sequence. There is no solution at this time.

Category 21.1 General QA failures

2005-01-15 **quality assurance QA software design flaws list**

RISKS; http://asktog.com/Bughouse/index.html 23 67

SOFTWARE ENGINEERING TIPS

Peter Ludemann contributed these pointers to bad software design in RISKS:

Bruce Tognazzini has started collected well-known bugs at http://asktog.com/Bughouse/index.html ... many of these have shown up before in Risks, such as "Harassing Confirmations & Missing Confirmations" and "'Smart' functions that aren't smart".

Readers might also enjoy (if that's the right word) Tognazzini's article on Security D'ohlts: http://asktog.com/columns/058SecurityD'ohlts.html and an older article on how inconvenience and security are confused: http://asktog.com/columns/051AirSecurity.html

---

Category 21.1 *General QA failures*

2005-01-15 **quality assurance QA map software Microsoft MapPoint directions long trip Norway**

RISKS 23 67

TAKE THE LONG WAY HOME

Two RISKS contributors pointed out a flaw in Microsoft's map software; Adam Shostack's report is as follows (and is entitled "MapPoint Explains Vikings?":

When going from Haugesund, Rogaland, Norway, to Trondheim, So-Trondelag, Norway, be aware that following Microsoft MapPoint's directions, will take you through England, France, Belgium, the Netherlands, Germany, Denmark, Sweden, and finally back into Norway. While this may be culturally sensitive and respectful of historic Viking routing, rooting, or looting, it is somewhat less efficient than other routes, as a quick glance at a map will show.

Start: Haugesund, Rogaland, Norway

End: Trondheim, So-Trondelag, Norway

Total Distance: 1685.9 Miles, Estimated Total Time: 47 hours, 31 minutes
(This is listed as the "quickest" route.)

Category 21.1 *General QA failures*

2005-01-24 **system configuration boot device printer USB drive documentation design denial of service DoS**

RISKS 23 68

BOOT THE PRINTER OFF THE SYSTEM TO BOOT

Lindsay Marshall had an interesting observation in RISKS about the unexpected consequenes of two configuration paramaters:

A neighbour of mine just bought a new Epson printer and were trying to install it on their laptop. They had a problem : they rebooted their system and it said "Not a system disk". They gave me a call and I wandered up to have a look. I hit a few keys and suddenly it booted again. Odd I thought (not having noticed a crucial event!). I got in as Administrator and installed the software for them and we connected up the printer and rebooted. "Not a system disk". I thought for a bit and looked in the BIOS and lo and behold, the first boot item was a USB disc, and the printer does indeed have a USB disc feature so that you can access camera memory cards via the printer. Unplug the printer and the system boots fine, plug it and no dice. (What I hadn't noticed above was that my neighbour had unplugged the printer from the USB as I was hitting keys.)

How could anyone expect everyday users with no experience of systems internals to deal with a situation like that? Why should a printer look like a disc anyway (at least by default), and why have the default BIOS setting to boot from USB first? A disaster waiting to happen and it happened.

Category 21.1 *General QA failures*

2005-01-24 **DatarDataRescue Interactive Disassembler Pro (IDA Pro) buffer overflow vulnerability privilege escalation attack**

DHS IAIP Daily; http://www.k−otik.com/english/advisories/2005/0059

DATARESCUE INTERACTIVE DISASSEMBLER PRO (IDA PRO) BUFFER OVERFLOW

A vulnerability has been identified in IDA Pro that could be exploited by attackers to execute arbitrary code with the privileges of the logged in user. The stack based overflow problem occurs when parsing long PE import library names. This flaw can be exploited by convincing a user to open a malicious Portable Executable file with a vulnerable version of IDA Pro, which may potentially lead to a system compromise.

Category 21.1 *General QA failures*

2005-01-26 **automobile operating system virus cell phone Bluetooth access control design flaw quality assurance QA**

RISKS; http://tinyurl.com/5p3jh 23 70

INFECTING CARS VIA CELL PHONES?

Karl Klashinsky noted a serious problem with software that has no security provisions:

The topic of software flaws in the embedded systems within modern automobiles has been discussed in RISKS several times. But here's a new twist (to me, at least), a case where the on-vehicle software is corrupted by a virus, inserted into the automobile's computing systems, via a blue-tooth enabled cell-phone.

Peter Neumann commented:

There's the obvious risk here… a vehicle can be infected by the cell-phone in the vehicle next to you while stopped in traffic or sitting in a parking lot. As this vulnerability becomes known in the cracker community, how long before someone tailors a virus specific to a vehicular target -- perhaps creating runaway-vehicle scenarios similar to the "faulty cruise control" incidents reported here in RISKS.

Category 21.1 *General QA failures*

2005-01-26 **ISC BIND 8.x / 9.x remote denial of service vulnerabilities denial of service DoS update issued**

DHS IAIP Daily; http://www.k−otik.com/english/advisories/2005/0064

ISC BIND 8.X / 9.X REMOTE DENIAL OF SERVICE VULNERABILITIES

Two vulnerabilities have been reported in ISC BIND 8.4.4, 8.4.5, and 9.3.0, which could be exploited by attackers to cause a Denial of Service. The first flaw affects BIND 8.x and results from a buffer overrun error when using a certain array to track nameservers/addresses, which may be exploited by a remote attacker to cause a Denial of Service. The second issue is present in the self-check function of BIND 9.x, and may be exploited to cause a Denial of Service. Upgrade to BIND version 8.4.6 or 9.3.1: http://www.isc.org/sw/bind/

Category 21.1 *General QA failures*

2005-01-27 **Openswan Pluto buffer overflow vulnerability code execution attack**

DHS IAIP Daily; http://securitytracker.com/alerts/2005/Jan/1013014.html

OPENSWAN PLUTO GET_INTERNAL_ADDRESSES() REMOTE BUFFER OVERFLOW LETS REMOTE AUTHENTICATED USERS EXECUTE ARBITRARY CODE

Openswan has a buffer overflow vulnerability; a remote authenticated user may be able to execute arbitrary code on the target system. A remote authenticated user can execute arbitrary code on the target system with the privileges of the 'pluto' process. The vendor has released fixed versions (1.0.9 and 2.3.0), available at: http://www.openswan.org/code/

Category 21.1 *General QA failures*

2005-02-01 **quality assurance QA bug glitch matching algorithm medical residents hospitals students mismatch**

RISKS; http://blogborygmi.blogspot.com/2005/01/selection-dysfunction.html 23 71

MEDICAL STUDENTS MISMATCHED TO HOSPITALS

In a serious problem for medical students, a program used to match student preferences with hospital preferences failed for urology residencies in January 2005. As a result of the error in the computer program, the match had to be re-run a few days after the first (wrong) run, causing disruption for residents who had already began to make their plans to move to distant cities.

RISKS correspondent Daniel Kahn Gillmor commented, "So, why wasn't a human reviewing the results of the match for reasonableness before publication? Why aren't the algorithms used in the match process freely available? What safeguards are there on the data-entry step (since GIGO continues to apply)? Why isn't there an audit process in place?"

Category 21.1 *General QA failures*

2005-02-02 **hardware failure CD scratch damage drive shatter break design control**

RISKS 23 71

HIGH-SPEED CD-DRIVES SHATTER DAMAGED DISKS

Henk Langeveld reported on a disturbing interaction of damaged CDs and new high-speed CD-drives:

I've had the nasty experience to have lost four CD's to newer high-speed CD and DVD-drives within a year.

The current state of technology will run CDs and DVDs at high speeds, and the centrifugal force of the drive increases the risk of any scratch on the media to result in one broken CD, and one ruined drive.

Peter G. Neumann added:
[Drew Dean commented to me on this: ``I believe programs such as Exact Audio Copy (EAC) do slow down the drive, and most CD/DVD burning software can write at slower speeds, but I'm not aware of any interface to tell an OS to always slow down reading." PGN]

In follow-up postings in RISKS 23.72, Eben King and Jonathan King and others provided helpful suggestions and links for utilities that can slow down fast CD-ROM drives.

Category 21.1 *General QA failures*

2005-02-11 **Avaya vendor product multiple vulnerabilities privilege escalation cross site scripting phishing information disclosure system compromise attacks**

DHS IAIP Daily; http://secunia.com/advisories/14210/

AVAYA VARIOUS PRODUCTS MULTIPLE VULNERABILITIES.

Avaya has acknowledged some vulnerabilities in various products, which can be exploited by malicious, local and remote users. Exploitation of these vulnerabilities can be used to bypass certain security restrictions and gain escalated privileges, conduct cross-site scripting and phishing attacks, disclose sensitive information, and compromise a vulnerable system. Solution available at: http://support.avaya.com/elmodocs2/security/ASA-2005-037_MS0 5-004-MS05-015.pdf

---

Category 21.1 *General QA failures*

2005-02-16 **DCP-Portal SQL injection vulnerability command execution no update issued**

DHS IAIP Daily; http://securitytracker.com/alerts/2005/Feb/1013216.html

DCP-PORTAL SQL INJECTION VULNERABILITY

Several input validation vulnerabilities were reported in DCP-Portal that could permit a remote user to inject SQL commands. The 'index.php' and 'forums.php' scripts do not properly validate user-supplied input in several parameters. If magic_quotes_gpc is set to off in the 'php.ini' configuration file, then a remote user can submit a specially crafted HTTP request to execute SQL commands on the underlying database. No solution is currently available.

Category 21.1 *General QA failures*

2005-02-16 **K Desktop Environment KDE open source X-Windows buffer overflow vulnerability root privileges code execution attack update issued**

DHS IAIP Daily; http://securitytracker.com/alerts/2005/Feb/1013217.html

KDE BUFFER OVERFLOW REMOTE ACCESS VULNERABILITY.

A buffer overflow vulnerability was reported in KDE in the 'fliccd' component of KDE-Edu, KStars, and INDI. A local user can obtain root privileges and a remote user may be able to gain access to the system. A local user can trigger several buffer overflow vulnerabilities in fliccd to execute arbitrary code on the target system. The Instrument Neutral Distributed Interface (INDI) support installs fliccd with set user id (setuid) root user privileges. As a result, a local user can gain root privileges. If the fliccd daemon is running (which is not the default configuration), then a remote user can gain access to the target system, potentially with root privileges. The vendor has issued a patch for 3.3.2, available at: ftp://ftp.kde.org/pub/kde/security_patches

---

Category 21.1 *General QA failures*

2005-02-16 **Typeseed vulnerability privilege escalation attack no update issued**

DHS IAIP Daily; http://securitytracker.com/alerts/2005/Feb/1013218.html

TYPESPEED VULNERABILITY LOCAL USERS GAIN ELEVATED PRIVILEGES

A format string vulnerability was reported in typespeed that could permit a local user to gain elevated privileges on the target system. A sprintf() call is made in 'file.c' without the appropriate format string specifier when processing data from the HOME environment variable. A local user can set the HOME environment variable to a specially crafted value to execute arbitrary code with 'games' group privileges. No solution is currently available.

Category 21.1 *General QA failures*

2005-02-22 **GProFTPD file transfer protocol remote format string vulnerabilities command execution attack update issued**

DHS IAIP Daily; http://www.k−otik.com/english/advisories/2005/0190

GProFTPD "gprostats" remote format string vulnerability.

A new vulnerability was reported in GProFTPD, which may be exploited by remote attackers to execute arbitrary commands. The problem is due to a format string error in the "gprostats" utility when parsing ProFTPD transfer logs, which may be exploited to compromise a system by performing a specially crafted FTP transfer. Update to version 8.1.9: http://mange.dynup.net/linux/gproftpd/gproftpd-8.1.9.tar.gz

---

Category 21.1 *General QA failures*

2005-02-24 **Cyrus IMAP server buffer overflow vulnerabilities code execution attack update issued**

DHS IAIP Daily; http://secunia.com/advisories/14383/

CYRUS IMAP SERVER BUFFER OVERFLOW VULNERABILITIES

Multiple vulnerabilities have been reported in Cyrus IMAP Server, which potentially can be exploited by malicious people to compromise a vulnerable system. These are due to off-by-one boundary errors. Successful exploitation may allow execution of arbitrary code. Update to version 2.2.11 or later: http://asg.web.cmu.edu/cyrus/download/

Category 21.1 *General QA failures*

2005-02-26 **identification authentication I&A Web form business registration fraud**

RISKS 23 77

CALIFORNIA LETS ANYONE FILL IN CORPORATE INFORMATION "CORRECTIONS"

Geoff Kuenning discovered that California corporation regulations require business owners to file registration information -- which can be done online. Unfortunately, there is no authentication of the identity proposed by a user, so anyone can damage the registration of any California-registered company for a $25 fee. Mr Kuenning reports that such companies happen to include Microsoft.

Category 21.1 *General QA failures*

2005-02-28 **phpBB PHP bulletin board vulnerabilities installation path discovery**

DHS IAIP Daily; http://www.k−otik.com/english/advisories/2005/0212

PHPBB ADMINISTRATOR SESSION HANDLING CRITICAL SECURITY UPDATE

Two vulnerabilities were reported in phpBB, which may be exploited by attackers to determine the installation path or bypass certain security features. The first problem resides in the "autologinid" (includes/sessions.php) variable and could be exploited by malicious users to gain administrator rights. The second flaw resides in the "viewtopic.php" script, and could be exploited to disclose the webroot path. Update to version 2.0.13: http://www.phpbb.com/downloads.php

---

Category 21.1 *General QA failures*

2005-03-02 **Cproxy input validation vulnerability directory traversal file disclosure service crash denial of service DoS no update issued**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2005/Mar/1013359.html

CPROXY INPUT VALIDATION VULNERABILITY

Several vulnerabilities were reported in CProxy. A remote user can view files on the target system and cause the service to crash. The server does not properly validate user-supplied input. A remote user can submit a specially crafted URL containing '../' directory traversal characters to view arbitrary files on the target system. There is no solution at this time.

Category 21.1 *General QA failures*

2005-03-02 **Computer Associates CA License multiple buffer overflow vulnerabilities code execution attack updates issued**

DHS IAIP Daily; http://www.idefense.com/application/poi/display?type=vulnera
bilities

COMPUTER ASSOCIATES LICENSE CLIENT/SERVER MULTIPLE BUFFER OVERFLOW VULNERABILITIES

Remote exploitation of buffer overflow vulnerabilities in Computer Associates License Server and License Client can allow attackers to execute arbitrary code. The vulnerabilities exist due to insufficient bounds checking on user-supplied values in GETCONFIG and GCR requests. Updates available at: http://supportconnectw.ca.com/public/ca_common_docs/security
_notice.asp

Category 21.1 *General QA failures*

2005-03-02 **RealPlayer WAV SMIL stack based buffer overflows file handling vulnerabilities code execution attack update issued**

DHS IAIP Daily; http://secunia.com/advisories/14456/

REALPLAYER WAV AND SMIL FILE HANDLING BUFFER OVERFLOWS.

Two vulnerabilities have been reported in various RealNetworks products, which can be exploited by malicious people to compromise a user's system: 1) A boundary error within the processing of WAV files can be exploited to cause a buffer overflow via a specially crafted WAV file; and 2) A boundary error within the processing of SMIL files can be exploited to cause a stack-based buffer overflow via a specially crafted SMIL file. Successful exploitation of the vulnerabilities allows execution of arbitrary code. Updates available at: http://service.real.com/help/faq/security/050224_player/EN/

Category 21.1 *General QA failures*

2005-03-03 **CA Unicenter Asset Management software input validation vulnerabilities password disclosure code execution attack updates issued**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2005/Mar/1013360.html

CA UNICENTER ASSET MANAGEMENT INPUT VALIDATION VULNERABILITIES

A remote authenticated user with access to the administrative console can obtain the SQL administrator password, displayed (in masked form) on the 'Change Credentials for Database' window. A remote authenticated user can create a specially crafted URL that, when loaded by a target user, will cause arbitrary scripting code to be executed by the target user's browser. The code will originate from the site running the Unicenter Asset Management software and will run in the security context of that site. As a result, the code will be able to access the target user's cookies (including authentication cookies), if any, associated with the site, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user. Vendor advisory and updates available at: http://supportconnect.ca.com/sc/solcenter/solresults.jsp?apa rno=QO64323

Category 21.1 *General QA failures*

2005-03-07 **X11 libXpm XPM image buffer overflow vulnerability system compromise code execution attack update issued**

DHS IAIP Daily; http://secunia.com/advisories/14460/

X11 LIBXPM XPM IMAGE BUFFER OVERFLOW VULNERABILITY

A vulnerability has been reported in libXpm, which potentially can be exploited by malicious people to compromise a vulnerable system. The vulnerability is caused due to boundary errors in "GetImagePixels()" and "PutImagePixels()". This may be exploited to cause a buffer overflow when a specially crafted XPM image file is processed. Successful exploitation may potentially allow execution of arbitrary code. The vulnerability has been fixed in the CVS repository.

Category 21.1 *General QA failures*

2005-03-09 **Novell iChain GUI Mini FTP server multiple vulnerabilities administrative access unlimited logins update issued**

DHS IAIP Daily; http://www.securitytracker.com/archives/summary/9000.html

NOVELL ICHAIN MULTIPLE VULNERABILITIES.

Multiple vulnerabilities were reported in Novell iChain GUI and Novell iChain Mini FTP Server. A remote user can gain administrative access, make unlimited login attempts without being locked out, or determine the installation path. Original advisories and updates available at: http://support.novell.com/cgi-bin/search/searchtid.cgi?/1009 6885.htm and http://support.novell.com/cgi-bin/search/searchtid.cgi?/1009 6886.htm and http://support.novell.com/cgi-bin/search/searchtid.cgi?/1009 6887.htm

---

Category 21.1 *General QA failures*

2005-03-10 **software quality assurance QS update error denial of service DoS underground railway subway tube train data corruption flaw bug**

RISKS 23 79

OYSTER CARD FAULT CAUSES PROBLEMS ON LONDON UNDERGROUND

"Automatic updates cause journey renewal problems"
by Daniel Thomas, *Computing*, 10 Mar 2005

Londoners were faced with travel problems this morning after an IT error meant hundreds of commuters could not renew journeys on their Oyster card.

The error, which affected the whole of the London Underground (LU) and Docklands Light Railway (DLR), was caused when an overnight electronic updating process went wrong.

Transport for London (TfL) and TranSys - the consortium that operates the Oyster card scheme - automatically updates the system each night to add new records and block stolen and canceled cards.

But a glitch in the system early this morning means commuters are unable to use machines at Underground or DLR station this morning to add new journeys onto the smart cards.

'Every morning information goes out about stopped cards and it was an error in the data that caused the problem,' said a spokeswoman for TranSys.

Passengers that have already paid for their journey or using prepay can still use the system as normal.

TfL and TranSys identified the error at 4am this morning and starting issuing a fix to the problem by 8.30am.

'We hope everything to be up and running again by the end of the morning,' said the TranSys spokeswoman. 'We are now looking into what actually caused the error and ways of ensuring this doesn't happen again.'

Category 21.1 *General QA failures*

2005-03-11 **MySQL multiple remote vulnerabilities remote authenticated attacker privilege escalation updates issued**

DHS IAIP Daily; http://www.securityfocus.com/bid/12781/info/

MYSQL AB MYSQL MULTIPLE REMOTE VULNERABILITIES

MySQL is reported prone to multiple vulnerabilities that can be exploited by a remote authenticated attacker. MySQL is reported prone to an insecure temporary file creation vulnerability. It is also prone to an input validation vulnerability that can be exploited by remote users that have INSERT and DELETE privileges on the 'mysql' administrative database and may be leveraged to load and execute a malicious library in the context of the MySQL process. It is reported that the vendor has addressed these vulnerabilities in MySQL versions 4.0.24 and 4.1.10a. Users should consult http://dev.mysql.com/downloads/ for availability of these downloads.

Category 21.1 *General QA failures*

2005-03-13 **MySQL MaxDB Web Agent multiple denial of service vulnerabilities input validation null pointer reference crash update issued**

DHS IAIP Daily; http://www.k−otik.com/english/advisories/2005/0263

MYSQL MAXDB WEB AGENT MULTIPLE DENIAL OF SERVICE VULNERABILITIES.

Several input validation errors have been identified in MySQL MaxDB and SAP DB Web Agent, which may be exploited by remote attackers to cause a Denial of Service. A remote attacker can request the function with invalid parameters to cause a null pointer dereference resulting in a crash of MySQL MaxDB Web Agent. Update to MySQL MaxDB 7.5.00.24: http://dev.mysql.com/downloads/maxdb/7.5.00.html

---

Category 21.1 *General QA failures*

2005-03-21 **Subdreamer Light global variables SQL injection vulnerability no update issued**

DHS IAIP Daily; http://secunia.com/advisories/14652/

SUBDREAMER LIGHT GLOBAL VARIABLES SQL INJECTION VULNERABILITY

A vulnerability in Subdreamer Light, which can be exploited by malicious people to conduct SQL injection attacks. Input passed to various global variables isn't properly sanitized before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code. Successful exploitation requires that "magic_quotes_gpc" is disabled. There is no vendor solution at this time.

Category 21.1 *General QA failures*

2005-03-23 **radio frequency identification devices RFID exploits vulnerabilities compromise privacy hole reverse engineering fraud theft**

RISKS; http://www.interesting-people.org/archives/interesting-people/ 23 81

RSA FINDS MORE FLAWS IN RFID

Jacqueline Emigh of eweek.com wrote:

After uncovering a security weakness in a radio-frequency identification tag from Texas Instruments Inc., researchers from RSA Security Inc.'s RSA Laboratories and The Johns Hopkins University are now eyeing future exploits against other RFID products in the interests of better security, one of the researchers said this week. Meanwhile, TI will keep making the compromised RFID tag in order to meet the needs of applications more sensitive to speed and pricing than to privacy, according to a TI official.

The Johns Hopkins University Information Security Institute and RSA first publicized their findings about the RFID security hole in January. In a paper posted at www.rfidanalysis.org, the researchers claim that by cracking a proprietary cipher, or encryption algorithm in one of TI's DST (digital signature transponder) RFID tags, they were able to circumvent the tags' built-in security enough to buy gasoline and turn on a car's ignition. The researchers from Johns Hopkins and RSA reverse-engineered and emulated the 40-bit encryption over two months.

Category 21.1 *General QA failures*

2005-03-23 **automobile car cruise control autopilot failure accident crash bug lockup freeze brakes ignition engine control**

RISKS 23 81

CRUISE-CONTROL TAKES BITS IN ITS TEETH?

Robert Scheidt reported on a serious problem and asked for clarification:

Recently in France a number of failures of "cruise control" systems especially on recent models of Renault made cars have been reported, some creating serious accidents (including a deadly one). In general it is reported that the car stays at his set speed and no matter what the driver does, including cutting the ignition and breaking, the car continues at that speed.

What's more surprising is that it is also reported that brakes become ineffective (the brake pedal resists pressure).

I could imagine that the cruise control being probably under control of some microprocessor, this microprocessor could "hang" due to some software problem and therefore that everything it controls just stays as it is. Especially in newer cars where fuel injection is completely electronically controlled (no mechanical link between the gas pedal and the fuel injection controls).

However, I have difficulties believing that the same microprocessor would control the brakes and make them ineffective. I wonder if somebody on this board has some insight on how the electronic controls of modern cars are designed and especially if a single component's failure (such as a common microprocessor) could affect multiple functions (e.g., acceleration and brakes).

There was a flurry of discussion in RISKS 23.82. Several correspondents confirmed that some automotive systems do in fact control brakes as well as speed.

Category 21.1 *General QA failures*

2005-03-24 **bank account redit card transfer third party registration vulnerability fraud theft design flaw**

RISKS 23 81

RISKY US BANK VISA PRODUCT

John Meissen analyzed the security flaws in a new Visa service:

US Bank has a Visa product targeted at teens (or rather, their parents), called VisaBuxx. It looks and acts like a standard Visa-logo debit card, but is more like a prepaid phone card - you pre-load it with value, and it's not directly tied to any bank account.

Their web site and marketing literature talk about being able to easily add value to the card by transferring money online from an existing US Bank checking account. Unfortunately, the system leaves a lot to be desired.

The usbank.com website has a link for the VisaBuxx program. When you click on it you're redirected to another site, called visabuxx.com. This site is apparently run by someone called "WildCard Systems". In order to transfer money from your US Bank checking account to the card you have to provide WildCard Systems with your checking account number and routing information and authorization to pull funds from the account, or give them your own debit card number. While WildCard Systems may be honorable and trustworthy, the risks in this are so obvious that it's painful. Meanwhile, the Terms Of Service published on the site go to great lengths to explicitly disavow any responsibility for anything bad that might result from the use of the site.

The correct way for the bank to have implemented this would have been to provide the ability to associate the card with your existing Internet banking identity, and then let you log in through the bank's website and tell the them to send money from an account to the card rather than allowing the card operators to pull money from your account. Having the ability to provide account data to the VisaBuxx website is useful for non-US Bank customers, but a legitimate US Bank customer I shouldn't be forced to do it.

I find it mind-boggling that financial corporations still can't see the obvious when it comes to protecting customer account data. When dealing with an official bank product I should NEVER have to tell the application anything about my accounts.

Category 21.1 General QA failures

2005-03-25 **Sybase lawsuit threat flaw vulnerability open disclosure Next Generation Security**

EDUPAGE; http://www.computerworld.com/

SYBASE BLOCKS FLAW DISCLOSURE WITH THREAT TO SUE

California-based Sybase Inc. has threatened to sue U.K.-based Next Generation Security (NGS) Software Ltd. If that company discloses the details of eight security flaws it discovered in 2004 in Sybase database software, Adaptive Server Enterprise Version 12.5.3. NGS notified Sybase of the flaws, and Sybase released a patched and updated version of the software in February 2005. NGS policy mandates that it wait for vendors to issue patches before publicly releasing information on software flaws. The company chose not to make a public disclosure of the database holes after receiving the Sybase letter threatening to sue. According to an e-mail statement from a Sybase spokeswoman, the company was motivated to prevent the disclosure out of concern for its users' security. ComputerWorld, 25 March 2005

Category 21.1 General QA failures

2005-03-28 **denial of service human error clock time data entry bank customers automated teller online services**

RISKS; http://tinyurl.com/djrmz 23 82

HUMAN ERROR SHUTS DOWN BARCLAY'S AUTOMATED TELLER SYSTEM

Michael "Streaky" Bacon [no, really] reported on a service interruption for customers of the British Barclay's Bank. The following reorganizes parts of his report to RISKs.

On 27 Mar 2005, the UK put its clocks forward one hour. This apparently caused problems for Barclays Bank - one of the UK's leading banks - with ATMs and other online services unavailable to customers in the South of the country. The text of the Daily Telegraph's report on the failure is reproduced below.

> Summer Time slip-up forces Barclays' cashpoints to close
> *The Daily Telegraph*, 28 March 2005
>
> Millions of Barclays customers were unable to withdraw money yesterday after the bank's cashpoint network crashed amid claims that a duty manager had accidentally put the clocks back instead of forward. More than 1,400 auto-tellers in the south of England and some on-line services were out of order. Barclays customers were unable to withdraw money from any bank, while cardholders with other banks were unable to use Barclays cash machines.
>
> The error came to light at 4am on 27 Mar 2005 when technicians noticed that customers' personal details were not being forwarded to the computers that control much of the bank's infrastructure. The problem was eventually resolved at 5pm. Executives trying to determine the cause of the problem admitted that a mistake during the switch to British Summer Time could have been to blame. Customer services staff were less ambiguous. One admitted: "A manager put the clocks back instead of forward and that has caused enormous problems."
>
> The bank's British network uses two servers based in Gloucestershire: one for operations north of the Wash and the other to control operations in the South. The Gloucester South server is understood to have been set one hour back instead of forward. The bank conceded that an error over the time change was to blame but denied that an individual manager made the mistake. Alistair Smith, a spokesman for the bank, said: "It seems that this problem may somehow be related to the time change, although I am told it was not to do with someone making a mistake while manually changing the time."

Mr Bacon then analyzes the situation as follows:

I would be surprised if the bank relied upon the actions of a human to change the time on its servers. For example, if the servers are not time synchronised through an atomic clock receiver or from an NTP Time Server, it begs serious questions regarding the time-standing of transactions.

Bi-annual time changes have been a part of computing at least since the first commercial systems began processing. Surely 54 years is not too short a time to have worked out the risks and put in place procedures to deal with them.

If it was indeed a human error, perhaps the heading on the relevant page should read: "Spring forward, fall back".

Another puzzling factor is that it apparently took 11 hours (4 am to 5 pm) to determine and correct the problem. In my experience, the first thing to be blamed is the last thing that was changed.

Category 21.1 General QA failures

2005-03-29 **phpCOIN vulnerability SQL injection command execution attack update issued**

DHS IAIP Daily; http://securitytracker.com/alerts/2005/Mar/1013592.html

PHPCOIN LETS REMOTE USERS INJECT SQL COMMANDS AND EXECUTE ARBITRARY FILES ON THE TARGET SYSTEM.

A vulnerability was reported in phpCOIN. A remote user can execute arbitrary files located on the target system. A remote user can also inject SQL commands. The software does not properly validate user-supplied input in the search engine query, the username and email fields when requesting a forgotten password, and in the domain name filed when ordering a product. A remote user can supply specially crafted values to execute SQL commands on the underlying database. The vendor has issued a fixed version (1.2.2), available at: http://www.phpcoin.com/auxpage.php?page=download

---

Category 21.1 General QA failures

2005-03-29 **EncapsBB vulnerability root file inclusion no update issued**

DHS IAIP Daily; http://secunia.com/advisories/14761/

ENCAPSBB "ROOT" FILE INCLUSION VULNERABILITY.

A vulnerability in has been reported in EncapsBB, which can be exploited by malicious people to compromise a vulnerable system. Input passed to the "root" parameter in "index_header.php" isn't properly verified, before it is used to include files. This can be exploited to include arbitrary files from external and local resources. Successful exploitation requires that "register_globals" is enabled. There is no solution at this time.

Category 21.1 General QA failures

2005-03-30 **Sylpheed application Multipurpose Internet Mail Extensions MIME attachment filename buffer overflow vulnerability system compromise update issued**

DHS IAIP Daily; http://secunia.com/advisories/14756/

SYLPHEED MIME-ENCODED ATTACHMENT FILENAME BUFFER OVERFLOW.

A vulnerability has been reported in Sylpheed, which potentially can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to a boundary error when displaying messages containing attachments with MIME-encoded filenames. This can be exploited to cause a buffer overflow via a specially crafted message. Update to version 1.0.4: http://sylpheed.good-day.net/

Category 21.1 General QA failures

2005-04-01 **NetVault buffer overflow vulnerability code execution attack no update issued**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2005/Apr/1013625.html

NETVAULT BUFFER OVERFLOWS LET LOCAL AND REMOTE USERS EXECUTE ARBITRARY CODE

A vulnerability exists in the processing of the 'configure.cfg' file. A local user with access to the file can create a computername 'Name=' entry that is longer than 111 bytes. When the NetVault Process Manager service starts (or restarts), a buffer overflow will be triggered and arbitrary code executed with System privileges. A remote user can connect to the target system on port 20031 and supply a specially crafted 'clientname' entry in the 'Available NetVault Machines' list to trigger a heap overflow and execute arbitrary code on the target server. A local user with write access to the 'configure.cfg' file can execute arbitrary code with System level privileges. No solution is currently available.

Category 21.1 General QA failures

2005-04-05 **BakBone NetVault heap based buffer overflow vulnerabilities system compromise no update issued**

DHS IAIP Daily; http://secunia.com/advisories/14814/

BAKBONE NETVAULT BUFFER OVERFLOW VULNERABILITIES

Some vulnerabilities in BakBone NetVault, which can be exploited by malicious people to compromise a vulnerable system. The vulnerabilities are caused due to some boundary errors in the communication handling. This can be exploited to cause a heap-based buffer overflow by sending some specially crafted traffic to port 20031. There is no vendor solution at this time.

Category 21.1 *General QA failures*

2005-04-11 **Maxtheon security ID disclosure vulnerability system compromise directory traversal attack update issued**

DHS IAIP Daily; http://www.secunia.com/advisories/14918/

MAXTHON SECURITY ID DISCLOSURE VULNERABILITY

A vulnerability has been reported in Maxthon, which can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to a design error where the security ID of a plug-in is not properly protected from being included and accessed on an external website via the script tag. This can be exploited to read and write arbitrary files via the "readFile()" and "writeFile()" API functions via directory traversal attacks. Update to version 1.2.2: http://www.maxthon.com/download.htm

---

Category 21.1 *General QA failures*

2005-04-11 **CA BrightStor ARCserve Backup remote buffer overflow vulnerability command execution attack update issued**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/0334

CA BRIGHTSTOR ARCSERVE BACKUP REMOTE BUFFER OVERFLOW VULNERABILITY

A buffer overflow vulnerability was identified in Computer Associates BrightStor ARCserve Backup UniversalAgent, which may be exploited by remote attackers to execute arbitrary commands. The flaw occurs when handling malformed requests containing a specially crafted "option" field (port 6050/TCP/UDP), which may be exploited by unauthenticated attackers to run arbitrary code with SYSTEM privileges. Refer to Source link for solutions.

Category 21.1 *General QA failures*

2005-04-11 **ModernBill cross site scripting file inclusion vulnerabilities cross site scripting attack**

DHS IAIP Daily; http://secunia.com/advisories/14890/

MODERNBILL CROSS-SITE SCRIPTING AND FILE INCLUSION VULNERABILITIES

Some vulnerabilities have been reported in ModernBill, which can be exploited by malicious people to conduct cross-site scripting attacks and compromise a vulnerable system. Input passed to the "c_code" and "aid" parameters in "orderwiz.php" isn't properly sanitized before being returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of a vulnerable site. Input passed to the "DIR" parameter in "news.php" isn't properly verified, before it is used to include files. This can be exploited to include arbitrary files from external and local resources. Update to version 4.3.1.

Category 21.1 *General QA failures*

2005-04-12 **K Desktop Environment KDE buffer overflow vulnerability system compromise code execution attack no update issued**

DHS IAIP Daily; http://secunia.com/advisories/14908/

KDE KDELIBS PCX IMAGE BUFFER OVERFLOW VULNERABILITY

A vulnerability in KDE kdelibs, which potentially can be exploited by malicious people to compromise a vulnerable system. The vulnerability is caused due to an error in the kimgio component when processing PCX image files. This may be exploited via a specially crafted image file to execute arbitrary code via an application linked against the vulnerable library. No vendor solution available.

Category 21.1 *General QA failures*

2005-04-12 **Microsoft security bulletin critical important updates Windows XP Server 2003 2000 2K Internet Explorer IE Word MSN Messenger**

DHS IAIP Daily; http://www.microsoft.com/technet/security/bulletin/ms05−apr.
mspx

MICROSOFT RELEASES APRIL 2005 SECURITY BULLETINS

Microsoft released its security bulletins for April 2005. There are five "Critical" (MS05-019 – MS05-023) and three "Important" (MS05-016 – MS05-018) updates. Software affected includes: Windows Server 2003, Windows XP SP1 and SP2, Windows XP 64-Bit Edition SP1 and 2003 (Itanium), Windows 2000 SP3 and SP4, Windows ME, Windows 98 SE, Windows 98, Internet Explorer, Word, Works Suite, Exchange Server 2003, 2003 SP1 and 2000 SP3, and MSN Messenger 6.2. Impact ranges from Denial of Service to remote code execution. Updates are available through the Source link and the US-CERT has provided additional information in "Technical Cyber Security Alert TA05-102A: Multiple Vulnerabilities in Microsoft Windows Components." US-CERT Website: http://www.us-cert.gov/cas/techalerts/TA05-102A.html

---

Category 21.1 *General QA failures*

2005-04-13 **Lotus Notes/Domino multiple vulnerabilities denial of service DoS system compromise attack update issued**

DHS IAIP Daily; http://secunia.com/advisories/14879/

LOTUS NOTES/DOMINO MULTIPLE VULNERABILITIES

Some vulnerabilities have been reported in Lotus Notes/Domino, which can be exploited by malicious people to cause a Denial of Service or compromise a vulnerable system. These vulnerabilities are due to boundary and format string errors. Update to Lotus Notes and Domino release 6.5.4 or 6.0.5.

Category 21.1 *General QA failures*

2005-04-19 **Concurrent Versioning System CVS buffer overflow memory leak vulnerability code execution denial of service DoS attack update issued**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2005/Apr/1013759.html

CVS BUFFER OVERFLOWS AND MEMORY LEAKS MAY LET REMOTE USERS EXECUTE ARBITRARY CODE OR DENY SERVICE

Several vulnerabilities were reported in Concurrent Versions System (CVS). A remote user may be able to trigger a buffer overflow and execute arbitrary code on the target system or cause the CVS service to crash. Some memory allocation, memory leak, and NULL pointer errors also exist and may allow a remote user to cause denial of service conditions. Fix available (1.11.20 stable version; 1.12.12 feature version): https://ccvs.cvshome.org/servlets/ProjectDownloadList

---

Category 21.1 *General QA failures*

2005-04-21 **Netref file creation vulnerability system compromise no update issued**

DHS IAIP Daily; http://secunia.com/advisories/15040/

NETREF FILE CREATION VULNERABILITY

A vulnerability in Netref, which can be exploited by malicious people to compromise a vulnerable system. Input passed to the "ad_direct" and "m_for_racine" parameters in "script/cat_for_gen.php" isn't properly verified before being used. This can be exploited to create a file with an arbitrary filename where the content can be controlled. No vendor solution is currently available.

Category 21.1 *General QA failures*

2005-04-21 **MySQL multiple remote vulnerabilities corrupt file malicious library execution attack update issued**

DHS IAIP Daily; http://www.securityfocus.com/bid/12781/discussion/

MYSQL AB MYSQL MULTIPLE REMOTE VULNERABILITIES

MySQL is reported prone to multiple vulnerabilities that can be exploited by a remote authenticated attacker to corrupt files with the privileges of the MySQL process, to manipulate functions in order to control sensitive data structures, and to execute a malicious library in the context of the MySQL process. Vendor solutions are available through Source link.

Category 21.1 *General QA failures*

2005-04-25 **MySQL MaxDB stack buffer overflow vulnerabilities command execution update issued**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/0389

MYSQL MAXDB WEBTOOL REMOTE STACK OVERFLOW VULNERABILITIES

Two vulnerabilities were identified in MySQL MaxDB, which may be exploited by remote attackers to execute arbitrary commands. These vulnerabilities are due to a stack overflow error and a lack of bounds checking. Update to MySQL MaxDB version 7.5.00.26: http://dev.mysql.com/downloads/maxdb/7.5.00.html

---

Category 21.1 *General QA failures*

2005-04-27 **NetTerm NetFtpd buffer overflow vulnerability command execution attack update issued**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/0407

NETTERM NETFTPD REMOTE USER AUTHENTICATION BUFFER OVERFLOW

A buffer overflow vulnerability was identified in NetFtpd, which could be exploited by remote attackers to execute arbitrary commands. The flaw resides in the authentication procedure and occurs when handling a specially crafted USER command, which could be exploited by a remote attacker to execute arbitrary code and compromise a vulnerable system. Upgrade to NetTerm version 5.1.1.1 or remove the NetFtpd application.

Category 21.1 *General QA failures*

2005-04-27 **Oracle multiple product vulnerabilities code execution information disclosure denial of service DoS attack alert**

DHS IAIP Daily; http://www.us−cert.gov/cas/techalerts/TA05−117A.html

ORACLE PRODUCTS CONTAIN MULTIPLE VULNERABILITIES

Various Oracle products and components are affected by multiple vulnerabilities. The impacts of these vulnerabilities include unauthenticated, remote code execution, information disclosure, and denial of service. Oracle released a Critical Patch Update in April that addresses more than seventy vulnerabilities in different Oracle products and components. The Critical Patch Update provides information about which components are affected, what access and authorization are required, and how data confidentiality, integrity, and availability may be impacted. US-CERT strongly recommends that sites running Oracle review the Critical Patch Update, apply patches, and take other mitigating action as appropriate. Critical Patch Update: http://www.oracle.com/technology/deploy/security/pdf/cpuapr2 005.pdf

---

Category 21.1 *General QA failures*

2005-05-30 **vulnerability hole Microsoft Windows operating system OS Remote Desktop protocol server private key disclosure DLL public key hardcoding design error no solution**

DHS IAIP Daily; http://www.securityfocus.com/bid/13818/info/

MICROSOFT WINDOWS REMOTE DESKTOP PROTOCOL SERVER PRIVATE KEY DISCLOSURE VULNERABILITY

The vulnerability presents itself because a private key that is used to sign the Terminal Server public key is hardcoded in a DLL. This allows the attacker to disclose the key and calculate a valid signature to carry out man in the middle attacks. An attacker could therefore cause the client to connect to a server under their control and send the client a public key to which they possess the private key. There is no solution at this time.

Category 21.1 *General QA failures*

2005-05-31 **vulnerability hole MyBB bulletin board cross-site scripting SQL injection user input checking database exploitation**

DHS IAIP Daily; http://www.securityfocus.com/bid/13827

MYBB MULTIPLE CROSS-SITE SCRIPTING AND SQL INJECTION VULNERABILITIES

MyBB is prone to multiple cross-site scripting and SQL injection vulnerabilities. These issues are due to a failure in the application to properly sanitize user supplied input. The application is prone to multiple SQL injection vulnerabilities. Successful exploitation could result in a compromise of the application, disclosure or modification of data, or may permit an attacker to exploit vulnerabilities in the underlying database implementation. Updates available at: http://mybboard.com/community/attachment.php?aid=862

Category 21.1 *General QA failures*

2005-05-31 **vulnerability hole Microsoft Windows operating system OS Hyperlink Object Library buffer overflow arbitrary code execution privilege execution**

DHS IAIP Daily; http://www.securityfocus.com/bid/12479

MICROSOFT WINDOWS HYPERLINK OBJECT LIBRARY BUFFER OVERFLOW VULNERABILITY

The Microsoft Windows Hyperlink Object Library is reported prone to a buffer overflow vulnerability. An attacker may exploit this condition to execute arbitrary code on a vulnerable computer, which may grant unauthorized access to the computer or lead to privilege escalation. It is reported that issue presents itself when a user follows a malformed link specially crafted by an attacker, however, other attack vectors also exist to exploit this vulnerability. Specifically, an application that employs the affected library by accepting and supplying parameters to the library may allow an attacker to exploit this vulnerability remotely and without user interaction. Updates available through Source link below.

Category 21.1 *General QA failures*

2005-05-31 **vulnerability hole PHP4 PHP5 SSI local remote arbitrary code execution vendor solutions**

DHS IAIP Daily; http://www.securityfocus.com/bid/11964

PHP MULTIPLE LOCAL AND REMOTE VULNERABILITIES

PHP4 and PHP5 are reported prone to multiple local and remote vulnerabilities that may lead to code execution within the context of the vulnerable process. PHP safe_mode_exec_dir is reported prone to an access control bypass vulnerability. A local attacker that can manipulate the directory name from which the PHP script is called, may bypass 'safe_mode_exec_dir' restrictions by placing shell metacharacters and restricted commands into the directory name of the current directory. This may allow them to gain access to potentially sensitive information, such as database credentials. Refer to Source link below for vendor solutions.

Category 21.1 *General QA failures*

2005-06-01 **vulnerability hole PeerCast URL remote format string arbitrary command execution denial-of-service DoS solution upgrade**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/0651

PEERCAST MALFORMED URL REMOTE FORMAT STRING VULNERABILITY

A vulnerability was identified in PeerCast, which may be exploited by remote attackers to execute 10 arbitrary commands or cause a denial of service. This flaw is due to a format string error when handling specially crafted HTTP requests (port 7144), which may be exploited by remote attackers to crash or compromise a vulnerable server. Upgrade to PeerCast version 0.1212: http://www.peercast.org/download.php

---

Category 21.1 *General QA failures*

2005-06-01 **vulnerability hole Symantec Brightmail AntiSpam information disclosure remote database access**

DHS IAIP Daily; http://www.securityfocus.com/bid/13828

SYMANTEC BRIGHTMAIL ANTISPAM REMOTE INFORMATION DISCLOSURE VULNERABILITY

Symantec Brightmail AntiSpam is susceptible to a remote information disclosure vulnerability. This issue is due to a failure of the application to properly ensure that remote database access is properly disabled. Original advisory and updates: http://securityresponse.symantec.com/avcenter/security/Conte nt/2005.05.31a.html

---

Category 21.1 *General QA failures*

2005-06-01 **vulnerability hole NASM IEEE_PUTASCII buffer overflow unauthorized access**

DHS IAIP Daily; http://www.securityfocus.com/bid/13506

NASM IEEE_PUTASCII REMOTE BUFFER OVERFLOW VULNERABILITY

NASM is prone to a remote buffer overflow vulnerability. An attacker exploits this issue by crafting a malicious source file to be assembled by the application. This file is sent to an affected user and if the user loads the file in NASM, the attack may result in arbitrary code execution. The attacker may then gain unauthorized access in the context of the user running NASM. Refer to Source link below for vendor solutions.

Category 21.1 *General QA failures*

2005-06-01 **vulnerability Microsoft Outlook Express file processing extension obfuscation**

DHS IAIP Daily; http://www.securityfocus.com/bid/13837/info

MICROSOFT OUTLOOK EXPRESS ATTACHMENT PROCESSING FILE EXTENSION OBFUSCATION VULNERABILITY

Microsoft Outlook Express is prone to an attachment file extension obfuscation vulnerability that may present a risk under certain configurations. Reports indicate that this may be leveraged to make the attached email message executable. It is possible to cause a default file handler to be invoked to process the attached email message and potentially allowing for code execution. This issue may lure a victim into a false sense of security and may result in inadvertent or unintentional execution of attacker supplied code. There is no solution at this time.

Category 21.1 *General QA failures*

2005-06-04 **remote vulnerability hole Bluetooth Protocol device pairing PIN no solution**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/0689

BLUETOOTH PROTOCOL DEVICE PAIRING PROCESS REMOTE VULNERABILITY

A vulnerability was identified in the Bluetooth Protocol, which may be exploited by remote attackers to bypass certain security measures. This flaw is due to a design error in the pairing process initialized by two Bluetooth devices in order to create a shared secret value, which may be exploited by an attacker to force the repairing process, determine a valid link key, crack the PIN (Personal Identification Number) and potentially hijack all the messages transferred between two Bluetooth devices. There is no solution at this time.

Category 21.1 *General QA failures*

2005-06-06 **vulnerability hole Sun Solaris privilege escalation**

DHS IAIP Daily; http://securitytracker.com/alerts/2005/Jun/1014108.html

SUN SOLARIS LIBC __INIT_SUID_PRIV() LETS LOCAL USERS GAIN ELEVATED PRIVILEGES

A vulnerability was reported in libc and libproject on Sun Solaris. A local user may be able to gain elevated privileges. A local user can invoke libproject(3LIB) to trigger a flaw in the libc(3LIB) __init_suid_priv() function and gain elevated privileges. Original advisory and update: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101 740-1

Category 21.1 *General QA failures*

2005-06-06 **vulnerability hole PortailPHP SQL injection exploit database implementation**

DHS IAIP Daily; http://www.securityfocus.com/bid/13708/exploit

PORTAILPHP ID PARAMETER SQL INJECTION VULNERABILITY

PortailPHP is prone to an SQL injection vulnerability. Successful exploitation could result in a compromise of the application, disclosure or modification of data, or may permit an attacker to exploit vulnerabilities in the underlying database implementation. No solution is currently available.

Category 21.1 *General QA failures*

2005-06-07 **vulnerability hole input validation user input sanitization failure arbitrary code execution PHP cross-site scripting information access solution upgrade**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/0697

FLATNUKE MULTIPLE INPUT VALIDATION VULNERABILITIES

Multiple input validation vulnerabilities reportedly affect FlatNuke. These issues are due to a failure of the application to properly sanitize user supplied input prior to using it in application critical actions such as generating Web content or loading scripts. An attacker may leverage these issues to execute arbitrary PHP code, execute client side script code in the browsers of unsuspecting users through cross site scripting attacks, and gain access to sensitive information. Other attacks are also possible. Upgrade to FlatNuke version 2.5.4: http://sourceforge.net/project/showfiles.php?group_id=93076& package_id=98622

Category 21.1 *General QA failures*

2005-06-08 **vulnerability hole IBM AIX operating system buffer overflow arbitrary code execution no solution**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2005/Jun/1014132.html

IBM AIX BUFFER OVERFLOWS LET LOCAL USERS EXECUTE ARBITRARY CODE

Several vulnerabilities were reported in IBM's AIX operating system, affecting the vscout, paginit, diagTasksWebSM, getlvname, and swcons commands and multiple "p" commands. A local user can supply specially crafted command line parameters to trigger a buffer overflow in the invscout, paginit, diagTasksWebSM, getlvname, and swcons commands and execute arbitrary code, potentially with root privileges. No solution is currently available.

Category 21.1 *General QA failures*

2005-06-09 **software vulnerability tcpdump BGP decoding infinite loop denial-of-service DoS ISIS packets**

DHS IAIP Daily; http://www.securityfocus.com/advisories/8671

TCPDUMP BGP DECODING ROUTINES DENIAL OF SERVICE VULNERABILITY

TCPDUMP is prone to a vulnerability that may allow a remote attacker to cause a denial of service condition in the software. The issue occurs due to the way tcpdump decodes Border Gateway Protocol (BGP) packets. A remote attacker may cause the software to enter an infinite loop by sending malformed ISIS packets resulting in the software hanging. Updates are available from vendors.

Category 21.1 *General QA failures*

2005-06-09 **vulnerability hole IBM AIX operating system buffer overflow arbitrary code execution no solution**

DHS IAIP Daily; http://www.securityfocus.com/bid/13914/discuss

IBM AIX GETLVNAME COMMAND LINE ARGUMENT LOCAL BUFFER OVERFLOW VULNERABILITY

IBM AIX getlvname is prone to a local buffer overflow vulnerability. A buffer overflow exists in the handling of the commandline arguments to getlvname. When parsing and concatenating the supplied arguments a length parameter is not checked and a typical overflow occurs. A successful attack allows arbitrary machine code execution with super user privileges, facilitating privilege escalation. Vendor solution is pending.

Category 21.1 General QA failures

2005-06-09 **vulnerability Cisco Voice VLAN 802.1x authentication bypass CDP packet spoofing**

DHS IAIP Daily; http://www.securityfocus.com/bid/13902/discuss

CISCO VOICE VLAN 802.1X AUTHENTICATION BYPASS VULNERABILITY

Cisco switches are susceptible to an authentication bypass vulnerability, allowing attackers to gain anonymous access to the voice VLAN. Attackers may spoof CDP packets, and impersonate a Cisco IP phone, in order to anonymously join the voice VLAN. This allows attackers to gain access to network resources without the expected 802.1x authentication sequence. As network administrators expect that switch port access is restricted to only authenticated users, a false sense of security may pervade. Vendor advisory and workarounds: http://www.cisco.com/warp/public/707/cisco-sn-20050608-8021x .shtml

---

Category 21.1 General QA failures

2005-06-13 **vulnerability eTrace plugin shell command no solution**

DHS IAIP Daily; http://secunia.com/advisories/15678/

E107 ETRACE PLUGIN SHELL COMMAND INJECTION VULNERABILITY

A vulnerability in the eTrace plugin for e107, which can be exploited by malicious people to compromise a vulnerable system. Input passed to the "etrace_cmd" and "etrace_host" parameters in "dotrace.php" isn't properly sanitized before being used in a "system()" call. This can be exploited to inject arbitrary shell commands. There is no solution at this time.

Category 21.1 General QA failures

2005-06-14 **Microsoft June 2005 security bulletin ten updates**

DHS IAIP Daily; http://www.microsoft.com/technet/security/bulletin/ms05−jun.
mspx

MICROSOFT ISSUES JUNE SECURITY BULLETIN

Microsoft issued its security update for June on Tuesday, June 14. Of the ten updates (MS05-025 – MS05-034) issued for June, three are critical, four are important, and three are moderate. Affected products and components are Internet Explorer, Windows HTML Help, Windows Server Message Block, Web Client Server, Outlook Web Access for Exchange Server, Outlook Express, Step-by-Step Interactive Training, Microsoft Agent, Telnet Client, and ISA Server 2000. Impacts include remote code execution, information disclosure, and escalation of privilege. See Source link and individual bulletins for updates.

Category 21.1 General QA failures

2005-06-15 **vulnerability hole Bitrix Site Manager exploit Web server arbitrary code execution no solution**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/0779

BITRIX SITE MANAGER REMOTE PHP FILE INCLUSION VULNERABILITY

A vulnerability was identified in Bitrix Site Manager, which may be exploited by attackers to compromise a vulnerable web server. This flaw is due to an input validation error in the "index.php" script when processing a specially crafted "SERVER[DOCUMENT_ROOT]" variable, which may be exploited by attackers to include arbitrary files and execute remote commands with the privileges of the web server. There is no solution at this time.

Category 21.1 General QA failures

2005-06-16 **vulnerability hole ultimate PHP Board weak password encryption no solution**

DHS IAIP Daily; http://www.securityfocus.com/bid/13975

ULTIMATE PHP BOARD WEAK PASSWORD ENCRYPTION VULNERABILITY

Ultimate PHP Board is prone to a weak password encryption vulnerability. This issue is due to a failure of the application to protect passwords with a sufficiently effective encryption scheme. This issue may allow a malicious user to gain access to user and administrator passwords for the affected application. There is no solution at this time.

Category 21.1 General QA failures

2005-06-16 **vulnerability gedit filename format string arbitrary code execution**

DHS IAIP Daily; http://www.securityfocus.com/bid/13699/solution

GEDIT FILENAME FORMAT STRING VULNERABILITY

gEdit is prone to a format string vulnerability. Exploitation may occur when the program is invoked with a filename that includes malicious format specifiers. This issue could be exploited to corrupt arbitrary regions of memory with attacker supplied data, potentially resulting in execution of arbitrary code in the context of the user running the program. See Source link below for vendor updates.

Category 21.1 General QA failures

2005-06-17 **vulnerability Sun Messaging server HTML injection attack no solution**

DHS IAIP Daily; http://sunsolve.sun.com/search/document.do?assetkey=1−26−101 770−1

SUN ONE/IPLANET MESSAGING SERVER WEBMAIL MSIE HTML INJECTION VULNERABILITY

Sun ONE/iPlanet Messaging Server Webmail is prone to an HTML injection vulnerability. This issue may allow a remote attacker to inject hostile HTML and script code into the session of a Webmail user. Sun has stated that this issue only affects users who access Webmail with Internet Explorer. There is no solution at this time.

Category 21.1 General QA failures

2005-06-17 **vulnerability hole Adobe Reader 7 XML Eternal Entity XXE JavaScript PDF update issued**

DHS IAIP Daily; http://www.zone−h.org/advisories/read/id=7674

ADOBE READER 7 VULNERABLE TO XML EXTERNAL ENTITY (XXE) ATTACK

Recent versions of Adobe Reader are vulnerable to XML External Entity (XXE) attacks. By including a JavaScript in a PDF file, and having this JavaScript parse an embedded XML document with a reference to an external entity, it is possible to read certain types of text files on the local computer, and have them sent to a remote attacker. Original advisory and updates available: http://www.adobe.com/support/techdocs/331710.html

---

Category 21.1 General QA failures

2005-06-20 **vulnerability hole Cisco VPN 3000 remote user valid groupnames updated version issued**

DHS IAIP Daily; http://securitytracker.com/alerts/2005/Jun/1014246.html

CISCO VPN 3000 LETS REMOTE USERS DETERMINE VALID GROUPNAMES

A vulnerability was reported in the Cisco VPN 3000 concentrators. A remote user can determine valid groupnames. When groupname authentication is used, the system provides a different response to a connection request with a valid groupname than it does with an invalid groupname. A remote user can connect to the target system repeatedly and send an IKE Aggressive Mode packet using different groupnames to attempt to determine valid groupnames. The system will respond only to packets with a valid groupname. The vendor has released a fixed version (4.1.7.F).

Category 21.1 General QA failures

2005-06-21 **vulnerability SpamAssassin remote denial-of-service DoS**

DHS IAIP Daily; http://www.securityfocus.com/bid/13978/solution

SPAMASSASSIN MALFORMED EMAIL HEADER REMOTE DENIAL OF SERVICE VULNERABILITY

SpamAssassin is prone to a remote denial of service vulnerability. This issue is due to a failure of the application to properly handle overly long email headers. An attacker may cause SpamAssassin to take inordinate amounts of time to check a specially crafted email message. By sending many malicious messages, it may be possible for attackers to cause extremely large delays in email delivery, denying service to legitimate users. See Source link for solution.

Category 21.1 *General QA failures*

2005-06-22 **vulnerability hole Veritas Backup remote heap overflow privilege escalation update issued**

DHS IAIP Daily; http://www.securityfocus.com/bid/14023/solution

VERITAS BACKUP EXEC ADMIN PLUS PACK OPTION REMOTE HEAP OVERFLOW VULNERABILITY

Veritas Backup Exec is affected by a remote heap overflow vulnerability. A remote attacker can exploit this issue by crafting and sending malicious data to the service and executing arbitrary code. Successful exploitation may result in a super user compromise. Original advisory and updates: http://seer.support.veritas.com/docs/276607.htm

---

Category 21.1 *General QA failures*

2005-06-22 **vulnerability hole Ipswitch WhatsUp Professional SQL injection data modification update issued**

DHS IAIP Daily; http://www.securityfocus.com/bid/14039/discuss

IPSWITCH WHATSUP PROFESSIONAL LOGIN.ASP SQL INJECTION VULNERABILITY

WhatsUp Professional is prone to an SQL injection vulnerability affecting its Web based front end. Successful exploitation could result in a compromise of the application, disclosure or modification of data, or may permit an attacker to exploit vulnerabilities in the underlying database implementation. The vendor has released WhatsUp Professional 2005 SP1a to address this issue.

Category 21.1 *General QA failures*

2005-06-22 **vulnerability hole Sun Java Web Start unauthorized access**

DHS IAIP Daily; http://www.securityfocus.com/bid/12847/solution

SUN JAVA WEB START SYSTEM PROPERTY TAGS REMOTE UNAUTHORIZED ACCESS VULNERABILITY

A remote unauthorized access vulnerability affects Java Web Start. This issue is due to a failure of the application to properly validate user supplied input prior to considering it as trusted. An attacker may leverage this issue to gain unauthorized read and write access to affected computers. Other attacks may also be possible. It should be noted that unauthorized access granted in this way will be with the privileges of the unsuspecting user that visits a malicious Website. See Source link for solutions.

Category 21.1 *General QA failures*

2005-06-24 **vulnerability hole Sun Solaris operating system local buffer overflow**

DHS IAIP Daily; http://www.securityfocus.com/bid/14049/info

SUN SOLARIS TRACEROUTE MULTIPLE LOCAL BUFFER OVERFLOW VULNERABILITIES

Sun Solaris traceroute is affected by multiple local buffer overflow vulnerabilities. These vulnerabilities present themselves when the application handles excessive data supplied through command line arguments. These issue are reported to affect /usr/sbin/traceroute running on Sun Solaris 10. Some reports indicate that this issue cannot be reproduced. It is also reported that this issue is only exploitable on the Solaris x86 platform.

Category 21.1 *General QA failures*

2005-06-24 **vulnerability hole IBM DB2 Universal Database authorization bypass fixes issued**

DHS IAIP Daily; http://www.securityfocus.com/bid/14057/info

IBM DB2 UNIVERSAL DATABASE UNSPECIFIED AUTHORIZATION BYPASS VULNERABILITY

IBM DB2 Universal Database is susceptible to an authorization bypass vulnerability. This issue is due to a failure of the application to properly enforce authorization restrictions for database users. Users with SELECT privileges on in a database may bypass authorization checks to execute INSERT, UPDATE, or DELETE statements. Further details are not available at this time. This BID will be updated as more information is disclosed. This vulnerability allows attackers to modify or destroy data without having proper authorization to do so. IBM has released an advisory, along with fixes to address this issue.

Category 21.1 *General QA failures*

2005-06-25 **software quality assurance QA bug flaw error usability**

RISKS; http://tinyurl.com/bdrm3 23 92

JCAHO SOFTWARE BUG CONFUSES HOSPITALS

Joint Commission Resources, a unit of the Joint Commission on Accreditation of Healthcare Organizations that enforces quality standards for hospitals found a flaw in software that it had sold to more than 1,000 hospitals that helps qualify for accreditation and payments from Medicare. The problem was a missing identification marker that alerts a hospital to the 250 standards among the 1,300 that the commission and its auditors regard as essential.

[Abstract by Peter G. Neumann]

Category 21.1 *General QA failures*

2005-06-28 **vulnerability hole phpBB remote PHP code execution**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/0904

PHPBB "VIEWTOPIC.PHP" REMOTE PHP CODE EXECUTION VULNERABILITY

A vulnerability was identified in phpBB, which may be exploited by attackers to compromise a vulnerable web server. This flaw is due to an input validation error in the "viewtopic.php" script that does not properly filter the "highlight" parameter before calling the "preg_replace()" function, which may be exploited by remote attackers to execute arbitrary PHP commands with the privileges of the web server. Solution: http://www.phpbb.com/downloads.php

---

Category 21.1 *General QA failures*

2005-06-28 **vulnerability hole CSV DB arbitrary command execution**

DHS IAIP Daily; http://secunia.com/advisories/15842/

CSV_DB / I_DB ARBITRARY COMMAND EXECUTION VULNERABILITY

A vulnerability has been reported in CSV_DB 1.0, which can be exploited by malicious people to execute arbitrary commands. Input passed to the "file" parameter in csv_db.cgi is not properly sanitized before being used. This can be exploited to execute arbitrary commands on the server by appending the commands to the end of the "file" parameter using the pipe character. The vendor has confirmed that the vulnerability also affects i_DB version 1.0.

Category 21.1 *General QA failures*

2005-07-14 **software quality assurance QA design flaw bounds checking impossible values data integrity nonsense sanity**

RISKS; http://www.cnn.com/2005/US/07/14/hot.summer.ap/index.html 23 94

TORRENTIAL METER ERROR

The utility department in Mascoutah (Illinois) sent Rose Mary Cook a bill for the use of 10 million gallons of water in a month, totalling $29,787 for the water and $43,581 for the ensuing sewer usage. The cause was not surprisingly the result of a broken meter.

[Abstract by Peter G. Neumann, who ask, "Why doesn't meter reading use sanity checking?"]

[MK adds that teachers of systems design and programming should drill their students in the principle that all inputs should be checked for reasonableness. For example, 10M gallons in, say, 30 days implies a continuous flow of almost 4 gallons _per second_ throughout the month. A well written program would have flagged the data error before sending the monstrous bill.]

Category 21.1 *General QA failures*

2005-07-17 **data corruption database medical records admissions consults disaster plan backups continuity planning failure catastrophe acquisition**

RISKS 23 94

LISBON HOSPITAL RECORDS SYSTEM DOWN 10 DAYS DUE TO DATABASE CRASH

Lisbon newspaper "O Público" reports today that the main information system for the Lisbon Hospital Center, which supports three large Lisbon hospitals, has not worked since July 8. It appears that the master patient index has become inaccessible, and may be lost. If a patient shows up without a hospital-issued card, which includes a patient id number, the patient's records cannot be accessed. Out- patient consultations and admissions are being processed manually, causing "great confusion." Emergency room admissions are much slower than usual. The waiting list for surgery also appears lost, although that has not been confirmed. A doctor at one of the hospitals and board member for a doctors union said that "No one knows for certain what will happen or when the problem will be solved." The assistant to the director of the hospital group explains that "The system failed totally eight days ago, and technicians tried to restore it immediately, but without success. At the beginning of last week, the US firm who supplied the system was brought in, and it is expected that the situation will be resolved by Monday." He also said that the failure was unexpected, that the hospital group did not the ability to fix it on their own, and that the breakdown "has had no impact on the normal functioning of the hospitals, except for the slowdown in patient registration."

So, it takes much longer to admit patients, their medical records are inaccessible unless they have registered before and bring with them their registration card (something that anyone dealing with a medical emergency will for sure remember to do), and doctors report confusion, but there's really no impact, according to the hospital group administration. A mission-critical system has no backup or immediate access to repair expertise.

For readers not familiar with Portugal, Lisbon public hospitals are notorious for poor financing, inefficiency, bureaucracy, and long waiting lists. They cater mostly to those who cannot afford private care, especially many pensioners in an aging city. Another common problem with public institutions in Portugal are poor procurement controls, especially for technology and informations services. Many purchases are made without much attention to cost of ownership, service guarantees, or access to parts and service. Some administrators are too easily seduced by fancy presentations by local representatives of foreign suppliers who have no local expertise or staying power.

[Report by Fernando Pereira]

Category 21.1 *General QA failures*

2005-07-24 **hacker vulnerability disclosure reward discovery TippingPoint**

EDUPAGE; http://news.com.com/2100-7350_3-5802411.html

PAYING HACKERS FOR BUGS

Computer-security firm TippingPoint has begun a program to pay rewards to individuals who report computer vulnerabilities. Not unlike similar programs from other companies, the TippingPoint deal offers a variable amount of money if a reported bug proves valid. The company will use the information to update its own protection software and will notify the maker of the vulnerable product about the problem. David Endler, director of security research at TippingPoint, said the reward program is intended to "reward and encourage independent security research" and to "ensure responsible disclosure of vulnerabilities." Not all security companies believe in bounties. Internet Security Systems, for one, said that paying for such bug reports amounts to having hackers do a company's research for it. An official from Internet Security Systems also noted that the bugs reported in such programs are typically very low-level problems, saying that the more extreme vulnerabilities are worth much more when used for hacking than if turned in to security companies. CNET, 24 July 2005

Category 21.1 *General QA failures*

2005-07-28 **vulnerability hole MySQL remote code execution compromise system**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1250

MYSQL EVENTUM PEAR XML_RPC REMOTE CODE EXECUTION VULNERABILITY

A vulnerability was identified in MySQL Eventum, which could be exploited by remote attackers to execute arbitrary commands. This flaw is due to an input validation error in the PEAR XML_RPC library when processing specially crafted XML documents, which could be exploited by attackers to compromise a vulnerable system. MySQL Eventum version 1.5.4 and prior are affected. Users should upgrade to MySQL Eventum version 1.5.5: http://dev.mysql.com/downloads/other/eventum/index.html

---

Category 21.1 General QA failures

2005-07-28 **vulnerability hole FileZilla Server Zlib library remote buffer overflow code execution**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1249

FILEZILLA SERVER ZLIB LIBRARY REMOTE BUFFER OVERFLOW VULNERABILITY

A vulnerability was identified in FileZilla Server, which could be exploited by remote attackers to cause a denial of service or execute arbitrary commands. This flaw is due to a buffer overflow error in the Zlib library when decompressing specially crafted data streams, which could be exploited, via a malformed stream embedded within network communication, to execute arbitrary commands. The vendor has stated that remote code execution was not possible since zlib was compiled with enabled buffer overflow protection. FileZilla Server versions prior to 0.9.9 are affected. Users should upgrade to FileZilla Server version 0.9.9 : http://sourceforge.net/project/showfiles.php?group_id=21558& package_id=21737

Category 21.1 General QA failures

2005-07-29 **vulnerability hole PHPmyGallery file inclusion system compromise**

DHS IAIP Daily; http://secunia.com/advisories/16260/

PHPMYGALLERY "CONFDIR" FILE INCLUSION VULNERABILITY

A vulnerability has ben discovered in PHPmyGallery which can be exploited by malicious people to compromise a vulnerable system. Input passed to the "confdir" parameter in "common-tpl-vars.php" isn't properly verified, before it is used to include files. This can be exploited to include arbitrary files from external and local resources. Successful exploitation requires that "register_globals" is enabled. The vulnerability has been reported in version 1.5 beta and prior (latest affected stable version is 0.995). The vendor recommends restricting access to the "_conf" directory. The vulnerability will reportedly be fixed in the upcoming 1.5 beta 2 version.

Category 21.1 General QA failures

2005-07-29 **vulnerability hole Novell eDirectory NMAS password bypass update issued**

DHS IAIP Daily; http://secunia.com/advisories/16267/

NOVELL EDIRECTORY NMAS PASSWORD CHALLENGE BYPASS

A security issue has been reported in Novell eDirectory, which can be exploited by malicious people to bypass certain security restrictions. The problem is caused due to an error in the NMAS (Novell Modular Authentication Service) component in the Forgotten Password portal. This makes it possible to change a user's password without answering the challenge question. Users should update to NMAS version 2.3.8. Original Advisory and patch:http://support.novell.com/cgi-bin/search/searchtid.cgi ?/2971485.htm

---

Category 21.1 General QA failures

2005-07-29 **open vulnerability disclosure Cisco router software Michael Lynn litigation**

EDUPAGE; http://www.siliconvalley.com/mld/siliconvalley/12255870.htm

CISCO AND SECURITY RESEARCHER AGREE TO DISAGREE

Security researcher Michael Lynn and Cisco Systems have reached an agreement that should put an end to Cisco's legal action against Lynn for speaking publicly about a flaw in the company's router software. Lynn, who until Wednesday was employed by Internet Security Systems (ISS), gave a presentation at the Black Hat Conference discussing the vulnerability. Cisco and ISS had discouraged Lynn from giving the presentation, saying that a patch had been issued for the flaw. Lynn believed Cisco had not been open with consumers about the severity of the problem, and he resigned from ISS to protest the company's position that he should not give the presentation. After he left ISS, however, Lynn faced legal action from Cisco, which argued that he had no right to make the presentation since he was no longer employed by ISS. Under the agreement, Lynn will stop disclosing information about the flaw, and the legal action will be canceled. Computer security expert Bruce Schneier applauded Lynn for his conviction in exposing what he thought was a serious flaw despite the risks of going public. Matt Bishop, professor of computer science at the University of California-Davis, said he sees the practice of exposing flaws publicly as a dangerous practice and that working with the affected vendor is preferable. San Jose Mercury News, 29 July 2005

Category 21.1 General QA failures

2005-08-02 **vulnerability hole BusinessMail SMTP denial-of-service DoS**

DHS IAIP Daily; http://secunia.com/advisories/16306/

BUSINESSMAIL SMTP DENIAL OF SERVICE VULNERABILITY

A vulnerability has been discovered in BusinessMail, which can be exploited by malicious people to cause a DoS (Denial of Service). The vulnerability is caused due to an error in the SMTP service, and can be exploited to cause the service to stop responding via an overly long user name in the "MAIL FROM" command. The vulnerability has been confirmed in BusinessMail version 4.6 (SMTP server 4.61.02). Other versions may also be affected.

Category 21.1 General QA failures

2005-08-02 **vulnerability BrightStor backup buffer overflow arbitrary code execution solution**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1305

COMPUTER ASSOCIATES BRIGHTSTOR BACKUP AGENTS BUFFER OVERFLOW ISSUE

A vulnerability was identified in Computer Associates BrightStor ARCserve Backup and BrightStor Enterprise Backup Agents, which may be exploited by remote attackers to execute arbitrary commands or cause a denial of service. This flaw is due to a stack overflow error when a string with a length over 3168 bytes is sent to port 6070, which may be exploited by unauthenticated attackers to run arbitrary code with SYSTEM privileges. Solutions: http://supportconnect.ca.com/sc/solcenter/sol_search.jsp

---

Category 21.1 General QA failures

2005-08-02 **vulnerability hole JID remote buffer overflow strings update issued**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1286

JABBERD "JID.C" JID HANDLING REMOTE BUFFER OVERFLOW VULNERABILITIES

Three vulnerabilities were identified in jabberd, which could be exploited by remote attackers to execute arbitrary code or cause a denial of service. These flaws are due to buffer overflow errors in "jid.c" when processing JID strings with long components (user, host or resource), which may be exploited to compromise a vulnerable system or cause a DoS. jabberd versions prior to 2.0s9 are affected. Users should upgrade to jabberd version 2.0s9: http://jabberd.jabberstudio.org/2/

Category 21.1 General QA failures

2005-08-03 **vulnerability multiple Openview Oracle arbitrary command execution SQL injection attack**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1316

ORACLE FOR OPENVIEW (OFO) MULTIPLE SECURITY VULNERABILITIES

Multiple vulnerabilities were identified in Oracle for Openview (OfO), which could be exploited by remote or local attackers to execute arbitrary commands or conduct SQL injection attacks. These flaws, initially reported in Oracle Critical Patch Update (July 2005), could be exploited by remote or local attackers to cause a denial of service, execute arbitrary commands or conduct SQL injection attacks. OfO customers who have support contracts directly from Oracle should obtain the Critical Patch Update (July 2005) from Oracle: http://www.oracle.com/technology/deploy/security/pdf/cpujul2 005.html OfO customers who have support from Hewlett-Packard should contact the normal support channel to obtain the Critical Patch Update (July 2005): http://www.hp.com/managementsoftware/contract_maint

---

Category 21.1 General QA failures

2005-08-06 **vulnerability hole PHP-Fusion SQL injection exploit database implementation**

DHS IAIP Daily; http://www.securityfocus.com/bid/14489/info

PHP-FUSION MESSAGES.PHP SQL INJECTION VULNERABILITY

PHP-Fusion is prone to an SQL injection vulnerability. This issue is due to a failure in the application to properly sanitize user-supplied input to the 'messages.php' script before using it in an SQL query. Successful exploitation could result in a compromise of the application, disclosure or modification of data, or may permit an attacker to exploit vulnerabilities in the underlying database implementation. Security Focus is not currently aware of any vendor-supplied patches for this issue.

Category 21.1 General QA failures

2005-08-08 **vulnerability MySQL buffer overflow user defined functions**

DHS IAIP Daily; http://www.appsecinc.com/resources/alerts/mysql/2005−002.html

BUFFER OVERFLOW IN MYSQL USER DEFINED FUNCTIONS

User-defined functions in MySQL allow a user in the database to call binary libraries on the operating system. Creating a user-defined function requires insert privileges on the mysql.func table. The init_syms() function uses an unsafe string function to copy a user specified string into a stack based buffer. Due to improper sanitation this buffer is able to be overflowed, overwriting portions of the stack. This allows an attacker to write 14 bytes of arbitrary data and eight bytes of hard coded data beyond the end of the buffer. Exploiting this vulnerability would require the ability to create user-defined functions. This is not typically granted to untrusted users. MySQL versions 4.0.25, 4.1.13, or 5.0.7-beta have been patched: http://dev.mysql.com/downloads/

Category 21.1 General QA failures

2005-08-08 **vulnerability Comdev eCommerce file inclusion system compromise**

DHS IAIP Daily; http://secunia.com/advisories/16346/

COMDEV ECOMMERCE FILE INCLUSION VULNERABILITY

A vulnerability has been discovered in Comdev eCommerce, which can be exploited by malicious people to compromise a vulnerable system. Input passed to the "path[docroot]" parameter is not properly verified, before it is used to include files. This can be exploited to include arbitrary files from external and local resources. Example: http://[host]/oneadmin/config.php?path[docroot]=[file] Successful exploitation requires that "magic_quotes_gpc" is disabled. The vulnerability has been confirmed in version 3.1. Other versions may also be affected. Solution: Edit the source code to ensure that input is properly verified.

Category 21.1 General QA failures

2005-08-08 **vulnerability PHPSiteStats authentication bypass access violation**

DHS IAIP Daily; http://www.securityfocus.com/bid/14493/solution

PHPSITESTATS UNSPECIFIED AUTHENTICATION BYPASS VULNERABILITY

PHPSiteStats is prone to an unspecified authentication bypass vulnerability. A successful attack can allow unauthorized attackers to bypass the authentication routines and gain access to the application. An attacker may then carry out other attacks against the vulnerable computer. PHPSiteStats 1.0 is prone to this issue. Other versions may be vulnerable as well. The vendor has released PHPSiteStats 1.1 to address this issue: http://prdownloads.sourceforge.net/phpsitestats/phpsitestats 1.1.zip?download

---

Category 21.1 General QA failures

2005-08-08 **vulnerability hole SysCP system compromise update issued**

DHS IAIP Daily; http://secunia.com/advisories/16347/

TWO VULNERABILITIES REPORTED IN SYSCP

Two vulnerabilities have been reported in SysCP, which can be exploited by malicious people to compromise a vulnerable system. 1) Input passed to a certain parameter is not properly verified before being used to include a language file. This can be exploited to include arbitrary files from external resources. 2) Input passed to the internal template engine is insufficiently sanitized, which can be exploited to inject arbitrary PHP code. Successful exploitation requires that register_globals is enabled. The vulnerabilities have been reported in versions 1.2.10 and prior. Users should update to version 1.2.11. http://www.syscp.de/wiki/EnDownloads

---

Category 21.1 *General QA failures*

2005-08-09 **patch fix update Red Hat critical Gaim update heap buffer overflow denial-of-service DoS**

DHS IAIP Daily; http://rhn.redhat.com/errata/RHSA−2005−627.html

RED HAT RELEASES CRITICAL GAIM SECURITY UPDATE

An updated gaim package that fixes multiple security issues is now available. A heap based buffer overflow issue was discovered in the way Gaim processes away messages. A remote attacker could send a specially crafted away message to a Gaim user logged into AIM or ICQ that could result in arbitrary code execution. A denial of service issue was also discovered in Gaim. A remote attacker could attempt to upload a file with a specially crafted name to a user logged into AIM or ICQ, causing Gaim to crash. A denial of service bug was found in Gaim's Gadu Gadu protocol handler. A remote attacker could send a specially crafted message to a Gaim user logged into Gadu Gadu, causing Gaim to crash. Please note that this issue only affects PPC and IBM S/390 systems running Gaim. Users of gaim are advised to upgrade to an updated package, which contains backported patches and is not vulnerable to these issues. Before applying this update, make sure all previously released errata relevant to your system have been applied.

Category 21.1 *General QA failures*

2005-08-09 **vulnerability Gravity Board X SQL injection file inclusion no patch**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1349

GRAVITY BOARD X SQL INJECTION AND FILE INCLUSION VULNERABILITIES

Two vulnerabilities have been identified in Gravity Board X, which could be exploited by attackers to include arbitrary files and/or conduct SQL injection and cross site scripting attacks. The first issue is due to an input validation error in the "deletethread.php" script when processing a specially crafted "board_id" parameter, which may be exploited by attackers to cause arbitrary scripting code to be executed by the user's browser. The second vulnerability is due to an input validation error in the "index.php" script that does not properly filter a specially crafted "email" variable, which may be exploited by remote users to conduct SQL injection attacks. The third flaw is due to an input validation error in the "editcss.php" script when processing a specially crafted "csscontent" variable, which could be exploited by attackers to execute arbitrary PHP commands. Gravity Board X version 1.1 and prior are affected. The FrSIRT is not aware of any official supplied patch for this issue.

Category 21.1 *General QA failures*

2005-08-09 **vulnerability AOL client software privilege escalation no patches**

DHS IAIP Daily; http://www.securityfocus.com/bid/14530/discuss

AOL CLIENT SOFTWARE LOCAL PRIVILEGE ESCALATION VULNERABILITY

AOL client software is susceptible to a local privilege escalation vulnerability. This issue is due to a failure of the software to properly secure its installation path against local modifications. This issue allows local users to replace the affected binary with an executable of their choice, allowing them to execute arbitrary code with SYSTEM privileges. This facilitates the complete compromise of the local computer. AOL version 9.0 Security Edition is reported susceptible to this vulnerability; other versions may also be affected. Security Focus is not currently aware of any vendor-supplied patches for this issue.

Category 21.1 *General QA failures*

2005-08-09 **Microsoft patches security vulnerability critical**

DHS IAIP Daily;
http://www.redmondmag.com/news/article.asp?EditorialsID=6852

MICROSOFT PATCHES NINE SECURITY VULNERABILITIES

Microsoft released six security bulletins Tuesday, August 9, including three bulletins rated "critical." All six bulletins involved Windows, and one of the bulletins also involved Internet Explorer. The most serious of the bulletins is a cumulative security update for Internet Explorer (MS05-038). The bulletin, which also applies to some versions of Windows, addresses three security flaws. Two of those are critical flaws that allow an attacker to take complete control of a computer over the Internet. The other flaw allows information disclosure. As a cumulative update for IE, the patch sets a kill bit for older versions of certain objects that have known security vulnerabilities. Those objects include the Microsoft HTML Help ActiveX control, the Microsoft MSAgent ActiveX control and a SharePoint Portal Services logging ActiveX control. The patch also changes the way IE Favorites behaves to close off a class of vulnerabilities. Another bulletin patches a critical vulnerability found in Windows Plug and Play that can allow remote code execution and elevation of privilege (MS05-039). The other bulletin involving a critical flaw is MS05-043 for a vulnerability in the Windows Print Spooler Service that could allow remote code execution. Microsoft Security Bulletin Summary for August 2005: http://www.microsoft.com/technet/security/bulletin/ms05-aug. mspx

---

Category 21.1 General QA failures

2005-08-10 **vulnerability Lasso Professional Server authentication bypass information disclosure**

DHS IAIP Daily; http://www.securityfocus.com/bid/14543/info

LASSO PROFESSIONAL SERVER REMOTE AUTHENTICATION BYPASS VULNERABILITY

Lasso Professional Server is susceptible to a remote authentication bypass vulnerability. This issue is due to a failure of the application to properly enforce defined security constraints. This vulnerability allows remote attackers to gain access to potentially sensitive information contained in Web pages they would normally be unable to see, potentially aiding them in further attacks. Depending on the contents and design of the targeted Web pages, attackers may possibly interact with the Website to cause data alterations or destruction. This issue is present in versions 8.0.4 and 8.0.5 of Lasso Professional Server. Fix for OmniPilot Software Lasso Professional Server 8.0.4: http://support.omnipilot.com/article_files/Security%20Fix%20 804-805.zi p Fix for OmniPilot Software Lasso Professional Server 8.0.5: http://support.omnipilot.com/article_files/Security%20Fix%20 804-805.zip

---

Category 21.1 General QA failures

2005-08-10 **vulnerability Nortel Contivity VPN Client local privilege escalation launch arbitrary files**

DHS IAIP Daily; http://www.securityfocus.com/bid/14542/info

NORTEL CONTIVITY VPN CLIENT LOCAL PRIVILEGE ESCALATION VULNERABILITY

Nortel Contivity VPN Client is susceptible to a local privilege escalation vulnerability. This issue is due to a failure of the application to properly lower the privileges of the running process when required. Due to the nature of the affected application, it executes with SYSTEM privileges. When a local user opens a dialog box to select digital certificates, they may use it to launch arbitrary files. Due to the failure of the application to properly revert to the users correct privileges, the executed file will be run with SYSTEM privileges. This vulnerability allows local attackers to access and execute arbitrary files with SYSTEM privileges, facilitating the compromise of the local computer. Security Focus is not aware of any vendor-supplied patches for this issue.

Category 21.1 General QA failures

2005-08-10 **vulnerability multiple MySQL UDF denial-of-service load arbitrary library**

DHS IAIP Daily;
http://www.securiteam.com/windowsntfocus/5VP0A00GLU.html

MYSQL UDF MULTIPLE VULNERABILITIES

User-defined functions in MySQL allow a user in the database to call binary libraries on the operating system. Creating a user-defined function requires insert privileges on the mysql.func table. The lack of proper length validation allow attackers to execute arbitrary code using MySQL UDL. Improper directory separator checking, allow attacker to perform directory traversal using MySQL UDL. The lack of proper checking allow attackers to cause a denial of service or load arbitrary library with MySQL UDL. The vendor has released patches for MySQL versions 4.0.25, 4.1.13 and 5.0.7-beta: http://dev.mysql.com/downloads/

Category 21.1 General QA failures

2005-08-10 **vulnerability WordPress remote code execution no patch**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1366

WORDPRESS "CACHE_LASTPOSTDATE" REMOTE CODE EXECUTION ISSUE

A vulnerability was identified in WordPress, which may be exploited by remote attackers to execute arbitrary commands. This flaw is due to an input validation error when processing a specially crafted "cache_lastpostdate" variable sent via cookies, which may be exploited by remote attackers to execute arbitrary PHP commands. WordPress version 1.5.1.3 and prior are affected. The FrSIRT is not aware of any official supplied patch for this issue.

Category 21.1 General QA failures

2005-08-11 **vulnerability McAfee ePolicy Orchestrator Local Information Disclosure**

DHS IAIP Daily; http://www.securityfocus.com/bid/14549/references

MCAFEE EPOLICY ORCHESTRATOR LOCAL INFORMATION DISCLOSURE VULNERABILITY

Network Associates McAfee ePolicy Orchestrator is susceptible to a local information disclosure vulnerability. This issue is due to incorrectly configured directory permissions in the default installation process of the application. This vulnerability allows local attackers to access arbitrary files located in the same partition as the affected directory with SYSTEM privileges. This will aid them in further attacks. Security Focus is not currently aware of any vendor-supplied patches for this issue.

Category 21.1 General QA failures

2005-08-11 **vulnerability multiple format string GNOME**

DHS IAIP Daily; http://secunia.com/advisories/16394/

GNOME EVOLUTION MULTIPLE FORMAT STRING VULNERABILITIES

Vulnerabilities have been reported in Evolution which can be exploited by malicious people to compromise a vulnerable system. 1) A format string error when displaying full vCard information attached to an e-mail message can be exploited to execute arbitrary code. Successful exploitation requires that the user clicks on "Show Full vCard" or saves the vCard to an address book and then views it under the "Contacts" tab. 2) A format string error exists when displaying specially crafted contact data retrieved from an LDAP server. 3) A format string error exists when displaying specially crafted task list data retrieved from remote servers and when the user saves the task list data under the "Calendars" tab. The vulnerabilities have been reported in versions 1.5 through 2.3.6.1 and have reportedly been fixed in 2.3.7 (unstable).

Category 21.1 General QA failures

2005-08-11 **vulnerability Adobe Version Cue 1.x Mac OS X privilege escalation update issued**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2005/Aug/1014776.html

ADOBE VERSION CUE 1.X FOR MAC OS X SYSTEM PRIVILEGE ESCALATION

A security vulnerability has been identified in a previous release of Adobe Version Cue, a feature of Adobe Creative Suite, that effects only computers on which Mac OS X and Version Cue Workspace are installed. If the vulnerability is exploited, a user with a local Mac OS X account could obtain system administrator access to local files and applications on that computer. The identified vulnerability is caused by special file permissions on internal Version Cue application files. This vulnerability cannot be exploited by users who do not have local login accounts on that computer. Users of Version Cue 1.x should download and install the security update: www.adobe.com/support/downloads/detail.jsp?ftpID=2985

Category 21.1 General QA failures

2005-08-12 **cyber security alert US-CERT NDMP exploit recommendations**

DHS IAIP Daily; http://www.us−cert.gov/cas/techalerts/TA05−224A.html

VERITAS BACKUP EXEC USES HARD-CODED AUTHENTICATION CREDENTIALS

VERITAS Backup Exec Remote Agent for Windows Servers is a data backup and recovery solution that supports the Network Data Management Protocol (NDMP). NDMP "...is an open standard protocol for enterprise-wide backup of heterogeneous network-attached storage." By default, the Remote Agent listens for NDMP traffic on port 10000/tcp. The VERITAS Backup Exec Remote agent uses hard-coded administrative authentication credentials. An attacker with knowledge of these credentials and access to the Remote Agent may be able to retrieve arbitrary files from a vulnerable system. The Remote Agent runs with SYSTEM privileges. Exploit code, including the credentials, is publicly available. US-CERT has also seen reports of increased scanning activity on port 10000/tcp. This increase may be caused by attempts to locate vulnerable systems. US-CERT recommends taking the following actions to reduce the chances of exploitation: * Use firewalls to limit connectivity so that only authorized backup server(s) can connect to the Remote Agent. The default port for this service is port 10000/tcp. * At a minimum, implement some basic protection at the network perimeter. When developing rules for network traffic filters, realize that individual installations may operate on non-standard ports. * In addition, changing the Remote Agent's default port from 10000/tcp may reduce the chances of exploitation. Please refer to VERITAS support document 255174 for instructions on how to change the default port.

Category 21.1 *General QA failures*

2005-08-12 **vulnerability exploit Microsoft Plug and Play US-CERT execute arbitrary code patches issued**

DHS IAIP Daily; http://www.us−cert.gov/current/current_activity.html#VU998653

EXPLOIT FOR VULNERABILITY IN MICROSOFT PLUG AND PLAY

US-CERT is aware of a public exploit for a vulnerability in Microsoft Plug and Play that could allow an attacker to locally or remotely execute arbitrary code or cause a denial-of-service condition on a vulnerable system. The exploit code targets Windows systems by connecting to NetBIOS ports 139/tcp or 445/tcp on a vulnerable system. A remote, unauthenticated attacker may be able to execute arbitrary code or cause a denial-of-service condition on Windows 2000. With Windows XP SP1, the remote user must be authenticated to exploit the vulnerability. A local, authenticated attacker may be able to execute arbitrary code or to create a denial-of-service condition on Windows XP SP2 and Server 2003 systems. Microsoft has released a patch to address this vulnerability in Microsoft Security Bulletin MS05-039. Administrators are encouraged to apply the appropriate fixes as soon as possible. VU#998653 - Microsoft Plug and Play contains a buffer overflow vulnerability: http://www.kb.cert.org/vuls/id/998653 Patches from Microsoft: http://www.microsoft.com/technet/security/bulletin/ms05-aug. mspx

---

Category 21.1 *General QA failures*

2005-08-15 **NIST cybersecurity flaw vulnerability database NVD encyclopedia**

EDUPAGE; http://www.fcw.com/article89911-08-15-05

NIST COMPILES CYBERSECURITY FLAWS DATABASE

Scientists at the National Institute of Standards and Technology (NIST) have created a vast database designed to collect information on virtually all known cybersecurity vulnerabilities, updated daily with new information. The National Vulnerability Database (NVD), which combines information held in all federal databases, currently has about 12,000 listings and includes links to industry resources. According to Peter Mell, senior computer scientist at NIST and creator of NVD, about 10 new vulnerabilities are added each day. Nell, who characterized the NVD as "an encyclopedia of everything," said it can be useful both for the public at large and for computer developers seeking current information about security weaknesses in a wide range of commercial products. Federal Computer Week, 15 August 2005

Category 21.1 *General QA failures*

2005-08-16 **vulnerability Adobe Acrobat remote buffer overflow PDF arbitrary code execution**

DHS IAIP Daily; http://www.kb.cert.org/vuls/id/896220

ADOBE ACROBAT CONTAINS A REMOTELY EXPLOITABLE BUFFER OVERFLOW

Adobe Acrobat is a suite of applications that allow users to manipulate PDF (Portable Document Format) files. A buffer within a core plug-in for Adobe Acrobat and Acrobat Reader can be overwritten using a specially-crafted PDF document. If a remote attacker can persuade a user to access a specially crafted PDF file, that attacker may be able to execute arbitrary code or crash the Adobe Acrobat/Acrobat Reader process. Users should upgrade to unaffected versions of Adobe Acrobat and Acrobat Reader. For a list of unaffected versions please see Adobe Security Advisory 321644: http://www.adobe.com/support/techdocs/321644.html

---

Category 21.1 *General QA failures*

2005-08-16 **vulnerability Kismet multiple integer underflow execute arbitrary commands denial-of-service DoS**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1422

KISMET MULTIPLE INTEGER UNDERFLOW AND UNSPECIFIED VULNERABILITIES

Multiple vulnerabilities were identified in Kismet, which could be explited by remote attackers to execute arbitrary commands or cause a denial of service. The first flaw is due to an error in the handling of unprintable characters in the SSID (the impact of this issue is currently unknown). The second issue is due to integer underflow errors in the pcap handling, which could be exploited to cause heap corruption. The third vulnerability is due to an integer underflow in CDP protocol dissector, which could be exploited by remote attackers to execute arbitrary commands. Products affected are Kismet versions prior to 2005-08-R1. Upgrade to Kismet version 2005-08-R1: http://www.kismetwireless.net/download.shtml

---

Category 21.1 General QA failures

2005-08-16 **vulnerability SafeHTML cross-site scripting**

DHS IAIP Daily; http://www.securityfocus.com/bid/14574/info

SAFEHTML UTF-7 AND CSS COMMENT TAG CROSS SITE SCRIPTING VULNERABILITIES

SafeHTML is prone to cross-site scripting vulnerabilities, specifically in dealing with UTF-7 encoding of characters and with CSS comment tags. Failure to filter HTML content can result in the exploitation of various latent vulnerabilities in Web based applications. A successful attack may facilitate HTML injection or cross-site scripting type issues. The vendor has released version 1.3.5 to resolve this issue. SafeHTML SafeHTML 1.3.2: http://pixel-apes.com/download/safehtml-1.3.5.zip

---

Category 21.1 General QA failures

2005-08-16 **vulnerability BlueZ arbitrary command execution update issued**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1431

BLUEZ "SECURITY.C" ARBITRARY COMMAND EXECUTION VULNERABILITY

A vulnerability was identified in BlueZ, which could be exploited by remote attackers to execute arbitrary commands. This flaw is due to an input validation error in "hcid/security.c" when processing and executing specially crafted bluetooth device names as command line arguments, which could be exploited by attackers to execute arbitrary commands or create pairings without the user's approval. Products affected are bluez-libs versions prior to 2.19 and bluez-utils versions prior to 2.19 Users should upgrade to bluez-libs-2.19 and bluez-utils-2.19: http://www.bluez.org/download.html

---

Category 21.1 General QA failures

2005-08-17 **vulnerability Microsoft Internet Explorer remote code execution no patch issued**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1450

MICROSOFT INTERNET EXPLORER "MSDDS.DLL" REMOTE CODE EXECUTION

A critical vulnerability was identified in Microsoft Internet Explorer, which could be exploited by remote attackers to execute arbitrary commands. This issue is due to a memory corruption error when instantiating the "Msdds.dll" (Microsoft Design Tools Diagram Surface) object as an ActiveX control, which could be exploited by an attacker to take complete control of an affected system via a specially crafted Web page. This vulnerability has been confirmed with Microsoft Internet Explorer 6 SP2 on Windows XP SP2 (fully patched). Note: It is currently unclear whether the "Msdds.dll" library is installed with Microsoft Office, Microsoft Visual Studio, or with other applications. More information will be provided when further details are available. Products affected are: Microsoft Internet Explorer 6 for Microsoft Windows XP SP2; Microsoft Internet Explorer 6 for Microsoft Windows XP SP1; Microsoft Visual Studio .NET 2003; and Microsoft Visual Studio .NET 2002. The FrSIRT is not aware of any official supplied patch for this issue.

Category 21.1 General QA failures

2005-08-17 **vulnerability phpPgAds SQL injection command execution upgrade**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1447

PHPPGADS SQL INJECTION AND COMMAND EXECUTION VULNERABILITIES

Multiple vulnerabilities were identified in phpPgAds, which could be exploited by remote attackers to execute arbitrary commands. The first issue is due to an input validation error in the XML-RPC library when processing, via an "eval()" call, certain XML tags nested in parsed documents, which could be exploited by remote attackers to execute arbitrary PHP commands. For additional information, see : FrSIRT/ADV-2005-1413 The second vulnerability is due to an input validation error in "lib-view-direct.inc.php" when processing a specially crafted "clientid" variable, which could be exploited by malicious users to conduct SQL injection attacks. The third flaw is due to an input validation error when processing specially crafted parameters, which may be exploited by remote attackers to include malicious files and execute arbitrary commands with the privileges of the web server. Products affected are phpPgAds versions prior to 2.0.6. Users should upgrade to phpPgAds version 2.0.6 : http://prdownloads.sourceforge.net/phpadsnew/

Category 21.1 General QA failures

2005-08-18 **vulnerability MailWatch MailScanner XML RPC upgrade**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1457

MAILWATCH FOR MAILSCANNER XML-RPC REMOTE CODE EXECUTION ISSUE

A vulnerability was identified in MailWatch for MailScanner, which could be exploited by remote attackers to execute arbitrary code. This flaw is due to an input validation error in the XML-RPC library when processing, via an "eval()" call, certain XML tags nested in parsed documents, which could be exploited by remote attackers to execute arbitrary PHP commands. For additional information, see : FrSIRT/ADV-2005-1413 Products affected are MailWatch for MailScanner versions prior to 1.0.2. Users should upgrade to MailWatch for MailScanner version 1.0.2: http://mailwatch.sourceforge.net/

Category 21.1 General QA failures

2005-08-18 **vulnerability Juniper Netscreen VPN username enumeration information disclosure**

DHS IAIP Daily; http://www.zone−h.org/advisories/read/id=7977

JUNIPER NETSCREEN VPN: USERNAME ENUMERATION VULNERABILITY

NTA Monitor has discovered a VPN username enumeration vulnerability in the Juniper Netscreen integrated Firewall/VPN products while performing a VPN security test for a customer. The vulnerability affects remote access VPNs (known as "Dialup VPNs" in ScreenOS) using IKE with pre-shared key authentication. Certificate authentication is not affected, nor is manual key authentication. In practice, we find that most Netscreen systems are configured for remote access with pre-shared key authentication (called "AutoKey IKE with Preshared keys" in ScreenOS), so this bug will affect the majority of users. The vulnerability allows an attacker to use a dictionary attack to determine valid VPN usernames on the Netscreen. Once a valid username is discovered, the attacker can then use this to obtain a hash from the Netscreen, which can then be cracked offline to determine the associated password. Once an attacker has a valid username and password, they can potentially gain access to the resources protected by the VPN. The issue is believed to affect all models of Juniper Netscreen running all ScreenOS software versions up to 5.2.0. Users should use certificate authentication rather than pre-shared key authentication.

Category 21.1 General QA failures

2005-08-19 **vulnerability Computer Associates Message Queuing denial-of-service DoS patches issued**

DHS IAIP Daily;
http://supportconnectw.ca.com/public/ca_common_docs/camsecur ity_notice.asp

COMPUTER ASSOCIATES MESSAGE QUEUING VULNERABILITIES

There are several vulnerability issues in the Computer Associates Message Queuing (CAM / CAFT) software. The CAM TCP port is potentially vulnerable to a Denial of Service (DoS) attack; buffer overflow conditions can potentially allow arbitrary code to be executed remotely with elevated privileges; and there is potential to launch a spoof CAFT and allow arbitrary commands to be executed with elevated privileges. This affects all versions of the CA Message Queuing software prior to v1.07 Build 220_13 and v1.11 Build 29_13 on the specified platforms. Patches are available for all affected users.

Category 21.1 General QA failures

2005-08-20 **vulnerability PCRE Regular Expression heap overflow no solution**

DHS IAIP Daily; http://www.securityfocus.com/bid/14620/references

PCRE REGULAR EXPRESSION HEAP OVERFLOW VULNERABILITY

PCRE is prone to a heap overflow vulnerability. This issue is due to a failure of the library to properly bounds check user-supplied input prior to copying data to an internal memory buffer. The impact of successful exploitation of this vulnerability depends on the application and the user credentials utilizing the vulnerable library. Successful attack may ultimately permit an attacker to control the contents of critical memory control structures and write arbitrary data to arbitrary memory locations. A solution is not currently known.

Category 21.1 General QA failures

2005-08-21 **vulnerability Land Down Under input validation bug SQL injection cross-site scripting attack no solution**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2005/Aug/1014747.html

LAND DOWN UNDER INPUT VALIDATION BUGS PERMIT SQL INJECTION AND CROSS-SITE SCRIPTING ATTACKS

Some input validation vulnerabilities were reported in Land Down Under. A remote user can conduct cross-site scripting attacks. A remote user can also inject SQL commands. A remote user can access the target user's cookies (including authentication cookies), if any, associated with the site running the Land Down Under software, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user. A remote user can execute SQL commands on the underlying database. No solution is currently known.

Category 21.1 General QA failures

2005-08-21 **vulnerability e-mail UNIX header buffer overflow upgrade**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1479

ELECTRONIC MAIL FOR UNIX EXPIRES HEADER BUFFER OVERFLOW VULNERABILITY

A vulnerability was identified in ELM (Electronic Mail for UNIX), which could be exploited by remote attackers to execute arbitrary commands. This flaw is due to a stack overflow error when processing specially crafted messages containing malformed "Expires" headers, which could be exploited by remote attackers to compromise a vulnerable system by convincing a user to read a specially crafted email. Products affected are Electronic Mail for UNIX (ELM) version 2.5-PL7 and prior Users should upgrade to Electronic Mail for UNIX (ELM) version 2.5-PL8: http://www.instinct.org/elm/files/tarballs/elm2.5.8.tar.gz

---

Category 21.1 General QA failures

2005-08-22 **vulnerability BEA WebLogic Portal unauthorized remote access patch issued**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1495

BEA WEBLOGIC PORTAL UNAUTHORIZED REMOTE ACCESS VULNERABILITY

A vulnerability was identified in BEA WebLogic Portal, which may be exploited by attackers to gain unauthorized access. This flaw occurs on Websites that use entitlements placed directly on desktop books, pages, or portlets, which could be exploited by remote attackers to access all the pages of the Book via specially crafted HTTP GET requests. No further details have been disclosed. Entitlements that are placed on Portals built from library books, pages, and portlets are not affected by this issue. Products affected are BEA Systems WebLogic Portal 8.1 SP1-SP4. Patch for BEA WebLogic Portal 8.1 SP4: ftp://ftpna.beasys.com/pub/releases/security/patch_CR238578_81SP4.zip

---

Category 21.1 General QA failures

2005-08-22 **vulnerability ELM header parsing buffer overflow system compromise update issued**

DHS IAIP Daily; http://secunia.com/advisories/16508/

ELM "EXPIRES" HEADER PARSING BUFFER OVERFLOW VULNERABILITY

A vulnerability has been reported in ELM, which can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to a boundary error when parsing the "Expires" header and can be exploited to cause a stack-based buffer overflow by sending a specially crafted e-mail to a user. Successful exploitation allows execution of arbitrary code. The vulnerability has been reported in versions 2.5 PL7, 2.5 PL6, and 2.5 PL5. Prior versions may also be affected. Users should update to version 2.5 PL8.

Category 21.1 General QA failures

2005-08-23 **vulnerability hole PCRE regular expressions Perl library buffer overflow execute arbitrary code restart update server processes**

DHS IAIP Daily; http://www.ubuntu.com/usn/usn−173−1

PCRE VULNERABILITY

A buffer overflow has been discovered in the PCRE, a library that provides Perl compatible regular expressions. Specially crafted regular expressions triggered a buffer overflow. On systems that accept arbitrary regular expressions from untrusted users, this could be exploited to execute arbitrary code with the privileges of the application using the library. The libpcre3 package is affected. The problem can be corrected by upgrading the affected package to version 4.5-1.1ubuntu0.4.10 (for Ubuntu 4.10), or 4.5-1.1ubuntu0.5.04 (for Ubuntu 5.04). However, a standard system upgrade is not sufficient to effect the necessary changes. Users should reboot their machines to ensure that all services using this library are restarted correctly. If not, please manually restart all server processes (exim, Apache, PHP, etc.). Users should also restart their desktop session.

Category 21.1 General QA failures

2005-08-24 **vulnerability HAURI anti-virus remote buffer overflow access violation patch issued**

DHS IAIP Daily; http://www.securityfocus.com/bid/14647/solution

HAURI ANTI-VIRUS ACE ARCHIVE HANDLING REMOTE BUFFER OVERFLOW VULNERABILITY

HAURI Anti-Virus is affected by a remote buffer overflow vulnerability when handling ACE archives. An attacker can exploit this issue by crafting a malicious ACE archive containing a specially crafted file name and sending this archive to a vulnerable computer. The attacker may exploit this vulnerability to gain unauthorized remote access in the context of the superuser. The vendor has released patches to address this issue in ViRobot Linux Server 2.0. Users running ViRobot Expert 4.0 and ViRobot Advanced Server can upgrade to vrazmain.dll version 5.8.22.137 through the online update functionality of the application. HAURI LiveCall users can upgrade to vrazmain.dll version 5.8.22.137 through the LiveCall Website. Hauri Patch ViRobot Unix/Linux Server Security Vulnerability Patch http://www.globalhauri.com/html/download/down_unixpatch.html

---

Category 21.1 General QA failures

2005-08-25 **vulnerability note pam_ldap authentication bypass update issued**

DHS IAIP Daily; http://www.kb.cert.org/vuls/id/778916

PAM_LDAP AUTHENTICATION BYPASS VULNERABILITY

pam_ldap provides LDAP authentication services for UNIX-based systems. A vulnerability in pam_ldap may allow a remote attacker to bypass the authentication mechanism. If a pam_ldap client attempts to authenticate against an LDAP server that omits the optional error value from the PasswordPolicyResponseValue, the authentication attempt will always succeed. Note that this vulnerability affects all versions of pam_ldap since version pam_ldap-169. However, if the underlying LDAP client library does not support LDAP version 3 controls, then this vulnerability is not present. This vulnerability was corrected in pam_ldap-180: http://www.padl.com/OSS/pam_ldap.html

---

Category 21.1 General QA failures

2005-08-29 **vulnerability Looking Glass cross-site scripting shell command injection no solution**

DHS IAIP Daily; http://secunia.com/advisories/16607/

LOOKING GLASS CROSS-SITE SCRIPTING AND SHELL COMMAND INJECTION

Vulnerabilities in Looking Glass, which can be exploited by malicious people to conduct cross-site scripting attacks and compromise a vulnerable system. Input passed to the "version" array parameter in footer.php and header.php is not properly sanitised before being returned to users. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site. Input passed to the "target" parameter in lg.php is not properly sanitised before being used in a "system()" call. This can be exploited to inject arbitrary shell commands via e.g. the "|" pipe character. The vulnerabilities have been confirmed in the latest available version. Other versions may also be affected. No official fix is currently known.

Category 21.1 General QA failures

2005-08-29 **vulnerability SqWebMail bug arbitrary scripting code attack update issued**

DHS IAIP Daily; http://securitytracker.com/alerts/2005/Aug/1014810.html

SQWEBMAIL BUG IN FILTERING IMG TAGS LETS REMOTE USERS INJECT ARBITRARY SCRIPTING CODE

A vulnerability was reported in SqWebMail. The software does not properly filter HTML code in e-mail messages. A remote user can send an HTML-based e-mail message containing arbitrary scripting code. When the target user views the message, the scripting code will be executed by the target user's browser. The code will originate from the site running the SqWebMail software and will run in the security context of that site. As a result, the code will be able to access the target user's cookies (including authentication cookies), if any, associated with the site, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user. A remote user can access the target user's cookies (including authentication cookies), if any, associated with the site running the SqWebMail software, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user. The vendor has issued a fixed development snapshot version (5.0.4.20050826): http://www.courier-mta.org/?download.php

---

Category 21.1 General QA failures

2005-08-30 **vulnerability Microsoft Internet Explorer IE remote code execution arbitrary commands no patch issued**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1571

MICROSOFT INTERNET EXPLORER REMOTE CODE EXECUTION VULNERABILITY

A vulnerability has been identified in Microsoft Internet Explorer, which potentially could be exploited by remote attackers to execute arbitrary commands. This flaw is due to an unspecified memory corruption error when processing malformed HTML pages, which could be exploited remote attackers to take complete control of an affected system via specially crafted Web pages. No further details have been disclosed. The FrSIRT is not aware of any official supplied patch for this issue.

Category 21.1 General QA failures

2005-08-30 **vulnerability multiple PHPLDAPAdmin user input sanitization arbitrary code execution no patch issued**

DHS IAIP Daily; http://www.securityfocus.com/archive/1/409529/30/0/threaded

PHPLDAPADMIN WELCOME.PHP MULTIPLE VULNERABILITIES

phpldapadmin is prone to multiple input validation vulnerabilities. These issues are due to a failure in the application to properly sanitize user-supplied input. phpldapadmin is prone to a directory traversal vulnerability. An attacker can exploit this vulnerability to retrieve arbitrary files on the vulnerable system in the security context of the Web server process. Information obtained may aid in further attacks against the underlying system; other attacks are also possible. phpldapadmin is prone to a remote file include vulnerability. An attacker can exploit this vulnerability to execute arbitrary PHP script code in the security context of the Web server process. phpldapadmin is also prone to a cross-site scripting vulnerability. An attacker may leverage this issue to have arbitrary script code executed in the browser of an unsuspecting user. This may facilitate the theft of cookie-based authentication credentials as well as other attacks. Security Focus is not currently aware of any vendor-supplied patches for this issue.

Category 21.1 General QA failures

2005-08-31 **vulnerability hole BNBT EasyTracker remote denial-of-service DoS HTTP parser code no patch issued**

DHS IAIP Daily; http://www.securityfocus.com/bid/14700/discuss

BNBT EASYTRACKER REMOTE DENIAL OF SERVICE VULNERABILITY

BNBT EasyTracker contains a denial of service vulnerability in its HTTP parser code. This issue is due to a failure of the application to properly handle malformed HTTP requests. If an attacker sends a malformed HTTP request to the application, reports indicate that the affected application will terminate unexpectedly. A remote attacker is able to terminate the application, denying service to legitimate users. Currently we are not aware of any vendor-supplied patches for this issue.

Category 21.1 *General QA failures*

2005-08-31 **vulnerability hole PHPXMLRPC PEaRXML_RPC remote code injection user input sanitization failure unauthorized access update issued**

DHS IAIP Daily; http://www.securityfocus.com/bid/14560/info

PHPXMLRPC AND PEAR XML_RPC REMOTE CODE INJECTION VULNERABILITY

PHPXMLRPC and PEAR XML_RPC are affected by a remote PHP code injection vulnerability. This issue is due to a failure in the application to properly sanitize user-supplied input. An attacker may leverage this issue to execute arbitrary server-side script code on an affected computer with the privileges of the Web server process. This may facilitate unauthorized access. The vendor has released version 1.2 of PHPXMLRPC and version 1.4 of PEAR XML_RPC to correct this problem.

Category 21.1 *General QA failures*

2005-08-31 **vulnerability HP-UX Java runtime environment JRE applet security bypass arbitrary file read write**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1593

HP-UX JAVA RUNTIME ENVIRONMENT (JRE) APPLET SECURITY BYPASS ISSUE

A vulnerability was identified in HP-UX, which could be exploited by remote attackers to execute arbitrary commands. This flaw is due to an error in Java Runtime Environment (JRE) when handling specially crafted applets, which may be exploited via a malicious webpage to read and/write arbitrary files on a vulnerable system and execute local applications with the privileges of the user running the untrusted applet. For additional information, see : FrSIRT/ADV-2005-0764 Products affected are HP-UX B.11.00 - HP-UX B.11.23 Users should upgrade to JRE revision 1.4.2.09.00 or 5.0.01.00 : http://www.hp.com/go/java

---

Category 21.1 *General QA failures*

2005-08-31 **vulnerability hole FlatNuke user input sanitization directory traversal arbitrary file read no solution**

DHS IAIP Daily; http://securitytracker.com/alerts/2005/Aug/1014824.html

VULNERABILITIES IN FLATNUKE

Some vulnerabilities have been discovered in FlatNuke. The software does not properly validate user-supplied input in the 'id' parameter. A remote user can supply a specially crafted parameter value containing a filename with '../' directory traversal characters and ending with '%00' to view arbitrary files on the target system. A remote user can view files on the target system with the privileges of the target web service. A remote user can access the target user's cookies (including authentication cookies), if any, associated with the site running the FlatNuke software, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user. A remote user can determine the installation path. No solution is currently known.

Category 21.1 *General QA failures*

2005-09-01 **vulnerability Plain Black Software WebGUI remote Perl arbitrary command execution update issued**

DHS IAIP Daily; http://www.securityfocus.com/bid/14732/info

PLAIN BLACK SOFTWARE WEBGUI REMOTE PERL COMMAND EXECUTION VULNERABILITIES

WebGUI may be exploited to execute arbitrary Perl commands. This issue presents itself due to insufficient sanitization of user-supplied data. Remote attackers may execute arbitrary Perl commands in the context of the Web server hosting the vulnerable application. This can facilitate unauthorized remote access. Versions of WebGUI prior to 6.7.3 are vulnerable. The vendor has released version 6.7.3 of WebGUI to address this issue.

Category 21.1 *General QA failures*

2005-09-02 **vulnerability Mod_SSL SSLVerifyClient security bypass unauthorized access update issued**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1625

MOD_SSL "SSLVERIFYCLIENT" DIRECTIVE SECURITY BYPASS VULNERABILITY

A vulnerability has been identified in mod_ssl, which could be exploited by remote attackers to bypass security policies and gain access to unauthorized contents. This flaw is due to an error in the "SSLVerifyClient" directive that does not properly validate client certificates, which could be exploited by remote attackers to bypass security restrictions and gain access, without a valid client certificate, to protected contents. mod_ssl version 2.8.23 and prior are affected. Users should upgrade to mod_ssl version 2.8.24: http://www.modssl.org/source/

Category 21.1 *General QA failures*

2005-09-03 **vulnerability WebCalendar PHP arbitrary code execution update issued**

DHS IAIP Daily; http://securitytracker.com/alerts/2005/Sep/1014849.html

VULNERABILITY IN WEBCALENDAR

A vulnerability was reported in WebCalendar. A remote user can execute arbitrary code on the target system. The 'includes/functions.php' does not properly initialize the 'includedir' parameter. A remote user can supply a specially crafted URL to cause the target system to include and execute arbitrary PHP code from a remote location. The PHP code, including operating system commands, will run with the privileges of the target web service. Impact: A remote user can execute arbitrary PHP code and operating system commands on the target system with the privileges of the target web service. The vendor has issued a fixed version (1.0.1): http://www.k5n.us/webcalendar.php?topic=Download

---

Category 21.1 *General QA failures*

2005-09-05 **vulnerability KDE kcheckpass insecure lock file creation privilege escalation patch issued**

DHS IAIP Daily; http://secunia.com/advisories/16692/

KDE KCHECKPASS INSECURE LOCK FILE CREATION VULNERABILITY

A vulnerability in kcheckpass can potentially be exploited by malicious local users to gain escalated privileges. The vulnerability is caused due to the insecure creation of the lock file in "/var/lock" by kcheckpass.c. This can be exploited via symlink attacks to create or overwrite arbitrary files with the privileges of the user running the affected application. Successful exploitation requires that the directory "/var/lock" is writable. The vulnerability affects KDE versions 3.2.0 through 3.4.2. Users should apply patch (KDE 3.4.2): ftp://ftp.kde.org/pub/kde/securi…st-3.4.2-kdebase-kcheckpass.diff 2065be8baea09c89416385ac5dd892a9

Category 21.1 *General QA failures*

2005-09-06 **software quality assurance QA design software engineering project management maintainability catastrophe mess disaster insurance calculations refunds errors**

RISKS; http://tinyurl.com/8qhuz (in German) 24 03

GERMAN GOVERNMENT SOFTWARE OVERPAYS PREMIUMS BY $25M PER MONTH

In the never-ending tale of woe surrounding the German social services and unemployment software A2LL (produced by T-Systems, the software arm of the former German state Telecom company), the Spiegel has just reported that the software miscalculates the health insurance premiums that the government pays every month - to the tune of 25 million Euros too much, every month. The bill is footed by the taxpayers, of course, since T-Systems wisely put a cap in to contract for reparations - a maximum of 5 million Euros is all T-Systems needs to pay.

….

According to *Der Spiegel*, an expert commission is already discussing what to do with the software, which was taken into service just in January of 2005. It has been declared to be in such a state of non-maintainability and non-adaptability ("nicht mehr wartungs- und entwicklungsfähig") that they are speaking about an entirely new software - to be written, of course, by T-Systems, who brought on this mess in the first place. They just are trying to decide whether to start a new central "solution" or a decentralized one for each unemployment office, as there are many local rules and insurance providers that seem to be causing difficulty.

The problem is with the insurance premiums for the unemployed, which was lowered retrospectively to save money for the government in March. A health insurance umbrella organization, VdAK, says it has difficulty in determining how much to pay back, if anything, because they do not know for exactly which people and months the wrong premium was calculated. A previous large error reported completely wrong data on who exactly was insured when to the insurance companies. The VdAK has said that when the German Social Services BA (Bundesagentur für Arbeit) gets their software straightened out, they will be glad - for a fee, of course - to see if they can repay the premiums payed in error.

[Summary by Deborah Weber-Wulff]

Category 21.1 *General QA failures*

2005-09-06 **vulnerability MAXdev MD-Pro XML-RPC arbitrary command execution**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1638

MAXDEV MD-PRO XML-RPC AND MULTIPLE UNSPECIFIED VULNERABILITIES

Multiple vulnerabilities were identified in MAXdev MD-Pro, which could be exploited by remote attackers to execute arbitrary commands. The first flaw is due to an input validation error in the XML-RPC library when processing certain XML tags nested in parsed documents, which could be exploited by remote attackers to execute arbitrary PHP commands. The second issue is due to unspecified errors in the Download, Search, Web links, Blocks, Messages, News, Comments, Settings, Stats, and Subjects modules. No further details have been disclosed. Products affected are MAXdev MD-Pro versions prior to 1.073. Users should upgrade to MAXdev MD-Pro version 1.073: http://www.maxdev.com/Downloads-index-req-viewdownload-cid-3.phtml

---

Category 21.1 *General QA failures*

2005-09-13 **vulnerability Linksys WRT54G wireless router arbitrary code execution**

DHS IAIP Daily; http://www.securityfocus.com/bid/14822/references

LINKSYS WRT54G WIRELESS ROUTER MULTIPLE REMOTE VULNERABILITIES

There have been multiple vulnerabilities found in the Linksys WRT54G router. In order to pentrate these vulnerabilities the attacker must have access to either the wireless, or internal LAN network segments of the affected device and exploitation from the WAN interface is only possible if the affected device has remote management enabled. This vulnerability allows for multiple issues that include executing arbitrary machine code in the context of the affected device and utilizing HTTP POST requests to upload router configuration and firmware files without proper authentication.

Category 21.1 General QA failures

2005-09-14 **vulnerability MIVA Merchant5 cross-site scripting user input sanitization arbitrary code execution**

DHS IAIP Daily; http://www.securityfocus.com/bid/14828/references

MIVA MERCHANT 5 MERCHANT.MVC CROSS-SITE SCRIPTING VULNERABILITY

MIVA Merchant 5 is prone to a cross-site scripting vulnerability. This issue is due to a failure in the application to properly sanitized user-supplied input. This issue may be leveraged by having arbitrary script code executed in the browser of an unsuspecting user in the context of the affected site. This vulnerability may facilitate the theft of cookie-based authentication credentials as well as other attacks.

Category 21.1 General QA failures

2005-09-16 **vulnerability Digital Scribe username SQL injection system compromise**

DHS IAIP Daily; http://secunia.com/advisories/16841/

DIGITAL SCRIBE "USERNAME" SQL INJECTION

A vulnerability has been reported in Digital Scribe, which can be exploited by malicious people to conduct SQL injection attacks and compromise a vulnerable system. Analysis showed that input passed to the "username" parameter in "login.php" is no't properly sanitized before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code, which can further be exploited to compromise a vulnerable system if combined with inappropriate functionality which allows editing the PHP files "header1.php", "header2.php", and "footer.php" via the template editing functionality.

Category 21.1 General QA failures

2005-09-22 **vulnerability Mozilla Suite Firefox spoofing cross-site scripting arbitrary command execution**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1824

MOZILLA SUITE AND FIREFOX MULTIPLE CODE EXECUTION VULNERABILITIES

There have been nine vulnerabilities identified in Mozilla Suite and Mozilla Firefox. These vulnerabilities may be exploited by remote attackers to execute arbitrary commands or conduct spoofing and cross site scripting attacks. The flaws include buffer overflows, heap overflow errors, stack corruption errors, malformed headers, unprivileged controls, integer overflow errors, error in high privileged "chrome" pages, errors in openings and input validation errors.

Category 21.1 General QA failures

2005-10-13 **sustainability databases NSF data integrity accessibility**

EDUPAGE; http://www.insidehighered.com/news/2005/10/13/digital

REPORT ADDRESSES SUSTAINABILITY OF DATABASES

A new report from a National Science Board task force calls on the federal government to implement a clear and focused strategy to ensure that growing collections of information in databases remain accessible and easy to use in the coming years. The report argues that the National Science Foundation (NSF), which has financed many technological developments in recent years, has not crafted policies and strategies that consider and address the range of technologies for storing data. The report praises the improvements that have been made to systems that collect various types of material in digital form and make those materials widely available online, but it says the need is "urgent" for a strategy to guarantee the viability of those materials. The concern, according to the report, is that as technology platforms continue to evolve, some digital content could be left in the lurch, unable to be accessed by newer systems. The report makes a number of recommendations for the NSF, including coordinating efforts between data storage and users of those data, promoting effective training, and supporting efforts to educate "a sufficient number of high-quality data scientists" to manage such systems. Inside Higher Ed, 13 October 2005

Category 21.1 *General QA failures*

2005-10-17 **software quality assurance QA testing failure errors data corruption fraud incompetence**

RISKS; http://tinyurl.com/create.php; 24 08

DOESN'T *ANYONE* CHECK THEIR RESULTS ANY MORE?

MassHighway admitted that the state had found 19 legends on the new signs with significant errors in mileage. That's 12 percent of the 164 new signs in the $1.05 million contract.

According to the contractor, some of the distances were calculated using Microsoft's Streets & Trips software. According to Microsoft, the software without a GPS hookup costs $39.95. This contractor was paid $130,000 by the state.

Apparently the contractor had tried to use Mapquest, but found it unreliable.

One sign on Interstate 93 north, near Exit 45 in Andover, reported that Manchester, N.H. Was 42 miles away, although the actual distance is just a bit more than 28 miles. Another sign on Route 128/95 in Needham reported that Wellesley is 7 miles away. The actual distance is slightly less than 3 miles. A sign on Route 3 north in Braintree listed the distance to I-93 as 5 miles when the distance by odometer was 3 miles.

[RISKS frequent contributor Monty Solomon used quotations from a couple of articles in the summary above.]

Category 21.1 *General QA failures*

2005-10-20 **smart card reader failure accusation fraud court case reliability**

RISKS; http://news.bbc.co.uk/1/hi/england/london/4361286.stm 24 08

SYSTEM FAILURE = COURT APPEARANCE

Nick Rothwell reports on an alarming consequence of a system failure:

>A woman is being summoned to court, and faces a 1000-pound fine if found guilty, over non-payment of a 1.20-pound London bus fare.

Most of London's transport system is moving over to the Oyster card system, where quasi-smartcards are touched against readers at tube station barriers or doors to buses. A card can contain season tickets, top-up funds for pay-as-you-go travel, or both.

According to the television news coverage today, Jo Cahill believed that she had paid on entering the bus, but the reader did not register her card in order to deduct the fare from the top-up funds. An inspector has treated her as a fare-dodger, even though she explained the situation and offered to pay.

This seems to set the precedent that users are required to confirm that the reader has indeed registered their card, even though the visual and audible signals are not always clear. Transport for London claims that its Oyster card readers rarely fail, although they do not specify whether or not users will always be taken to court when they do fail. (I frequently get onto buses where the reader has a post-it note saying "reader broken" stuck to it.)<

Category 21.1 *General QA failures*

2005-10-27 **vulnerability Oracle password system weak protection warning**

DHS IAIP Daily;
http://news.com.com/Oracle+password+system+comes+under+fire/ 2100−1002_3−5918305.html?tag=nefd.top

ORACLE PASSWORD SYSTEM COMES UNDER FIRE

Experts warn that attackers could easily uncover Oracle database users' passwords because of a weak protection mechanism, putting corporate data at risk of exposure. Joshua Wright of the SANS Institute and Carlos Sid of Royal Holloway College, University of London, say they have found a way to recover the plain text password from even very strong, well-written Oracle database passwords within minutes. In a presentation given at the SANS Network Security conference in Los Angeles, on Wednesday, October 26, they said that the technique that Oracle uses to store and encrypt user passwords doesn't provide sufficient security. The researchers shared how passwords are encrypted before being stored in Oracle databases. Wright and Cid identified several vulnerabilities, including a weak hashing mechanism and a lack of case preservation (all passwords are converted to uppercase characters before calculating the hash). Wright and Cid wrote "By exploiting these weaknesses, an adversary with limited resources can mount an attack that would reveal the plain text password from the hash for a known user." The researchers said that Oracle users can protect their systems by requiring strong passwords and assigning limited user rights. Presentation at SANS: http://www.sans.org/rr/special/index.php?id=oracle_pass

---

Category 21.1 *General QA failures*

2005-10-27 **vulnerability Sun Solaris Management Console HTTP TRACE information disclosure cookies authentication data patch issued**

DHS IAIP Daily; http://www.securityfocus.com/bid/15222/references

SUN SOLARIS MANAGEMENT CONSOLE HTTP TRACE INFORMATION DISCLOSURE VULNERABILITY

Sun Solaris Management Console is prone to an information disclosure vulnerability. The Solaris Management Console (smc(1M)) is a graphical user interface that provides access to Solaris system administration tools which includes a Web server that runs on port 898. The SMC Web server enables the HTTP TRACE method by default which may allow a local or remote unprivileged user the ability to access sensitive information -- such as cookies or authentication data -- contained in the HTTP headers of an HTTP TRACE request. Security Focus reports that Sun has addressed these issues with a patch or workaround. Patch: http://sunsolve.sun.com/search/document.do?assetkey=1-26-102 016-1

Category 21.1 *General QA failures*

2005-10-27 **vulnerability hole NovellZenworks patch management SQL injection patch issued**

DHS IAIP Daily; http://www.securityfocus.com/bid/15220/references

NOVELL ZENWORKS PATCH MANAGEMENT MULTIPLE SQL INJECTION VULNERABILITIES

ZENworks Patch Management is prone to multiple SQL injection vulnerabilities. These issues are due to a failure in the application to properly sanitize user supplied input before using it in SQL queries. Successful exploitation could result in a compromise of the application, disclosure or modification of data, or may permit an attacker to exploit vulnerabilities in the underlying database implementation. These vulnerabilities can only be exploited if a non-privileged account has been created. Only an administrator can create such an account. Security Focus reports that Novell has addressed these issues in ZENworks Patch Management version 6.2 and later. Novell Upgrade ZEN_PatchMgmt_Upd6.2.iso
http://download.novell.com/Download?buildid=5_kRStyf9wU~

Category 21.1 *General QA failures*

2005-10-31 **vulnerability hole Avaya Ethereal arbitrary code execution denial-of-service DoS attack update future release**

DHS IAIP Daily; http://secunia.com/advisories/17392/

AVAYA MULTIPLE ETHEREAL VULNERABILITIES

Avaya has acknowledged vulnerabilities in Ethereal which can be exploited by malicious people to cause a Denial of Service attack or compromise a vulnerable system. These attacks can include remote attackers sending malicious packets that could cause Ethereal to crash or execute arbitrary code. In order for an attacker to exploit these vulnerabilities an authenticated local system user would first manually start the Ethereal application. According to Secunia, the vendor is reportedly considering to include an update for a future release.

Category 21.1 *General QA failures*

2005-10-31 **vulnerability Subdreamer login SQL injection system compromise source code edit user input sanitization**

DHS IAIP Daily; http://secunia.com/advisories/17378/

SUBDREAMER LOGIN SQL INJECTION VULNERABILITIES

Vulnerabilities have been found in Subdreamer. These can be exploited by attackers to conduct SQL injection attacks and compromise a vulnerable system. The vulnerability can be exploited to access the administration section where arbitrary PHP files can be uploaded and executed via the Image Manager panel. Secunia reports that the problem can be fixed by editing the source code to ensure that input is properly sanitized.

Category 21.1 *General QA failures*

2005-10-31 **vulnerability hole IBM AIX chcons local buffer overflow boundary checking arbitrary code execution no update**

DHS IAIP Daily; http://www.securityfocus.com/bid/15247/references

IBM AIX CHCONS LOCAL BUFFER OVERFLOW VULNERABILITY

IBM AIX chcons is prone to a local buffer overflow vulnerability. This issue arises because the application fails to perform boundary checks prior to copying user-supplied data into insufficiently sized memory buffers. This issue presents itself when 'DEBUG MALLOC' is enabled. If the affected utility has setuid-superuser privileges, then a successful attack allows arbitrary machine code execution with superuser privileges. Security Focus reports that IBM has released advisories to address this issue. Fixes are not currently available. Advisories: http://www-1.ibm.com/support/docview.wss?uid=isg1IY78241, http://www-1.ibm.com/support/docview.wss?uid=isg1IY78253

Category 21.1 *General QA failures*

2005-11-02 **vulnerability Cisco IOS system timers heap buffer overflow denial-of-service DoS result**

DHS IAIP Daily; http://www.securityfocus.com/bid/15275/discuss

CISCO IOS SYSTEM TIMERS HEAP BUFFER OVERFLOW VULNERABILITY

Cisco IOS is vulnerable to a heap based buffer overflow exploitation. Cisco has released an advisory stating that IOS upgrades are available to address the possibility of exploitation of heap based buffer overflow vulnerabilities which could lead to a Denial of Service. Security Focus was not aware if the advisory addresses a specific heap overflow or just provides security enhancements to mitigate attempts to exploit other heap overflow vulnerabilities. Cisco Security Advisory: http://www.cisco.com/warp/public/707/cisco-sa-20051102-timer s.shtml References: http://www.securityfocus.com/bid/15275/references

---

Category 21.1 *General QA failures*

2005-11-02 **vulnerability Cisco airspace wireless LAN unencrypted access**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/2278

CISCO AIRESPACE WIRELESS LAN CONTROLLERS UNENCRYPTED NETWORK ACCESS

A vulnerability has been identified in Cisco Airespace Wireless LAN (WLAN) Controllers. This may be exploited by attackers to bypass security policies. This vulnerability is due to an error in the Lightweight Access Point Protocol (LWAPP) mode that accepts unencrypted traffic from end hosts even when configured to encrypt traffic, which could be exploited by attackers to send malicious traffic into a secure network.

Category 21.1 *General QA failures*

2005-11-02 **vulnerability multiple Simple PHP blog input validation arbitrary code execution no solution**

DHS IAIP Daily; http://www.securityfocus.com/bid/15283/discuss

SIMPLE PHP BLOG MULTIPLE INPUT VALIDATION VULNERABILITIES

The Simple PHP Blog is prone to multiple input validation vulnerabilities. These issues are due to a failure in the application to properly sanitize user-supplied input. An attacker may leverage these issues to have arbitrary script code executed in the browser of an unsuspecting user in the context of the affected site. These may facilitate the theft of cookie-based authentication credentials as well as other attacks. Security Focus did not report a solution to this vulnerability.

Category 21.1 *General QA failures*

2005-11-03 **denial of service DoS outage bug flaw glitch backup failure business continuity**

RISKS; http://www.vnunet.com/vnunet/news/2145336/software-bug-crashes-japanese 24 09

SOFTWARE BUG CRASHES JAPANESE STOCK EXCHANGE

"The Tokyo Stock Exchange suffered its worst ever outage yesterday when trading was suspended for four and a half hours due to a software problem. A spokesman said that the glitch appeared to be connected to the decision to expand the trading system's capacity last month in response to high trading volumes. The modified system had worked well, but crashed when the automatic monthly clean-up of the software was implemented. A back-up system also failed because it uses the same software."

[Excerpt contributed by Mark M. Bennison]

Category 21.1 *General QA failures*

2005-11-04 **vulnerability hole CuteNews template local file inclusion arbitrary code execution update issued**

DHS IAIP Daily; http://secunia.com/advisories/17435/

CUTENEWS "TEMPLATE" LOCAL FILE INCLUSION VULNERABILITY

A vulnerability has been found in CuteNews which could be exploited by attackers to disclose sensitive information and compromise a vulnerable system. The vulnerability is caused when input passed to the "template" parameter in "show_archives.php" and "show_news.php" is not properly verified before it is used to include files. This can be exploited to include arbitrary files from local resources. This can further be exploited to execute arbitrary PHP code by including the "inc/ipban.mdu" script where PHP code can be injected via the "add_ip" parameter. Successful exploitation requires disabling of "magic_quotes_gpc." The vulnerability has been fixed in an updated 1.4.1 version (build 178).

Category 21.1 *General QA failures*

2005-11-04 **software quality assurance QA testing costs electronic toll system**

RISKS; http://tinyurl.com/8sq6v 24 09

ELECTRONIC TOLL GLITCH CAUSES DOUBLE-BILLING

Fast Lane double-billed 8,498 accounts this week, an error Massachusetts Turnpike Authority officials attributed yesterday to the electronic toll company running the system. The computer glitch drew money Tuesday out of credit card and checking accounts belonging to Fast Lane customers, then mistakenly docked the same customers Wednesday. The total wrongly withdrawn could amount to tens of thousands of dollars, said the Turnpike spokeswoman, Mariellen Burns.

[Contributed by Monty Solomon]

Category 21.1 *General QA failures*

2005-11-05 **vulnerability hole Macromedia Flash Player SWF arbitrary code execution update issued**

DHS IAIP Daily; http://secunia.com/advisories/17430/

MACROMEDIA FLASH PLAYER SWF FILE HANDLING ARBITRARY CODE EXECUTION VULNERABILITY

A vulnerability has been reported in Macromedia Flash Player which could be exploited to compromise a user's system. The vulnerability is caused due to missing validation of the frame-type identifier that is read from a SWF file. This value is used as an index in Flash.ocx to reference an array of function pointers. This can be exploited via a specially crafted SWF file to cause the index to reference memory that is under the attacker's control, which causes Flash Player to use attacker-supplied values as function pointers. Secunia recommends updating to Flash Player 8 (8.0.22.0) or apply Flash Player 7 update (7.0.61.0 or 7.0.60.0).

Category 21.1 *General QA failures*

2005-11-06 **vulnerability Cisco IOS heap overflow system reload remote code execution**

DHS IAIP Daily; http://www.securiteam.com/securitynews/6E0011PEKA.html

CISCO IOS HEAP-BASED OVERFLOW VULNERABILITY

The Cisco Internetwork Operating System (IOS) may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. In many cases, a heap-based overflow in Cisco IOS will simply corrupt system memory and trigger a system reload when detected by the "Check Heaps" process, which monitors for such memory corruption. In a successful attack against an appropriate heap-based overflow, it is possible to achieve code execution without the device crashing immediately. Successful exploitations of heap-based buffer overflow vulnerabilities in Cisco IOS software often result in a Denial of Service. In some cases it is possible to overwrite areas of system memory and execute arbitrary code from those locations. In the event of successful remote code execution, device integrity will have been completely compromised. Cisco has included additional integrity checks in its software that are intended to reduce the likelihood of arbitrary code execution. The advisory is posted on Cisco's website. Cisco: http://www.cisco.com/en/US/products/products_security_adviso ry09186a008055ef31.shtml

---

Category 21.1 *General QA failures*

2005-11-07 **vulnerability hole Magpie RSS httpsrequest arbitrary command execution update issued**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/2335

MAGPIERSS "HTTPSREQUEST" FUNCTION REMOTE COMMAND EXECUTION ISSUE

A vulnerability has been identified in MagpieRSS, which could be exploited by remote attackers to execute arbitrary commands. The vulnerability is due to an input validation error in the "_httpsrequest" function of Snoopy when passing malformed URLs to the "exec()" call, which could be exploited by remote attackers to execute arbitrary commands via a specially crafted URL. FrSIRT recommends upgrading to MagpieRSS version 0.72.

Category 21.1 *General QA failures*

2005-11-08 **critical vulnerability update fix US-CERT Microsoft Windows Image Processing arbitrary code execution denial-of-service DoS**

DHS IAIP Daily; http://www.us−cert.gov/cas/techalerts/TA05−312A.html

MICROSOFT WINDOWS IMAGE PROCESSING VULNERABILITIES

Microsoft has released updates that address critical vulnerabilities in Windows graphics rendering services. A remote, unauthenticated attacker exploiting these vulnerabilities could execute arbitrary code or cause a denial of service on an affected system. The Microsoft Security Bulletin for November 2005 addresses multiple buffer overflows in Windows image processing routines. Viewing a specially crafted image from an application that uses a vulnerable routine may trigger these vulnerabilities. If this application can access images from remote sources, such as Websites or e-mail, then remote exploitation is possible. Microsoft has provided the updates to correct these vulnerabilities in Microsoft Security Bulletin MS05-053. MS05-053: http://www.microsoft.com/technet/security/bulletin/MS05-053. mspx

---

Category 21.1 *General QA failures*

2005-11-08 **vulnerability Microsoft Windows graphics rendering engine WMF/EMF arbitrary code execution update issued**

DHS IAIP Daily; http://www.securityfocus.com/bid/15352/references

MICROSOFT WINDOWS GRAPHICS RENDERING ENGINE WMF/EMF FORMAT CODE EXECUTION VULNERABILITY

Multiple vulnerabilities were identified in Microsoft Windows, which could be exploited by remote attackers to execute arbitrary commands or cause a denial of service. The first issue is due to heap overflow errors in "GDI32.DLL" when processing malformed Windows Metafile (WMF) and Enhanced Metafile (EMF) images, which could be exploited by convincing a user to visit a malicious Website using Internet Explorer, read a malicious email using Outlook, or open a specially crafted Office document containing a malicious image. The second flaw is due to an integer overflow error in the "PlayMetaFileRecord()" function of "GDI32.DLL" that does not properly handle malformed Windows Metafile (WMF) images, which could be exploited by convincing a user to visit a malicious Website using Internet Explorer, read a malicious email using Outlook, or open a specially crafted Office document containing a malicious image. The third vulnerability is due to an error in the "GetEnhMetaFilePaletteEntries()" function of "GDI32.DLL" when processing malformed Enhanced Metafile (EMF) images, which could be exploited to cause a denial of service via a malicious image. Security Focus reports that Microsoft has released a bulletin that includes fixes for supported versions of the operating system. Bulletin: http://www.microsoft.com/technet/security/bulletin/ms05-nov. mspx

---

Category 21.1 *General QA failures*

2005-11-09 **vulnerability VERITAS NetBackup buffer overflow denial-of-service DoS arbitrary command execution**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/2349

VERITAS NETBACKUP VOLUME MANAGER DAEMON BUFFER OVERFLOW ISSUE

A vulnerability has been identified in VERITAS NetBackup, which could be exploited by remote attackers to execute arbitrary commands or cause a denial of service. This is due to a buffer overflow error in a shared library used by the volume manager daemon (vmd) that does not properly handle specially crafted requests port 13701, which could be exploited by remote attackers to execute arbitrary commands with root/SYSTEM privileges. FrSIRT reports that this issue is formally resolved in NetBackup Enterprise Server/Server Security Packs. Security Packs: http://support.veritas.com/menu_ddProduct_NBUESVR_view_DOWNL OAD.htm

---

Category 21.1 *General QA failures*

2005-11-11 **vulnerability multiple Nortel CallPilot privilege escalation update issued**

DHS IAIP Daily; http://secunia.com/advisories/17509/

NORTEL CALLPILOT MULTIPLE VULNERABILITIES

Nortel Networks has found multiple vulnerabilities in Nortel CallPilot, which potentially can be exploited by malicious, local users to gain escalated privileges, or by malicious people to cause a DoS (Denial of Service), or compromise a user's system or vulnerable system. The vulnerabilities have been reported in versions 3.0 and 4.0. The vulnerability in MS05-050 (SA17160) also affects versions 1.07 and 2.x. The vendor recommends users follow the instructions in Security Advisory P-2005-0056-Global (access to this document requires an active support agreement with Nortel): http://www130.nortelnetworks.com...63252&RenditionID=REND359 659

Category 21.1 *General QA failures*

2005-11-14 **vulnerability Cisco Internet Key Exchange packets handling denial-of-service DoS update issued**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/2406

CISCO INTERNET KEY EXCHANGE PACKETS HANDLING VULNERABILITIES

Multiple vulnerabilities were identified in various Cisco products, which could be exploited by remote attackers to cause a denial of service. These flaws are due to errors in ISAKMP when handling malformed Internet Key Exchange Phase 1 packets, which could be exploited by remote attackers to cause a denial of service that may result in the restart of the device. FrSIRT reports that Cisco has a fixed version available. Fixed version: http://www.cisco.com/warp/public/707/cisco-sa-20051114-ipsec .shtml#software

---

Category 21.1 *General QA failures*

2005-11-17 **quality assurance issues design flaw AAA Website registration identity theft risk**

RISKS 24 11

AAA WEB INTERFACE SECURITY ISSUES

Marty Lyons writes about the quality assurance issues with the new Website of the American Automobile Association (AAA). His story:

To sign up for an account, I needed to supply a membership number (printed on your plastic member card), and my name (also printed on the card), along with an email address, and a chosen account name. A few seconds later, I was logged in, and was able to check my account info, including mailing address, and type of credit card used for membership.

There was no verification of identity at all during account establishment. At a minimum, mandating that a user-entered postal code match the AAA database prior to creating the account would have afforded some protection.

So with a AAA member number and name, someone is well on their way to identity theft -- the rest of your wallet not required. Since many places take AAA cards to provide discounted services (hotels, car repair, restaurants, movie theatres, etc.) you can imagine the RISK. I've sent a letter to the organization letting them know their web registration needs to be redesigned.

Category 21.1 *General QA failures*

2005-11-17 **software design quality assurance QA date handling leap years input range testing**

RISKS 24 09

AND WE THOUGHT DATE PROBLEMS WERE OVER WITH Y2K

In a Q&A session about our airline's new staff travel online booking system, the following was asked:

Q. I am unable to book [a flight] online because my date of joining is February 29. What should I do?

A. Because you joined in a leap year the system is unable to identify your date of joining. You will need to ask Employee Services to change your date to February 28 for staff travel purposes.

The risk: if the booking system doesn't recognise February 29 then there are going to be a lot of empty flights on that date!! In this post-Y2K age, it is astonishing that we are still suffering from such date issues and this is not even with legacy systems, but brand new ones.

[Contributed by Chris Brady]

Category 21.1 *General QA failures*

2005-11-17 **vulnerability Qualcomm Eudora worldMail server directory traversal arbitrary file retrieval**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/2479

QUALCOMM EUDORA WORLDMAIL SERVER DIRECTORY TAVERSAL VULNERABILITY

A vulnerability has been identified in Qualcomm Eudora WorldMail Server. This may be exploited by attackers to retrieve arbitrary files from a vulnerable system. This flaw is due to an input validation error in the IMAP daemon that does not properly handle specially crafted commands containing directory traversal sequences. This may may be exploited by authenticated attackers to retrieve arbitrary files from a vulnerable system or read/manage other user's email messages.The FrSIRT is not aware of any official supplied patch for this issue.

Category 21.1 General QA failures

2005-11-17 **vulnerability multiple Hitachi Wireless IP5000 VoIP**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/2475

HITACHI WIRELESSIP5000 IP PHONE MULTIPLE REMOTE VULNERABILITIES

Multiple vulnerabilities have been identified in Hitachi WirelessIP5000 IP Phone. They could be exploited by remote attackers to gain unauthorized access or cause a denial of service. The issues include a design error where a default password ("0000") can be used to access administrative functions,a vulnerability which resides in the default index page of the HTTP server (port 8080), an error in the HTTP server that does not require authentication, a design error where the device provides an SNMP service accessible with any credentials, and an
undocumented open port (TCP/3390).

Category 21.1 General QA failures

2005-11-22 **vulnerability hole Microsoft Internet Explorer IE JavaScript no patch issued**

DHS IAIP Daily; http://www.securityfocus.com/bid/13799/references

VULNERABILITY IN THE WAY INTERNET EXPLORER HANDLES ONLOAD EVENTS COULD ALLOW REMOTE CODE EXECUTION

Microsoft Internet Explorer has been affected by a remote code execution vulnerability. This vulnerability presents itself when the browser handles a JavaScript 'onLoad' handler in conjunction with an improperly initialized 'window()' JavaScript function. This issue was originally publicly reported in May 2005 as being a stability issue that caused the browser to close. Since then, new information has been posted that indicates remote code execution could be possible. This issue may be exploited to execute arbitrary remote code in the context of the user running the affected application. Failed exploitation attempts likely result in the application crashing. Security Focus reports having no knowledge of a vendor-supplied patch for this issue.

Category 21.1 General QA failures

2005-11-23 **quality assurance issues design flaw bad erroneous date handling**

RISKS 24 11

HANDLING ERRONEOUS DATES

RISKS contributor Mike Albaugh noticed a food-product label that said, "BEST BEFORE 29 FEB 2006". Mr. Albaugh wonder whether this was the work of a lazy programmer or the fault of a date-manipulation library. He continues:

The computer scientist in me wants to know if the comparison to a (currently) non-existent date should:
* always fail (Cookies are stale now),
* always succeed (Cookies will never get stale)
* throw an exception (Cookies should not exist in this universe)

Category 21.1 General QA failures

2005-11-29 **vulnerability hole Cisco IOS HTTP server HTML injection cross-site scripting**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/2657

CISCO IOS HTTP SERVER HTML INJECTION AND CROSS SITE SCRIPTING ISSUE

A vulnerability has been identified in Cisco IOS, which could be exploited by attackers to inject malicious HTML code. This issue is due to an input validation error in the "dump" option (/level/15/exec/-/buffers/assigned/dump) of the HTTP Server that does not properly validate certain data before being displayed in the Web interface, which may be exploited by remote attackers to cause arbitrary HTML code to be executed by the user's browser in the security context of an affected server (e.g. change the "ENABLE" password by injecting HTML code via the "/level/15/configure/-/enable/secret/" link).

Category 21.1 *General QA failures*

2005-11-29 **vulnerability Microsoft Windows SynAttackProtect denial-of-service DoS attack**

DHS IAIP Daily; http://www.securityfocus.com/bid/15613/references

MICROSOFT WINDOWS SYNATTACKPROTECT PREDICTABLE HASH REMOTE DENIAL OF SERVICE VULNERABILITY

Microsoft Windows is prone to a denial of service vulnerability. The vulnerability arises due to a design error in the function responsible for the hash table management for "SynAttackProtect." Reports indicate that the affected function used by the TCP/IP stack creates a predictable hash, allowing an attacker to send a large number of SYN packets with an identical hash value. A successful attack can eventually lead to a denial of service condition due to the lookup algorithm becoming very inefficient at performing searches. Solution: http://www.securityfocus.com/bid/15613/solution

---

Category 21.1 *General QA failures*

2005-11-30 **software glitch quality assurance QA issue design flaw LAPD police law enforcement computer upgrade**

RISKS 24 12

LAPD SOFTWARE GLITCH

A software glitch has interrupted the sweeping overhaul of city emergency communications, which could delay the upgrade of police car computer systems by up to two years, officials said Monday. News about the glitch in the city's $15 million contract with Northrop Grumman Information Technology drew a strong reaction from the City Council's Public Safety Committee.

[Abstract by Peter G. Neumann]

Category 21.1 *General QA failures*

2005-11-30 **quality assurance issues design flaw Y2K++ bad year data McGraw-Hill TruSource programming errors**

RISKS 24 11

ERRONEOUS YEARS IN RETIREMENT DATA

Contributor Jim Horning's employer had outsourced its 401(k) plan administration to TruSource, a division of Union Bank of California, N.A.

When Mr. Horning looked through some retirement-plan data, he noticed a chart containing dates from the 31st and 41st centuries. The chart for the Pioneer High Yield Fund "(SINCE 03/31/98)" was labeled, "4098 3099 2000 1001 4001 4002 2003 1004 4004 3005". Mr. Horning concludes, "[A]pparently the dates escaped the notice of the humans (if any) at McGraw-Hill and TruSource who were in the loop in the preparation of these documents. It is interesting to speculate what combination of programming errors would yield this precise sequence of dates."

[Abstract by Karthik Raman]

RISKS Contributor Paul E. Ford conjectures that the dates are poorly formatted but correct:

Given the rising sequence in the last 2 digits and selective set in the first digit, I would surmise that these represent some sort of quarter data. So, 98Q4 through 05Q3. Any possibility the second position 0s are actually Qs?

Mr. Horning responds, "Paul, What sharp eyes you have! You could see those Qs even when I transcribed the data by hand. I can barely see them as Qs on the original, even given your helpful suggestion, but I do believe that you are correct."

Peter Neumann concludes:

Also noted by Amos Shapir, who observed that the date labels are placed three quarters apart. But that still does not explain the "4002", which looks as if it should have been "3002". Before running Jim's item in RISKS-24.11, I explicitly asked him to check whether the "4002" was accurately represented by him, and he did verify that. So, I suspect that the "4002" may have been a recording error in the original, or else a lapse in the reporting schedule.

Category 21.1 General QA failures

2005-11-30 **vulnerability Perl format string arbitrary code execution user input sanitization**

DHS IAIP Daily; http://www.securityfocus.com/bid/15629/references

PERL PERL_SV_VCATPVFN FORMAT STRING VULNERABILITY

Perl is susceptible to a format string vulnerability. This issue is due to a failure of the programming language to properly handle format specifiers in formatted printing functions. An attacker may leverage this issue to write to arbitrary process memory, facilitating code execution in the context of the Perl interpreter process. This can result in unauthorized remote access. Developers should treat the formatted printing functions in Perl as equivalently vulnerable to exploitation as the C library versions, and properly sanitize all data passed in the format specifier argument. Solution: http://www.securityfocus.com/bid/15629/solution

Category 21.1 General QA failures

2005-12-01 **Japan Tokyo Stock Exchange human data-input error multimillion dollar loss Mizuho Securities Co. software quality assurance design flaw**

RISKS; http://business.timesonline.co.uk/article/0,,13133-1948579,00.html 24 12

HUMAN ERROR RESULTS IN $MULTIMILLION LOSS

Japanese financial-services firm Mizuho Securities Co. Said Thursday it erroneously placed sell orders because of a simple human data-input mistake that apparently ignored an error warning. This cost Mizuho at least 27 billion yen ($225 million). The company mistakenly sold 610,000 shares of J-Com Co. At 1 yen (less than 1 cent) per share, instead of the request to sell just one share at 610,000 yen ($5,080). The mishap sent the benchmark Nikkei 225 index down 1.95 percent on the Tokyo Stock Exchange. Mizuho Financial Group dropped 3.4 percent to 890,000 yen ($7,416.67).

[Abstract by Peter G. Neumann]

RISKS contributor Tomas Uribe follows-up:

One would think that "money-critical" systems would have more stringent safeguards against this type of thing. Also, someone must have made $225 million as well--who might have been the lucky ones who bought the discounted shares?

Jeremy Epstein dug through the RISKS archive to find a similar mishap at the Tokyo Stock Exchange (RISKS-21.81):

Before the Tokyo market opened Friday, a UBS Warburg trader entered what was intended to be an order to sell 16 Dentsu shares at 610,000 yen ($4,924.53) each or above. Instead, the trader keyed in an order to sell 610,000 Dentsu shares at 16 yen apiece.

Peter Neumann remarks, "I knew the new case sounded familiar! Perhaps the 610,000 is a default number for an erroneous field? That's quite a coincidence."

In another follow-up, "RsH" writes:

As per the information in the Reuters item http://asia.news.yahoo.com/051211/3/2c7vk.html the actual loss may be lower or more than the $225 million as the amount of the premium that will need to be paid to by back shares is still to be determined. The sale order was for about 41 times the actual number of shares actually outstanding, incidentally.

It turns out that the Tokyo Stock Exchange's own software was responsible for part of the problem, as it prevented the cancellation of the order from being processed!

RsH echoes Jeremy Epstein's comment: Also note that this is NOT the first time this has happened at the TSE, and they have yet to fix their system!

The Times, a UK newspaper had the following story about how this episode at the TSE concluded:

The president of the Tokyo Stock Exchange resigned yesterday to take responsibility for the "fat-finger" trading error that sparked a day of mayhem on Tokyo markets earlier this month. Takuo Tsurushima resigned along with Sadao Yoshino, the bourse's managing director, and Yasuo Tobiyama, its head of computer systems. The incident has left considerable turmoil in its wake: Mizuho Securities lost 40 billion yen (Â£195 million) on the botched trade and two Japanese day traders made Y2.5 billion in a few minutes.

Western investment houses who made money from the error have been publicly criticized by the Japanese Government and agreed to pay the profits they made into an investors' protection fund.

Losses from the trade were sufficient to force Mizuho to cancel all end-of-year bonuses from the securities arm. The trader, believed to be a 24-year-old woman relatively inexperienced on the dealing floor, had wanted to sell one share in J Com, a new telecoms firm, for Y600,000. She mistyped the order and sold 600,000 shares at Y1 each.

Category 21.1 General QA failures

2005-12-01 **automobile brake testing failure quality assurance failure lack of feedback**

RISKS; http://www.theregister.co.uk/2005/11/29/mercedes_brake_test_fiasco/ 24 11

MERCEDES AUTOMOBILE TEST FAILURE

RISKS contributor Andre Kramer summarizes an article from _The Register_:

The Register reports that an automotive journalist was fired for rigging a radar enhanced (assumedly computer controlled) automobile brake system demonstration. Apparently, the Mercedes engineers (under duress) helped simulate the demonstration, which could not have worked in an enclosed space, by manual braking. However, the demo went badly wrong and the article http://www.theregister.co.uk/2005/11/29/mercedes_brake_test_fiasco/ correctly identified the risk of false trust in a new system that would have resulted from the attempted smoke and black mirrors going undetected. [Risks of lack of feedback from expensive car suspension systems could also be noted.]

Category 21.1 General QA failures

2005-12-02 **Microsoft Internet Explorer IE design flaw crack Google Desktop Search hijack user information**

DHS IAIP Daily;
http://www.eweek.com/article2/0,1759,1895579,00.asp?kc=EWRSS03129TX1K0000614

IE DESIGN FLAW LETS HACKER CRACK GOOGLE

An unpatched design flaw in Microsoft Corp.'s Internet Explorer browser could give malicious hackers an easy way to use the Google Desktop application to covertly hijack user information. The vulnerability was discovered in the cross-domain protections in Internet Explorer and a proof-of-concept exploit has been published. A spokesperson for Microsoft acknowledged the flaw in a statement and said the company was unaware of active attacks against IE users. The hacker who discovered the vulnerability used the Google Desktop utility to prove his findings, but in theory, any domain or application that depends on the IE cross-domain security model is vulnerable. Google spokesperson Sonya Boralv said initial investigations show that the problem resides in IE and not as a result of any vulnerabilities in Google Desktop, the downloadable utility that lets PC users merge desktop and search results on the well-known browser interface.

Category 21.1 General QA failures

2005-12-04 **GPS speed restriction design flaw Transport Canada device safety-critical systems**

RISKS; http://www.cnn.com/2005/AUTOS/12/01/canada_gps_speed/index.html 24 11

RISKS OF GPS-BASED AUTOMATIC SPEED RESTRICTION ON VEHICLES

Jeremy Epstein complains about a device Transport Canada is testing which, if you have GPS increases the resistance in the gas pedal if you try to exceed the speed limit. Mr. Epstein remarks, "Bad idea." He writes:

I'm not an expert in GPS systems, but I've seen them get confused, especially when there are nearby parallel roads. I wouldn't want it to hold my speed to 25 MPH because it thinks I'm on the dirt road that runs parallel to a highway. And if the device changes its mind suddenly, the results could be catastrophic - I'm pushing hard on the accelerator because (for whatever reason) I decide to exceed the speed limit, and suddenly it decides the speed limit has increased - now I'm flooring the car because it reduces its resistance factor. Conversely, if I have a normal pressure on the accelerator, and the speed limit drops, the device might cause my speed to drop precipitously. I'm sure there are lots of other GPS-based risks - what does the device do if it can't find a GPS signal?

Category 21.1 General QA failures

2005-12-05 **vulnerability flaw Microsoft SQL Server 2000 2K profiler database**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1896302,00.asp

FLAW FOUND IN MICROSOFT'S SQL SERVER 2000 PROFILER

A recently discovered vulnerability in Microsoft Corp.'s SQL Server 2000 database allows users to mask their login names. The vulnerability was discovered by Imperva, a researcher and vendor of data-center security products. The flaw shows up in the use of SQL Profiler in Microsoft SQL Server 2000 to audit connections to SQL Server 2000 by using the Audit Login event class. When login names contain leading zero characters, those names are not visible in the contexts of the SQL Profiler graphical user interface, a trace file that is saved by SQL Profiler, and in a trace table that is saved by SQL Profiler. Microsoft put out an advisory that stated that the problem only applies to the Profiler in SQL Server 2000. The problem is fixed in the Profiler in SQL Server 2005 when users use the Profiler to audit connections to SQL Server 2005. Microsoft recommends that users audit connections to SQL Server 2000 by using server-side tracing and by loading the resulting data from a server-side trace file into a database table by using the fn_trace_gettable function. Microsoft Advisory: http://support.microsoft.com/default.aspx?scid=kb;en-us;910741

Category 21.1 General QA failures

2005-12-05 **Microsoft Internet Explorer IE design flaw crack Google Desktop Search fortified**

DHS IAIP Daily; http://www.pcpro.co.uk/news/81024/google−fortifies−desktop −s earch−against−ie−flaw.html

GOOGLE FORTIFIES DESKTOP SEARCH AGAINST IE FLAW

Google has altered its Desktop Search so that it can no longer be used in digital attacks in conjunction with a flaw in Microsoft's Internet Explorer (IE). On Friday, December 2, an Israeli hacker reported having discovered a means of remotely using Google desktop search to remotely search the computers logged on to a specially built website using Microsoft's IE. Problems in the way the browser handles Cascading Style Sheets (CSS) led to a short cut round the restrictions the browser places on interaction between different domains. Hacker Matan Gillon posted proof-of-concept code last week, but now says that it now "no longer works because Google slightly changed their site's code." However, Google told reporters that the flaw is a problem with IE, rather than the search giant's software, so the CSS problem remains at large.

Category 21.1 General QA failures

2005-12-05 **Microsoft unpatched Internet Explorer IE Trojan horse vulnerability flaw exploit**

DHS IAIP Daily; http://news.zdnet.co.uk/0,39020330,39240189,00.htm

TROJANS TARGET UNPATCHED IE FLAW

Computer users have been warned that several Trojan horses that exploit an unpatched flaw in Internet Explorer (IE) have been discovered. Two exploits that use the recently disclosed vulnerability were reported by antivirus company Sophos on Friday, December 2. Called Clunky-B and Delf-LT, the exploits could allow malicious code to be executed remotely on a user's PC. These Trojans could "download anything, including a 'banker Trojan' that gives up your bank details," according to a Sophos spokesperson. Systems running Microsoft IE on Windows XP Service Packs 1 and 2 are vulnerable to attack. Machines running Windows 98, Windows 98 SE, Windows Me and Windows 2000 Service Pack 4 are also vulnerable to the exploits. Microsoft is not due to issue another round of security patches until Tuesday, December 13. Some security experts have suggested the company should roll out an unscheduled patch before this time to address this flaw. However, it's not clear whether the flaw will even be addressed in the next Microsoft security bulletin. Sophos advised users to turn off the Active Scripting facility in IE, as a stop-gap measure.

Category 21.1 *General QA failures*

2005-12-08 **design flaw malicious anti-piracy approach MacInTouch Printer Setup Mac OS X Tiger**

RISKS 24 12

MALCIOUS ANTI-PIRACY MEASURE IN MACINTOUCH

Veteran RISKS contributor Monty Solomon reports of a dangerous design flaw in MacInTouch printer set up software for Mac OS X Tiger:

[MacInTouch Reader]
Printer Setup Repair, the widely-used utility for Mac OS X printers, has taken a malicious approach to combating software piracy. With version 5.0.3 for Mac OS X Tiger, if the user enters a pirated serial number known to the program, the program will immediately and without any warning remove all user preferences and the user keychain, and possibly do other unknown damage to the user's system.

The response of John Goodchild, President of Fixamac Software, Inc to this was:

Thank you for bringing this to our attention. We have examined our code and discovered an error in the area that rejects pirated registration codes. The original objective was to delete the Printer Setup Repair preferences but a misplaced space in the code allowed the entire user preferences folder to be erased. This would only occur if a pirated code was used. The error was probably overlooked since there was a need to block a new batch of pirated codes quickly. There was no such error in the area that handles legitimate registration codes and in no way can occur if a legitimate registration code is entered incorrectly since the user name is also a part of our internal tests. We have fixed the problem and posted an update. This was not a malicious act on our part, rather an effort to protect our product from software pirates, and we regret any damage that may have been caused by the use of pirated registration codes. Anyone who downloaded Printer Setup Repair 5.0.3 between 11-05-05 and 12-06-05 should download the current release from our web site.

Category 21.1 *General QA failures*

2005-12-08 **Microsoft Internet Explorer IE7 security improvements blog entry developers**

DHS IAIP Daily;
http://www.techweb.com/wire/security/174906971;jsessionid=WRE35TOIAV2AUQSNDBECKH0CJUMEKJVN

MICROSOFT TO BEEF UP INTERNET EXPLORER 7 SECURITY

Microsoft is changing Internet Explorer (IE) 7's security zones in a bid to create a more attack-resistant browser, according to a public blog entry written by three developers at the software giant. Like its predecessors, IE 7 enforces security policies by clumping sites into four security categories, or zones, dubbed Internet, Intranet, Trusted Sites, and Restricted Sites. Typically, the Intranet zone comes with fewer restrictions than the Internet zone. In the past, however, attackers have sometimes managed to fool IE into treating an outside site as in one of the less-secure zones, known as a "zone-spoofing attack." To prevent some of these attacks, IE 7 will instead treat all sites as being in the more-secure Internet zone, unless the PC is really part of a managed network (such as is often the case in a corporate environment). "This change effectively removes the attack surface of the intranet zone for home PC users," wrote Vishu Gupta, Rob Franco and Venkat Kudulur, on the trio's "IEblog".

Category 21.1 *General QA failures*

2005-12-09 **eBay auction Microsoft Excel zero-day exploit code**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1899697,00.asp

EBAY PULLS BIDDING FOR MICROSOFT EXCEL VULNERABILITY

An unknown security researcher chose a novel way to issue a warning for a code execution flaw in Excel -- posting it for sale on eBay. But the auction was pulled late Thursday, December 8, after discussions between Microsoft and eBay Inc. When the auction was squashed, the bidding had reached $53 and had attracted 19 offers. A spokesperson for Microsoft confirmed that the eBay listing was indeed a legitimate security flaw in Excel. In the listing, posted by a seller named "fearwall," the issue is described as a zero-day vulnerability that was discovered on Tuesday, December 6, 2005, and reported to Microsoft. The seller openly taunts the software giant, poking fun at the company's delays in providing fixes for known security bugs. "It can be assumed that no patch addressing this vulnerability will be available within the next few months. So, since I was unable to find any use for this by-product of Microsoft developers, it is now available for you at the low starting price of $0.01 (a fair value estimation for any Microsoft product)," the listing read.

Category 21.1 General QA failures

2005-12-12 **vulnerability attack Web Internet Mozilla Firefox bug arbitrary code execution**

DHS IAIP Daily;
http://www.infoworld.com/article/05/12/12/Hnmozillabug_1.html

NEW ATTACK TARGETS KNOWN MOZILLA BUG

Computer users who have not upgraded to the latest version of Mozilla Corp.'s Firefox browser may now have an extra incentive to do so, thanks to a hacker going by the name of Aviv Raff. On Sunday, December 11, Raff published a sample code (http://aviv.raffon.net/2005/12/11/MozillaUnderestimateVulnerabilityYetAgainPlusOldVulnerabilityNewExploit.aspx) that could be used to take over the computers of Firefox users running version 1.0.4 or earlier of the browser. The exploit takes advantage of a known bug (http://www.mozilla.org/security/announce/mfsa2005-50.html) in the way that Firefox processes the popular Javascript Web programming language. "I think it's been enough time for people to upgrade from v1.0.4. of Firefox. So, here is the PoC [proof of concept] exploit for the…vulnerability," he wrote on his blog. The bug was fixed in Mozilla version 1.0.5, which was released last July, and has also been fixed in version 1.7.9 of the Mozilla Suite, said Mike Schroepfer, vice president of engineering with Mozilla Corp. In some ways, this latest exploit is similar to the attack code that has been circulating for Microsoft's Internet Explorer browser, said Russ Cooper, scientist with security vendor Cybertrust Inc. "It can install and run code of the attacker's choice if a victim visits a malicious Website," he said.

Category 21.1 General QA failures

2005-12-12 **vulnerability hole Nortel SSL VPN Web interface remote command execution upgrade issued**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/2845

NORTEL SSL VPN WEB INTERFACE REMOTE COMMAND EXECUTION VULNERABILITY

A vulnerability has been identified in Milliscripts, which may be exploited by attackers to execute arbitrary commands. This is due to an input validation error in the "tunnelform.yaws" script when processing a specially crafted "a" parameter, which may be exploited by attackers to inject arbitrary commands via the embedded Java Applet and cause malicious scripting code to be executed by the user's browser in the security context of an affected Website. Solution: Upgrade to version 5.1.5.

Category 21.1 General QA failures

2005-12-13 **vulnerability Microsoft DirectX DirectShow AVI processing buffer overflow solution issued**

DHS IAIP Daily; http://www.securityfocus.com/bid/15063/references

MICROSOFT DIRECTX DIRECTSHOW AVI PROCESSING BUFFER OVERFLOW VULNERABILITY

A buffer overflow vulnerability exists in the Microsoft Windows DirectX component. This issue is related to processing of .AVI (Audio Visual Interleave) media files. The specific vulnerability exists in DirectShow and could be exposed through applications that employ DirectShow to process .AVI files. Successful exploitation will permit execution of arbitrary code in the context of the user who opens a malicious .AVI file. This issue could be exploited through any means that will allow the attacker to deliver a malicious .AVI file to a victim user. In Web-based attack scenarios, exploitation could occur automatically if the malicious Webpage can cause the .AVI file to be loaded automatically by Windows Media Player. Other attack vectors such as email or instant messaging may require the victim user to manually open the malicious .AVI. Solution:
http://www.securityfocus.com/bid/15063/solution

Category 21.1 General QA failures

2005-12-14 **Microsoft Software Update Services SUS glitch security patches**

DHS IAIP Daily;
http://www.infoworld.com/article/05/12/14/HNmspatches_1.html

MICROSOFT'S SECURITY PATCHES HIT SNAG

Some users of Microsoft Corp.'s Software Update Services (SUS) may be experiencing a minor annoyance, thanks to a glitch in the company's latest security patches, released Tuesday, December 13. The latest update may be changing the status of software updates that had been previously approved by administrators who use the service, according to Microsoft. "If you synchronize your server after December 12, 2005, all previously approved updates may be unapproved and the status may appear as 'updated,'" Microsoft said in a note published Wednesday, December 14. SUS is used by Microsoft administrators to gain more control over which Microsoft software patches get installed on their network. When a patch has been tested and determined to be appropriate for installation, it can be marked as "approved" and then automatically installed on the PCs being managed by the service. Tuesday's glitch disrupts that process. The problem is that the latest updates appear to have overwritten a file that is used to keep track of approved updates, said Russ Cooper, a scientist at security vendor Cybertrust Inc. The simplest solution is to simply restore this file, called Approveditems.txt, from a backup copy, Cooper said.

Category 21.1 General QA failures

2005-12-16 **compiler trust trusted computing base Trojan horse insertion code software engineering quality assurance design flaws subversion**

RISKS; http://www.acsa-admin.org/2005/abstracts/47.html 24 13

COUNTERING TRUSTING TRUST THROUGH DIVERSE DOUBLE-COMPILING

David A. Wheeler published a paper about trusting compilers.

>Everyone here should be familiar with Ken Thompson's famous "Reflections on Trusting Trust." If not, see: < http://www.acm.org/classics/sep95/>. The "trusting trust" attack subverts the compiler binary; if attacker succeeds, you're doomed. Well, till now.

I've written a paper on an approach to counter this attack. See: "Countering Trusting Trust through Diverse Double-Compiling."

Here's the abstract:

An Air Force evaluation of Multics, and Ken Thompson's famous Turing award lecture "Reflections on Trusting Trust," showed that compilers can be subverted to insert malicious Trojan horses into critical software, including themselves. If this attack goes undetected, even complete analysis of a system's source code will not find the malicious code that is running, and methods for detecting this particular attack are not widely known. This paper describes a practical technique, termed diverse double-compiling (DDC), that detects this attack and some unintended compiler defects as well. Simply recompile the purported source code twice: once with a second (trusted) compiler, and again using the result of the first compilation. If the result is bit-for-bit identical with the untrusted binary, then the source code accurately represents the binary. This technique has been mentioned informally, but its issues and ramifications have not been identified or discussed in a peer-reviewed work, nor has a public demonstration been made. This paper describes the technique, justifies it, describes how to overcome practical challenges, and demonstrates it.<

Category 21.1 General QA failures

2005-12-16 **vulnerability quality assurance Q&A Microsoft Internet Explorer IE7 critical fix**

DHS IAIP Daily; http://news.com.com/Microsoft+patch+jams+up+IE/2100−1002_3−5 999193.html

MICROSOFT PATCH JAMS UP IE

The "critical" security fix for Internet Explorer (IE) available last Tuesday, December 13, is causing trouble for users who have been testing the new IE 7 browser. Microsoft has received "scattered reports of users experiencing odd browser behavior" after installing the latest security update, Jeremy Dallman, project manager for IE security at the company, wrote in a Friday, December 16, posting to a corporate blog. Three different problems have been reported: The browser could crash right after starting up; links may come up blank; or multiple windows may open when the browser is initiated, according to the posting. "After investigating several of these reports, we have traced these issues to a common source," Dallman wrote. The culprit is IE 7, the next version of Microsoft's Web browser, which is in beta testing. The problems occur only if IE 7 is installed on a machine alongside IE 6. That double-IE configuration is not supported by the fix, according to Dallman's note. When installed next to IE 6, the first beta of IE 7 will add an incorrectly configured key to the Windows Registry the first time it is run, he wrote. This can be resolved by deleting the key from the Windows Registry.

Category 21.1 General QA failures

2005-12-20 **Kansas state lottery non-random pseudo-random number generator winning quality assurance QA software design flaw**

RISKS; http://abcnews.go.com/US/story?id=1425383 24 13

"RANDOM" LOTTERY WINNERS?

The same three numbers (5-0-9) came up in the same order on 16, 17, and 18 Dec 2005 in the Kansas Lottery Pick Three. On the third night, many people apparently chose 5-0-9, costing the lottery nearly twice what was paid in. Lottery security officials insist that the system was working normally. (Perhaps the random-number generator had gone to seed?)

[Abstract by Peter G. Neumann]

Category 21.1 General QA failures

2005-12-21 **vulnerability Cisco downloadable RADIUS policies information disclosure**

DHS IAIP Daily; http://www.securityfocus.com/bid/16025/info

CISCO DOWNLOADABLE RADIUS POLICIES INFORMATION DISCLOSURE VULNERABILITY

Cisco PIX and VPN 3000 concentrators, when managed by Cisco Secure Access Control Servers are vulnerable to an information disclosure vulnerability. This issue is due to a design flaw that communicates sensitive information over an unencrypted communications channel. This issue allows remote attackers with the ability to gain access to sensitive information if they can sniff network packets traveling between affected devices and the RADIUS server. This information potentially aids them in further attacks. Specific Cisco versions and products affected by this issue are not currently known. The list of affected packages will be updated as further information is disclosed.

Category 21.1 *General QA failures*

2005-12-23 **spreadsheet software quality assurance assumptions questions**

RISKS; http://www.sciencenews.org/articles/20051217/mathtrek.asp 24 13

QUESTIONING SPREADSHEET SOFTWARE QUALITY ASSURANCE

Spreadsheets create an illusion of orderliness, accuracy, and integrity. The tidy rows and columns of data, instant calculations, eerily invisible updating, and other features of these ubiquitous instruments contribute to this soothing impression. At the same time, faulty spreadsheets and poor spreadsheet practices have been implicated in a wide variety of business and financial problems.

[Abstract by Peter G. Neumann]

RISKS moderator Dr Neumann (PGN) adds:

PGN-excerpted from a nice article with a bunch of references, including Ivars' 1996 book, Fatal Defect: Chasing Killer Computer Bugs, which itself cited some earlier RISKS reports. The last two references are particularly relevant:

The European Spreadsheet Risks Interest Group (EuSpRIG) has a Web site at http://www.eusprig.org/.

Spreadsheet Research, maintained by Ray Panko of the University of Hawaii, is a repository for research on spreadsheet development, testing, use, and technology: http://panko.cba.hawaii.edu/ssr/.

Category 21.1 *General QA failures*

2005-12-24 **PC NetLink unsafe temporary files elevated privileges target unsafe arbitrary information Security Tracker solution patch**

DHS IAIP Daily; http://securitytracker.com/alerts/2005/Dec/1015408.html

PC Netlink 'slsmgr' unsafe temporary files lets local users gain elevated privileges.

A vulnerability was reported in PC NetLink in the 'slsmgr' command. A local user may be able to gain elevated privileges on the target system. The '/opt/lanman/sbin/slsmgr' command in PC NetLink 2.0 opens files in the '/tmp' directory in an unsafe manner. A local user can cause arbitrary information to be written to the filesystem with the permissions of the user running 'slsmgr'. A local user is then able to write files to execute arbitrary code on the target system. The code will run with the privileges of the target user running 'slsmgr'. Security Tracker reports that a fix has been issued for PC NetLink 2.0 (for Solaris 7, 8 and 9) with patch 121209-01 or later. Solution: http://sunsolve.sun.com/search/document.do?assetkey=1-26-102 122-1

Category 21.1 *General QA failures*

2005-12-24 **PC NetLink unsafe temporary files elevated privileges target unsafe arbitrary information Security Tracker solution patch**

DHS IAIP Daily; http://securitytracker.com/alerts/2005/Dec/1015409.html

PC NetLink 'slsadmin' unsafe temporary files lets local users gain elevated privileges.

A vulnerability was reported in PC NetLink in the 'slsadmin' command. A local user may be able to gain elevated privileges on the target system. The '/etc/init.d/slsadmin' command in PC NetLink 2.0 opens files in the '/tmp' directory in an unsafe manner. A local user can cause arbitrary information to be written to the filesystem with the permissions of the user running 'slsadmin'. As a result, the local user can cause arbitrary code to be executed. A local user can write files to execute arbitrary code on the target system. The code will run with the privileges of the target user running 'slsadmin'. Security Tracker reports that a solution is available for PC NetLink 2.0 (for Solaris 7, 8 and 9) with patch 121332-01 or later. Solution: http://www.sunsolve.sun.com/search/document.do?assetkey=1-26 -102117-1

Category 21.1 *General QA failures*

2005-12-26 **Golden FTP Server APPE buffer overflow vulnerability boundary error command supplying argument Secunia connected trusted networks**

DHS IAIP Daily; http://secunia.com/advisories/18245/

Golden FTP Server APPE command buffer overflow vulnerability.

A vulnerability in Golden FTP Server can be exploited to compromise a vulnerable system. The vulnerability is caused due to a boundary error in the handling of the "APPE" FTP command. This can be exploited to cause a buffer overflow by supplying an overly long argument. The vulnerability has been confirmed in version 1.92. Other versions may also be affected. Secunia reports that the problem can be avoided by using the product only when connected to trusted networks.

Category 21.1 *General QA failures*

2005-12-28 **Microsoft Window Graphics Engine WMF format code execution vulnerability malicious file remotely attacker privileges Security Focus patches**

DHS IAIP Daily; http://www.securityfocus.com/bid/16074/discuss

MICROSOFT WINDOWS GRAPHICS RENDERING ENGINE WMF FORMAT UNSPECIFIED CODE EXECUTION VULNERABILITY.

Microsoft Windows WMF graphics rendering engine is affected by a remote code execution vulnerability. The problem presents itself when a user views a malicious WMF formatted file, triggering the vulnerability when the engine attempts to parse the file. The issue may be exploited remotely or by a local attacker. Any code execution that occurs will be with SYSTEM privileges due to the nature of the affected engine. Microsoft Windows XP is considered to be vulnerable at the moment. It is likely that other Windows operating systems are affected as well. Security Focus is not aware of any vendor-supplied patches for this issue.

Category 21.1 *General QA failures*

2005-12-29 **quality assurance QA bank system automatic debit**

RISKS; BBC http://news.bbc.co.uk/1/hi/uk/4567944.stm 24 14

AUTOMATIC DONATIONS MULTIPLIED BY 100

Approximately 10,000 UK supporters of Greenpeace who make regular donations by direct debit have have accidentally had their bank accounts debited by a hundred times their usual amount, with its software adding two noughts to the latest batch of direct debit demands.

I would hazard a guess that some manual intervention was made, perhaps to update the records for a new calendar year, leading to a mistake by a real human being rather than "the computer."

[Abstract and comments by Nick Rothwell]

Category 21.1 *General QA failures*

2005-12-31 **denial of service DoS vulnerability Enterprise Server Attachment Service TIFF attachment Blackberry heap buffer overflow no update software**

DHS IAIP Daily; http://www.securityfocus.com/bid/16098/solution 23

BLACKBERRY ENTERPRISE SERVER ATTACHMENT SERVICE TIFF ATTACHMENT DENIAL OF SERVICE VULNERABILITY

Research In Motion Blackberry Enterprise Server is prone to denial of service attacks. This issue affects the Attachment Service and may be triggered by a malformed TIFF attachment. The issue is reportedly caused by a heap-based buffer overflow. Security Focus reports that the vendor has stated that this issue will result in a denial of service, and it is therefore not believed that the issue is exploitable beyond a denial of service at the time of writing. This BID will be updated if further information is made available that contradicts this assumption. Security Focus is unaware of any vendor-supplied patches for this issue.

Category 21.1 *General QA failures*

2005-12-31 **denial of service DoS vulnerability Enterprise Server Router SRP Pack Blackberry no update software**

DHS IAIP Daily; http://www.securityfocus.com/bid/16100/solution 23

BLACKBERRY ENTERPRISE SERVER ROUTER SRP PACKET DENIAL OF SERVICE VULNERABILITY

The Blackberry Enterprise Server Router component is prone to a denial of service vulnerability. This vulnerability may be triggered by sending malformed SRP (Server Routing Protocol) packets to the router. This could only be exploited by an attacker who can communicate with the router. Security Focus reports that the vendor has acknowledged the issue and stated that it will be corrected in future releases. Security Focus is unaware of any vendor-supplied patches for this issue.

Category 21.1 *General QA failures*

2006-01-03 **denial of service DoS Intel Graphics Accelerator driver Microsoft Windows XP 2000 2K crash**

DHS IAIP Daily; http://www.securityfocus.com/bid/16127/references 23

INTEL GRAPHICS ACCELERATOR DRIVER REMOTE DENIAL OF SERVICE VULNERABILITY

The Intel Graphics Accelerator driver is susceptible to a remote denial of service vulnerability. This issue is demonstrated to occur when the affected driver attempts to display an overly long text in a text area. This allows attackers to crash the display manager on Microsoft Windows XP, or cause a complete system crash on computers running Microsoft Windows 2000. Other operating systems where the affected display driver is available are also likely affected.

Category 21.1 *General QA failures*

2006-01-03 **denial of service vulnerability DoS BlackBerry Enterprise Server Phenoelit German hacker group Research in Motion software fixes**

DHS IAIP Daily; http://www.informationweek.com/showArticle.jhtml;jsessionid= HCQOZBHQGSYK0QSNDBCSKHSCJUMEKJVN?articleID=175800729 23

HACKERS FIND SECURITY HOLE IN BLACKBERRY ENTERPRISE SERVER

Research In Motion's (RIM) BlackBerry Enterprise Server product may be vulnerable to denial of service attacks, according to a group of German hackers, called Phenoelit, that identifies security flaws. Phenoelit found a problem in the way the server's BlackBerry Router handles Server Routing Protocol packets. An attacker could cause denial of service by sending "specially crafted" packets to the router, according to the U.S. Computer Emergency Readiness Team. The result could be disrupted communications between the BlackBerry Enterprise Server and BlackBerry devices. In a prepared statement, Research In Motion said it "has already developed software fixes for the issues identified by [the group] and although there have been no customer reports of any actual problems, RIM has also provided temporary precautionary measures that can be taken in the mean time until customers are able to implement the software updates." RIM asks companies to make sure their BlackBerry Enterprise Server and BlackBerry Router are located behind the corporate firewall. RIM calls it an "internal-only vulnerability" that can be caused by an inside attacker.

Category 21.1 *General QA failures*

2006-01-04 **buffer overflow vulnerability ESRI ArcPad arbitrary command execution**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2006/0032 23

ESRI ARCPAD ".APM" FILE HANDLING REMOTE BUFFER OVERFLOW VULNERABILITY

A vulnerability has been identified in ESRI ArcPad, which could be exploited by remote attackers to execute arbitrary commands. This flaw is due to a buffer overflow error when processing malformed ".amp" files containing an overly long "COORDSYS" string attribute, which could be exploited by attackers to compromise a vulnerable system by convincing a user to open a specially crafted "apm" file. The FrSIRT is not aware of any official supplied patch for this issue.

Category 21.1 General QA failures

2006-01-06 **denial of service DoS IBM Lotus Domino vulnerability**

DHS IAIP Daily; http://secunia.com/advisories/18328/ 23

IBM LOTUS DOMINO DENIAL OF SERVICE AND UNSPECIFIED VULNERABILITIES

Some vulnerabilities have been reported in Lotus Domino, which potentially can be exploited by malicious users to cause a denial of service (DoS), or with unknown impact. Analysis is as follows: 1) Some unspecified potential security issues have been reported in "Agents"; 2) An unspecified boundary error in CD to MIME Conversion may cause a buffer overflow. This may be exploited to cause the router service to crash or become unresponsive; 3) A stack overflow error in Domino for AIX when evaluating a long formula in "Design" can potentially be exploited to crash Domino via an overly long recursive formula; 4) Some unspecified errors in the Directory Services can potentially be exploited to cause a DoS, e.g. via a crash when performing LDAP searches; 5) An unspecified error in the IMAP Server may cause the service to become unresponsive and unable to initiate new IMAP sessions; 6) An unspecified error may cause the server to crash when compact was executed from the client; 7) Several unspecified errors may cause the Web server to crash when handling corrupted bitmap images or when performing the "Delete Attachment" action.

Category 21.1 General QA failures

2006-01-18 **vulnerability Oracle products critical patch update**

DHS IAIP Daily; http://www.us−cert.gov/cas/techalerts/TA06−018A.html 23

TECHNICAL CYBER SECURITY ALERT TA06-018A:
ORACLE PRODUCTS CONTAIN MULTIPLE VULNERABILITIES

Oracle has released a critical patch update that addresses more than eighty vulnerabilities in different Oracle products and components. The impact of these vulnerabilities varies depending on the product, component, and configuration of the system. Potential consequences include the execution of arbitrary code or commands, information disclosure, and denial of service. Vulnerable components are likely to be available to attackers via remote networks and with limited or no prior authorization. An attacker who compromises an Oracle database may be able to gain access to sensitive information. According to Oracle, three of the vulnerabilities corrected un the Oracle Critical Patch Update for January 2006 affect Oracle Database Client-only installations. US-CERT recommends that sites running Oracle review the Critical Patch Update, apply patches, and take other mitigating action as appropriate. US-CERT is tracking all of these issues under VU#545804:
http://www.kb.cert.org/vuls/id/545804 Oracle Critical Patch Update - January 2006:
http://www.oracle.com/technology/deploy/security/pdf/cpujan2 006.html

---

Category 21.1 General QA failures

2006-01-18 **Oracle database server vulnerability flaws update release**

DHS IAIP Daily; 23
http://www.techweb.com/wire/security/177101585;jsessionid=VA
JPECC3JG220QSNDBGCKHSCJUMEKJVN

ORACLE FIXES 82 DATABASE, SERVER FLAWS

Oracle on Tuesday, January 17, patched 82 different vulnerabilities in its flagship database and other server products, leading security company Symantec to raise the overall Internet threat status and others puzzling over the exact extent of the risk. The Critical Patch Update fixes 37 flaws in Oracle's Database, 17 in its Application Server, 20 in the Collaboration Suite, 27 in E-Business Suite, and one each in the PeopleSoft Enterprise Portal and JD Edwards HTML Server. While the number may seem staggering to those not used to Oracle's quarterly security updates -- Windows users, for instance, go into shock when Microsoft releases more than a dozen fixes in a given month -- January's batch is actually smaller than the October 2005 bunch. Then, Oracle patched 106 different bugs. Many of this quarter's fixed vulnerabilities were tagged by Oracle with its highest risk ratings -- unlike other vendors such as Microsoft, Oracle breaks out risk rankings into numerous sub-categories -- with notes that they're easy to exploit and have a potentially wide range of impact. Among the bugs are many which can be exploited remotely, and 61 which can be used by anonymous (non-authenticated) users.

Category 21.1 General QA failures

2006-01-18 **Cisco CallManager denial of service DoS vulnerability**

DHS IAIP Daily; http://www.cisco.com/warp/public/707/cisco−sa−20060118−ccmdos.shtml 23

CISCO CALLMANAGER DENIAL OF SERVICE

Vulnerable versions of Cisco CallManager do not manage TCP connections and Windows messages aggressively, leaving some well known, published ports vulnerable to denial of service attacks. CallManager does not time out TCP connections to port 2000 aggressively enough, leading to a scenario where memory and CPU resources are consumed with enough open connections. In specific scenarios, CallManager will leave the TCP connection open indefinitely until either the CallManager service is restarted or the server is rebooted.

Category 21.1 General QA failures

2006-01-25 **Gartner Oracle security vulnerability exploit**

DHS IAIP Daily; http://www.techweb.com/wire/security/177103864;jsessionid=O40E1UZM0ACXCQSNDBGCKH0CJUMEKJVN 23

Gartner bashes Oracle over security.

Oracle security practices are raising red flags, a Gartner analyst recently warned, and administrators should hunker down in protecting their database systems. Just five days after Oracle released a critical security update that patched 82 vulnerabilities, a Gartner researcher said in an online advisory that "Oracle can no longer be considered a bastion of security." Rich Mogull wrote, "The range and seriousness of the vulnerabilities patched in this update cause us great concern.... The database products alone include 37 vulnerabilities, many rated as easily exploitable and some potentially allowing remote database access. Oracle has not yet experienced a mass security exploit, but this does not mean that one will never occur." Mogull noted that Oracle administrators had avoided patching by relying on the database's strong security and the fact that the software was deployed deep within an enterprise's defenses. That no-patching procedure won't cut it now. To keep databases secure, Mogull recommended that companies shield all Oracle systems, patch known bugs -- "because incomplete information from Oracle will make shielding incomplete," he said in an aside -- and pressure Oracle to get on the security stick.

Category 21.1 General QA failures

2006-01-26 **Oracle advisory vulnerability patch immediately**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1915359,00.asp 23

ORACLE ADVISES USERS: PATCH CRITICAL HOLE -- NOW.

Oracle is advising its customers to quickly apply a database patch for a flaw security experts are calling "very severe." Security experts warn the hole could allow even unsophisticated users to take control of Oracle databases. The patch, known as DB18, fixes a hole that affects most supported versions of the Oracle database software, including Oracle versions 8, 9 and 10. The hole is "very severe" and allows users to bypass the Oracle database's authentication and become administrative "super users," according to Shlomo Kramer, CEO of Imperva, which discovered the hole. However, Kramer and others say Oracle may be downplaying the seriousness of the threat out of concern that malicious hackers could be tipped off to the severity of the issue. Oracle Corp. said that it patches security holes in the order of their severity and categorized DB18 as a serious vulnerability with the potential for wide impact in the January Critical Patch Update [CPU], according to an e-mail statement. Researchers in Imperva's Application Defense Center discovered the security hole "a few months ago," though it has existed for years, Kramer said. "It goes all the way back to Version 8, but it wasn't patched until now."

Category 21.1 *General QA failures*

2006-01-31 **Perl programming scripting language vulnerability printing functions write arbitrary process memory code execution solution update**

DHS IAIP Daily; http://www.securityfocus.com/bid/15629/discuss 23

PERL PERL_SV_VCATPVFN FORMAT STRING INTEGER WRAP VULNERABILITY.

Perl is susceptible to a format-string vulnerability. This issue is due to the programming language's failure to properly handle format specifiers in formatted printing functions. An attacker may leverage this issue to write to arbitrary process memory, facilitating code execution in the context of the Perl interpreter process. This can result in unauthorized remote access. Developers should treat the formatted printing functions in Perl as equivalently vulnerable to exploitation as the C library versions, and should properly sanitize all data passed in the format specifier argument. Solution: Webmin has released updated versions of Webmin and Usermin to fix the insecure usage of the formatted printing functions. See the following Website for more solution details: http://www.securityfocus.com/bid/15629/solution

---

Category 21.1 *General QA failures*

2006-01-31 **Winamp music player quality assurance QA buffer overflow vulnerability flaw**

DHS IAIP Daily; http://secunia.com/advisories/18649/ 23

WINAMP COMPUTER-NAME-HANDLING BUFFER-OVERFLOW VULNERABILITY.

ATmaCA has discovered a vulnerability in Winamp, which can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to a boundary error during the handling of filenames including a computer name. This can be exploited to cause a buffer overflow via a specially crafted playlist containing a filename starting with an overly long computer name (about 1040 bytes). Solution: Update to version 5.13.

Category 21.1 *General QA failures*

2006-02-11 **quality assurance design municipal property tax human user error quality assurance QA plausibility**

RISKS; http://tinyurl.com/rq8p8 24 15

TRUSTING THE COMPUTER CAUSES TAX REVENUE SHORTFALL FOR TOWN

In Valparaiso, Indiana, someone pressed the wrong key in the municipal-tax program and accidentally altered the property value for a house originally evaluated at $121,900 so that it was appraised at $400M. No one noticed. The tax bill went from $1,500 to $8M, causing a significant increase in the anticipated municipal tax revenues. Although the faulty tax bill was corrected, the town planners had already lowered the property tax rate to take into account the imaginary $8M windfall and therefore faced a budget deficit for municipal services and schools.

Category 21.1 *General QA failures*

2006-02-28 **Oracle 11i security vulnerability flaw patches Integrigy**

DHS IAIP Daily; http://news.com.com/Oracle+patches+11i+security+flaws/2100 −1 002_3−6044020.html?tag=cd.lede 23

ORACLE PATCHES 11I SECURITY FLAWS.

Oracle has issued an upgrade to its E-Business Suite 11i diagnostics module containing a number of the security fixes, according to applications security firm Integrigy. Oracle made an unusual move by alerting its users about the security patches, according to Integrigy's advisory. Historically, Oracle has released product upgrades but not disclosed whether they included security fixes, Integrigy noted. The "Diagnostics Support Pack February 2006 with Oracle Diagnostics 2.3 RUP A" aims to address security flaws in Oracle diagnostics Web pages and Java classes, according to Integrigy. "The significant (security) issue is (that) some diagnostics can be executed without any authentication, and it is possible to configure the diagnostics to be unrestricted," according to the Integrigy report. Although the company releases quarterly security updates, "Oracle has not previously provided customers a notification that security fixes were included (in an upgrade)," Integrigy noted in its report.

Category 21.1 *General QA failures*

2006-03-01 **vulnerability Oracle E-Business Suite SQL injection command patch update**

DHS IAIP Daily; http://securitytracker.com/alerts/2006/Mar/1015699.html 23

ORACLE E-BUSINESS SUITE 'ORACLE DIAGNOSTICS' BUGS LET REMOTE USERS ACCESS FUNCTIONS AND INJECT SQL COMMANDS.

A vulnerability was reported in Oracle E-Business Suite. A remote user can access diagnostic functions and can inject SQL commands. Analysis: The Oracle Diagnostics Webpages and Java classes in Oracle E-Business Suite contain several vulnerabilities. A remote user can access some of the diagnostic functions. A remote user can also inject SQL commands. There are some permission errors may let remote users access functions or data without authorization. Affected version: 11i. Solution: The vendor has issued the following fix: "Diagnostics Support Pack February 2006 with Oracle Diagnostics 2.3 RUP A." The fix will be included in the next quarterly Critical Patch Update (April 18, 2006).

Category 21.1 *General QA failures*

2006-03-08 **Symantec Ghost software multiple vulnerabilities data modification privilege escalation arbitrary code execution**

DHS IAIP Daily; http://www.hackerscenter.com/archive/view.asp?id=23418 23

SYMANTEC GHOST MULTIPLE VULNERABILITIES.

Three vulnerabilities have been reported in Symantec Ghost, which can be exploited by malicious, local users to gain knowledge of potentially sensitive information, modify certain data, and potentially gain escalated privileges. Analysis: Default administrator login ID and password left behind during installation can be used by local users to modify or delete stored administrative tasks. This can be exploited to modify tasks to run arbitrary code on the local system. Insecure permissions in the shared memory sections within the Sybase SQLAnywhere database used by Symantec Ghost can potentially be exploited to gain access to, and to modify information stored in the database. A boundary error in the login dialog box of dbisqlc.exe, which is installed as a part of the SQLAnywhere package, can cause a buffer overflow. This can potentially be exploited to gain access to information stored in the database that is not normally accessible. Vulnerable: Symantec Ghost 8.x; Symantec Ghost Solution Suite 1.x. Solution: Update to Symantec Ghost 8.3 that is shipped as a part of Symantec Ghost Solutions Suite 1.1.

Category 21.1 *General QA failures*

2006-03-08 **quality assurance QA error failure Scholastic Aptitude Test (SAT) scores students admissions**

RISKS; College Board http://tinyurl.com/zj8wh 24 19

DAMP PAPERS CAUSE ERRORS IN SAT TEST SCORES

On the order of 4000 [4,400] students taking the October 2005 Scholastic Aptitude Tests (SATs) received scores lower than they should have been [and 600 got higher scores than they achieved], due to [initially] unexplained "technical problems" [later described as dampness that expanded the paper sheets]. Some scores on the reasoning section were as much as 100 [actually as bad as 450] points too low (out of 800 [or 2400]). This may be unfortunate for those students, considering that the final acceptances and rejections are being decided before the affected universities have been notified. Similar scanning problems were noted in an earlier SAT chemistry test, although on a smaller scale.

[An NPR "All Things Considered" story by Claudio Sanchez on April 25 reported that "Angry parents -- and their lawyers -- are demanding answers." The College Board announced new quality assurance measures to prevent a repetition of the scanning errors including scanning the sheets twice (once on each of two days) and comparing the results to spot mechanical problems.]

[Abstract by Peter G. Neumann; updated information inserted by MK]

Category 21.1 *General QA failures*

2006-03-09 **quality assurance QA automatic word processor spell checker conversion correction errors**

Language Log http://itre.cis.upenn.edu/~myl/languagelog/archives/002911.html

THE CUPERTINO EFFECT

Benjamin Zimmer posted an amusing analysis of a peculiar automatic correction in some word processing software: the misspelling "cooperatino" (for "cooperation") is corrected to "Cupertino." Apparently some European translators have dubbed this problem "The Cupertino Effect." Zimmer writes,

>Here's a brief sampling of the hundreds of Cupertinos one can find on the ".int" domain used by international groups like the UN, the EU and NATO:

* Within the GEIT BG the Cupertino with our Italian comrades proved to be very fruitful. (NATO Stabilisation Force, "Atlas raises the world," 14 May 2003)

* The fact that Secretary General Robertson is going to join this session this afternoon in the European Union headquarters gives you already an idea of how close and co-ordinated this Cupertino is and this action will be. (NATO Press Point, 19 Mar. 2001)

* Safe blood transfusion services are being addressed in Freetown and Lungi, using WHO RB funds in Cupertino with the Red Cross Society of Sierra Leone and in Bo by MSF/Belgium. (WHO/EHA report on Sierra Leone, 1 May 2000)

* Could you tell us how far such policy can go under the euro zone, and specifically where the limits of this Cupertino would be? (European Central Bank press conference, 3 Nov. 1998)

* Co-ordination with the World Bank Transport and Trade Facilitation Programme for South East Europe will be particularly important in the area of trade facilitation and shall be conducted through regular review mechanisms and direct Cupertino. (European Agency for Reconstruction, "Focal area: Justice and home affairs") . . . .<

Apparently another automatic correction changes "coperation" to "copulation" as in the following examples:

* "Albania was very interested in concluding a customs copulation agreement."

* "The Heads of State and Government congratulated SATCC for the crucial role it plays in strengthening copulation and accelerating the implementation of regional programmes in this strategic sector. (Southern African Development Community, Communique from the 1982 SADC Summit)"

* "The Western Balkan countries confirmed their intention to further liberalise trade amongst each other. They requested that they be included in the pan-european system of diagonal copulation, which would benefit trade and economic development. (International Organization for Migration, Foreign Ministers Meeting, 22 Nov. 2004)"

Category 21.1 *General QA failures*

2006-03-10 **quality assurance QA automatic spreadsheet format conversion correction errors**

RISKS 24 19

MS-EXCEL DAMAGES EXPERIMENTAL DATA

Biomedical researchers reported that MS-Excel converted some gene names into dates, damaging data sets and causing rejection of the damaged data. The authors listed 30 gene names such as DEC1 that got converted to dates (e.g., to 1-Dec). A worse problem occurred when data identifiers contained the letter E in a string of digits; these identifiers were irreversibly converted to floating point numbers in scientific notation. The authors wrote,

>There is another default conversion problem for RIKEN clone identifiers identifiers of the form nnnnnnnEnn, where n denotes a digit. These identifiers are comprised of the serial number of the plate that contains the library, information on plate status, and the address of the clone. A search … identified more than 2,000 such identifiers out of a total set of 60,770. For example, the RIKEN identifier "2310009E13" was converted irreversibly to the floating-point number "2.31E+13." A non-expert user might well fail to notice that approximately 3% of the identifiers on a microarray with tens of thousands of genes had been converted to an incorrect form, yet the potential for 2,000 identifiers to be transmogrified without notice is a considerable concern. Most important, these conversions to an internal date representation or floating-point number format are irreversible; the original gene name cannot be recovered.<

Peter G. Neumann commented, "If some computer virus or trojan did this sort of damage to the results of thousands of high-cost biomedical experiments, I imagine that we'd see a serious effort to put some people in jail. I'm not suggesting that any similar sort of retribution is appropriate here, but perhaps some rehabilitation would be in order. . . ."

Category 21.1 *General QA failures*

2006-03-27 **Microsoft .NET Framework SDK ildasm buffer overflow vulnerability denial-of-service DoS system compromise**

DHS IAIP Daily; http://secunia.com/advisories/19406/ 23

MICROSOFT .NET FRAMEWORK SDK ILDASM BUFFER OVERFLOW.

A vulnerability has been discovered in Microsoft .NET Framework SDK, which can be exploited by malicious people to cause a denial-of-service and potentially compromise a user's system. Analysis: The vulnerability is caused due to a boundary error within ildasm when disassembling a DLL file. This can be exploited to cause a heap based buffer overflow when a specially crafted DLL is disassembled. Affected software: Microsoft .NET Framework 1.x. Solution: Do not use ildasm to disassemble untrusted DLL files.

Category 21.1 *General QA failures*

2006-03-28 **bounds sanity checking quality assurance QA control QC procedures debit bank data input error correction**

RISKS; AP http://tinyurl.com/o45wj 24 22

DEBIT CARD TYPO RENDERS COUPLE PENNILESS

An AP item datelined Palmdale, California notes that George Beane was charged $4,334.33 for four burgers at Burger King. To make a long story short, the cashier entered $4.33 and then forgetfully reentered the same amount again, resulting in a debit-card charge that instantly was paid out of his Bank of America account, wiping out their balance. After this was discovered, the bank insisted the funds were on a three-day hold and the debit could not be be reversed. [The AP article said, "Burger King did not charge the Beanes for their meal, and the couple got their $4,334.33 back on Friday."] "For those three days, those were the most expensive value burgers in history," Pat Beane said.

[Abstract by Peter G. Neumann; additions by MK]

Mark Feit added in RISKS 24.23:

>[Debit-card] Transactions at countertop terminals do have a bounds check, but it happens at the wrong point in the transaction. The customer receipt and store copy are printed *after* the charge has been committed to the clearing house, leaving the cardholder with no way to approve the amount. (Even restaurants, which have an extra step where you add a gratuity, have this problem, because the final figure is still un-verified by the customer.) Even if the customer refuses to consummate the transaction by signing, it's still a done deal and the only recourse for correcting it is to take it up with the bank.

I suspect that's what happened in this case, and it's a very good reason to use a real credit card instead of a debit card.<

Category 21.1 General QA failures

2006-04-03 **MySQL query logging bypass vulnerability input data handling no solution**

DHS IAIP Daily; http://www.securityfocus.com/bid/16850/references 23

MYSQL QUERY LOGGING BYPASS VULNERABILITY.

MySQL is susceptible to a query logging bypass vulnerability. This issue is due to a discrepancy between the handling of NULL bytes in input data. Analysis: This allows attackers to bypass the query logging functionality of the database so they can cause malicious SQL queries to be improperly logged. This may help them hide the traces of malicious activity from administrators. Vulnerable: MySQL AB MySQL 5.0.18; MandrakeSoft Linux Mandrake 2006.0 x86_64; MandrakeSoft Linux Mandrake 2006.0; MandrakeSoft Linux Mandrake 10.2 x86_64; MandrakeSoft Linux Mandrake 10.2; MandrakeSoft Corporate Server 3.0 x86_64; MandrakeSoft Corporate Server 3.0. Solution: Currently, Security Focus is not aware of any vendor-supplied patches for this issue.

Category 21.1 General QA failures

2006-04-10 **Oracle Server flaw vulnerability warning exploit code published**

DHS IAIP Daily; 23
http://www.infoworld.com/article/06/04/11/77308_HNoracleexpl oitcode_1.html

ORACLE SERVER FLAW SPARKS WARNING.

A software security expert warned users of Oracle Server that a software flaw could allow any user to read, modify, and delete data used by Oracle applications and that Oracle may have unwittingly shown hackers how to exploit the previously unknown hole. Alex Kornbrust of Red-Database-Security said that an article posted on Oracle's MetaLink knowledge base on Thursday, April 6, identified an unpatched security hole that allows Oracle users with read-only privileges to delete or modify rows of data used by Oracle applications. Sample code published with the knowledge base article showed Oracle customers how the flaw could be exploited, he said. An Oracle spokesperson said the company is preparing a patch to address the vulnerability in a future Critical Patch Update.

Category 21.1 General QA failures

2006-04-12 **quality assurance QA bounds checking**

RISKS; AP; Fox News http://tinyurl.com/m5n57 24 24

TELECOM MALAYSIA BILLS SUBSCRIBER FOR $218 TRILLION

An AP newswire story reported on Yahay Wahab, who was billed for the equivalent of $218 trillion after disconnecting his late father's phone line. He "was ordered to pay up within 10 days or face prosecution…."

Even more fascinating, the AP report included the following sentence:

"It wasn't clear whether the bill was a mistake, or if Yahaya's father's phone line was used illegally after after his death."

Would anyone like to calculate how long it would take to use a single phone to rack up $218 trillion of charges?

[Commentary by MK]

Category 21.1 General QA failures

2006-04-19 **Oracle PeopleSoft software US CERT vulnerability warning**

DHS IAIP Daily; http://www.uscert.gov/cas/techalerts/TA06−109A.html 23

US-CERT TECHNICAL CYBER SECURITY ALERT TA06-109A: ORACLE PRODUCTS CONTAIN MULTIPLE VULNERABILITIES.

Oracle 11 products and components are affected by multiple vulnerabilities. The impacts of these vulnerabilities include remote execution of arbitrary code, information disclosure, and denial-of-service. Systems affected: Oracle Database 10g; Oracle9i Database; Oracle8i Database; Oracle Enterprise Manager 10g Grid Control; Oracle Application Server 10g; Oracle Collaboration Suite 10g; Oracle9i Collaboration Suite; Oracle E-Business Suite Release 11i; Oracle E-Business Suite Release 11.0; Oracle Pharmaceutical Applications; JD Edwards EnterpriseOne, OneWorld Tools; Oracle PeopleSoft Enterprise Tools; Oracle Workflow; Oracle Developer Suite 6i. For more information regarding affected product versions, refer to the Oracle Critical Patch Update -- April 2006. Solution: Apply the appropriate patches or upgrade as specified in the Oracle Critical Patch Update -- April 2006: http://www.oracle.com/technology/deploy/security/pdf/cpuapr2 006.html Note that this Critical Patch Update only lists newly corrected issues. Updates to patches for previously known issues are not listed.

Category 21.1 *General QA failures*

2006-04-28 **HP Oracle OpenView multiple vulnerabilities solution update**

DHS IAIP Daily; http://secunia.com/advisories/19859/ 23

HP ORACLE FOR OPENVIEW MULTIPLE VULNERABILITIES.

HP has acknowledged some vulnerabilities in HP Oracle for Openview, which can be exploited by malicious people to conduct SQL injection attacks, compromise a vulnerable system or with unknown impacts. Analysis: Details have been disclosed for the following vulnerabilities: 1) An input validation error in the Log Miner component ("dbms_logmnr_session" package) can be exploited to manipulate SQL queries by injecting arbitrary SQL code. 2) A boundary error in the "VERIFY_LOG" procedure (provided by the "sys.dbms_snapshot_utl" package) can be exploited by a malicious user to cause a buffer overflow and execute arbitrary code on the system. Affected software: HP Oracle for OpenView 8.x; HP Oracle for OpenView 9.x. Solution: Install the Oracle Critical Patch Update -- April 2006.

Category 21.1 *General QA failures*

2006-05-02 **MySQL remote information disclosure buffer overflow vulnerabilities execute arbitrary code solution update**

DHS IAIP Daily; http://www.securityfocus.com/bid/17780/discuss 23

MYSQL REMOTE INFORMATION DISCLOSURE AND BUFFER OVERFLOW VULNERABILITIES.

MySQL is susceptible to multiple remote vulnerabilities. Analysis: A buffer overflow vulnerability due to insufficient bounds checking of user supplied data before copying it to an insufficiently sized memory buffer. This issue allows remote attackers to execute arbitrary machine code in the context of affected database servers. Failed exploit attempts will likely crash the server, denying further service to legitimate users. Two information disclosure vulnerabilities due to insufficient input sanitization and bounds checking of user supplied data. These issues allow remote users to gain access to potentially sensitive information that may aid them in further attacks. For a complete list of vulnerable products: http://www.securityfocus.com/bid/17780/info Solution: The vendor has released version 5.0.21 of MySQL to address these issues. Versions 4.0.27, 4.1.19, and 5.1.10 are also scheduled to be released in the future. For more information: http://www.securityfocus.com/bid/17780/references

---

Category 21.1 *General QA failures*

2006-05-09 **telephone central switch programming quality assurance QA bug error design flaw area code long distance dialling denial of service DoS**

RISKS 24 28

RISKS OF INADEQUATE TESTING HIT BELL CANADA

In the 613 area code (Ottawa, Eastern Ontario) in Canada, BELL Canada prepared to switch to requiring the area code for all calls including local ones. Rod Davidson reported on a glitch that appeared because of poor testing and planning:

>There is a local 866 exchange so that the phone number 866-1234 (just made up) is a local call. As of this morning, when I tried to dial 1-866-123-4567 I received the message "This is not a long distance call." as soon as I pressed the "4" in the sequence. Dialing "866-1234" got me the message "The mailbox of 866-1234 is full." I'm not really surprised.<

The situation was made worse by BELL Canada operators, who either ignored his explanation of the problem or proposed a service call for a problem that resided at the central office. Davidson pointed out, "When someone reports unusual system behavior (and reports they observed it on several different phone lines) it should raise some sort of red flag."

Category 21.1 General QA failures

2006-05-23 **bounds checking sanity check software programming error quality assurance QA**

RISKS 24 30

PARKING METER CHARGES $8M FOR 63-YEAR PARKING STAY

A humor column in today's _LA Times_ featured a photograph of a self-pay parking kiosk with a mis-set date of 16 May 1943, showing an amount due of $8,082,022.84.

Sanity checking, you ask? Not bloody likely. An auxiliary display shows the fee in larger characters; it reads 8.1E+6. When you have an programmer so clueless as to calculate money values in floating point, there is little hope for subtleties like sanity checking.

As a side point, I'm fascinated that things like parking kiosks now use chips powerful enough to have floating-point support, at least as a library. A 4-bitter would be adequate for the task, though it's not clear to me that this particular programmer could have written the code needed to compute the fee on a 4-bit machine.

[Abstract and commentary by Geoff Kuenning]

21.2 Security product QA failures

Category 21.2 *Security product QA failures*

1997-01-16 **QA quality assurance pornography**

AP

Flintstones-viewers in Springfield, MO were startled in mid January when the Playboy Channel was patched into the Cartoon Channel for several minutes at mid-day while the audio remained in the stone age. At least one concerned mother complained to the cable-TV provider.

Category 21.2 *Security product QA failures*

1997-01-19 **phone fraud QA**

PA News

In England, British Telecom installed 5,000 new pay-phones (adding to a total of 135,000) that were equipped for pre-paid phone cards. Unfortunately, software errors allowed an unspecified technique to be used to make expensive long-distance calls and calls to cellular phones without paying anything. The error was discovered five months after the phones were installed. Losses are unknown but estimated to be in the millions of pounds of lost revenue and obligatory payments to international interexchange carriers. In February, British Telecom assured pay-phone owners that they would not be charged for the fraudulent calls.

Category 21.2 *Security product QA failures*

1997-01-21 **QA**

RISKS 18 78

Older Apollo workstations, now sold and supported by HP, will fail at 14:59 GMT on November 2, 1997 when the high bit of the Domain/OS system clock will set its high bit. Patches are available only for newer releases of the operating system.

Category 21.2 *Security product QA failures*

1997-01-23 **QA**

RISKS 18 79

Software error gave some investors at Schwab (a big brokerage) cause for alarm when Telebroker, an automated phone response system, gave some callers the impression that they had gone broke by ignoring several important mutual funds in tallying net worth. The error lasted more than a day.

Category 21.2 *Security product QA failures*

1997-02-02 **QA**

EDUPAGE

An Assistant Commissioner of the Internal Revenue Service has conceded to a panel created by Congress that a $4-billion computer systems modernization project has failed, that IRS computers "do not work in the real world," and that the agency is incapable of bringing its computer capabilities up to the right level because it lacks the "intellectual capital" for the job. He proposed contracting out the processing of paper returns filed by individuals and abandoning a "big bang" approach to systems modernization in favor an incremental, piecemeal one. Though characterizing the systems as "dysfunctional," the administrator told that panel that the IRS "is wholly dependent on them." (New York Times 31 Jan 97)

Category 21.2 *Security product QA failures*

1997-02-04 **QA Human factors**

RISKS 18 81

The security feature of FORD car radios can easily be subverted by employees who don't understand the purpose of the system. In a case reported to RISKS in February, Paddy Spencer describes how he got his radio code reset with no questions asked — and then had the code helpfully written on a company-supplied label stuck to the side of the radio.

Category 21.2 *Security product QA failures*

1997-02-08 **QA**

PA News

The British National Lottery experienced a software failure that prevented identification of the winners of the nine-million pound jackpot.

Category 21.2 *Security product QA failures*

1997-02-20 **QA**

RISKS 18 83

Several dozen Massachusetts residents received multiple copies of their new driver's license in mid-February. The software glitch was identified and repaired quickly.

Category 21.2 *Security product QA failures*

1997-03-06 **QA Explorer**

EDUPAGE

Microsoft responded to flaws in Internet Explorer security by developing and posting patches within a week.

Category 21.2 *Security product QA failures*

1997-03-07 **QA**

RISKS 18 88

Intuit Inc. sent a letter to its MacInTax users in early March detailing a potential pitfall for electronic filers. Users who fail to save their documents before filing them electronically may receive word from the IRS of an incomplete filing. Intuit Vice President Larry Wolfe said the problem is "absolutely covered" under Intuit's general product guarantee. "If a customer has filed an incomplete electronic return with MacInTax, Intuit will pay the penalty plus any interest assessed by the IRS," he said.

Category 21.2 *Security product QA failures*

1997-03-07 **QA infowar**

RISKS 18 88

After a bombing in the Basque region of northern Spain, two groups of secret policemen fired at each other when, due to unknown factors, their computers were unable to obtain any information about each other's cars. They assumed that the armed men they were confronting were terrorists and started shooting at each other.

Category 21.2 *Security product QA failures*

1997-03-07 **Explorer QA**

RISKS 18 88

More Internet Explorer security holes have been discovered. Eliashim showed that "hostile links" can be embedded in newsgroup messages or in messages received by Internet Mail as shortcuts. A group of University of Maryland students demonstrated that a newly-discovered bug could let a hacker remotely break into a user's computer or install viruses onto the system.

Category 21.2 *Security product QA failures*

1997-03-13 **QA**

RISKS 18 90

MS-Office 97 internal formats are different from Office-95, causing problems for 3rd party utilities such as anti-virus scanners. Microsoft eventually provided utilities for older versions of its products to read files saved by newer versions.

Category 21.2 *Security product QA failures*

1997-03-20 **QA computers cannot lie**

RISKS 18 92

Bank of America in Santa Rosa, CA insisted that $37,000 deposit must be correct even though honest clients insisted they handed in only $3,700.

Category 21.2 *Security product QA failures*

1997-03-24 **QA**

RISKS 18 93

Lubbock County, Texas county computer program has thoroughly scrambled people and crimes; e.g., labeling people fined for not wearing seat belt as accused child molesters. Computer consultants insist that the criminal record "has complete data integrity."

Category 21.2 *Security product QA failures*

1997-03-27 **QA**

RISKS 18 94

The bank clearing system in the UK failed in the last week of March, leaving many people without credit for their salary. Coming just before the four-day Easter break, this problem left many people in difficulty over the long weekend.

Category 21.2 *Security product QA failures*

1997-03-29 **QA**

Seattle Post-Intelligencer

Sandoz Pharmaceutical Corp's automated check system cut a refund for $1.99 using the ZIP code as an amount: 98002. Barry Lyn Stoller stupidly cashed the check and disappeared with the $98,002. Found in March 1997, apparently derelict. Arrested for theft. In May, he pleaded guilty to theft. Moral: don't think that accounting errors can legitimately contribute money to your lifestyle.

Category 21.2 *Security product QA failures*

1997-03-31 **QA model**

RISKS 18 96

The Bank of Tokyo-Mitsubishi Bank Ltd. lost $83M because of a bad computer model; National Westminster Bank PLC lost $139M in a similar failure due to bad parameters in a financial model. These cases support the view that too many amateurs are creating complex mathematical models using easy-to-use spreadsheets and other tools but failing to create test suites that would point to problems in assumptions and initial values.

Category 21.2 *Security product QA failures*

1997-04-17 **QA storage capacity**

RISKS, PA News 19 9

Saturation of MSN's server disk drives led to a two-day shutdown of the entire MSN e-mail system, preventing 2.5 million people from receiving their mail from MSN (and an unknown percentage with access only to MSN from sending e-mail). Of course, any of the affected people could have signed up to AOL for a practically unlimited time just by using one after another of the millions of AOL "FREE" diskettes we have all received. Tell me: has anyone bothered to buy any diskettes lately or are we all using reformatted AOL disks?

Category 21.2 *Security product QA failures*

1997-04-17 **QA**

RISKS 19 9

Another victim of the infamous Bre-X fraud was the Toronto Stock Exchange, where unprecedented volume of trading in the stock resulted in buffer overflows and multiple system crashes because of two 20-year-old bugs that had gone unnoticed. Moral: remember to include volume and stress tests in your quality assurance suites.

Category 21.2 *Security product QA failures*

1997-04-28 **QA**

RISKS 19 11

The Microsoft spell-check software that comes with Office 95 suggests an interesting correction for the string "zzzz." It recommends "sex."

Category 21.2 *Security product QA failures*

1997-05-02 **DNS denial of service QA internet domain names**

RISKS 19 12

When MAI Network Services of McLean, VA provided Internet backbone operators with incorrect routing tables on 97.04.23, large portions of the Internet went dead for 20 minutes to three hours. The corrupt tables also flooded MAI servers and, by inadvertence, an innocent ISP as well, FL Internet Exchange.

Category 21.2 *Security product QA failures*

1997-05-09 **QA Pentium hardware**

RISKS 19 13

According to an article in an electrical engineering journal, some cheap Pentium motherboards will fail quickly because of the poor quality and number of capacitors used to smooth out the power to the CPU chip. Spikes delivered to the processor could account for mysterious lockups and erratic behavior.

Category 21.2 *Security product QA failures*

1997-05-09 **privacy database QA**

RISKS 19 14

The Kansas Sex-Offender Database that was published on the Web in May is full of egregious and irresponsible errors. In one county, 14 of the 16 addresses listed as residences of convicted sex offenders were wrong. The sex offenders had moved. No one bothered to check the correctness of the addresses listed, with the result that innocent people were already being harassed for being on the list. Makes you wish one of the bureaucrats responsible for the list had rented a dwelling where a pervert used to live. . . .

Category 21.2 *Security product QA failures*

1997-05-09 **QA crypto**

RISKS 19 13

A bank decided to make mutual fund information available to its customers on a Web site. To secure access to a member's portfolio, the SSL code generated a unique 40-bit session key for each session. Unfortunately, the session key was foolishly constructed using the IP address as part of the value. When many employees from a single Internet site visited their portfolio, they ended up forcing the session keys to recycle within 40 minutes, resulting in access to an earlier inquirer's portfolio when an innocent later inquirer visited the site. Moral: don't make assumptions about sources of randomness and uniqueness. Birthdays are not unique. IP addresses are not unique. People's full names are not unique. Cartesian products of variables that don't have mutually exclusive values are not unique.

Category 21.2 *Security product QA failures*

1997-05-15 **QA Pentium bug hardware**

RISKS 19 15

The floating-point arithmetic on Pentium II and Pentium Pro chips was reported as bad. See <http://www.x86.org/secrets/Dan0411.html> for details.

Category 21.2 *Security product QA failures*

1997-06-12 **QA accounting**

RISKS 19 22

Jim Griffith summarized yet another huge accounting error: >CNNfn reports that a computer glitch at Smith Barney caused half a million customer accounts to be credited with $19 million each for a brief period Wednesday night. Company representatives claim that customers did not have access to the money, and that the balances were only visible to Smith Barney brokers and any customers who happened to look at their account balances via the Internet during the brief period that the problem exists. The problem was reportedly quickly noticed and fixed.

$19 million x 525,000 accounts = 9,975,000,000,000. That's $9.975 trillion, folks. Methinks someone misplaced the national debt by mistake...<

Category 21.2 *Security product QA failures*

1997-06-26 **QA interface**

RISKS 19 23

Michael Passer reported that Ctrl-Enter, which normally introduces a page break in MS-Word 97 and other word-processing packages, is redefined without warning when using Word as the e-mail editor in MS-Outlook: it sends the e-mail message at once. Bad form: changing the meaning of common keystrokes _in the same program_ as a function of context is not cool, even when the keystroke redefinition is quietly noted on the File pull-down menu.

Category 21.2 *Security product QA failures*

1997-07-16 **QA hardware calculation**

RISKS 19 24

A RISKS correspondent found that the newest revision of the DEC ALPHA motherboard has a defective pow() function. "Try 'pow(1.234567, 7.654321)'. If you don't get 5.017something, you have the same problem."

Category 21.2 *Security product QA failures*

1997-07-16 **QA spreadsheets**

RISKS 19 24

Research on production spreadsheets reveals that in 300 files tested and in experiments with more than 1000 users, many spreadsheets contained serious errors. See <http://panko.cba.hawaii.edu/ssr/Mypapers/whatknow.htm> for a summary of findings of many independent studies showing cell-wise and sheet-wise error rates. For example, a study by ". . .Coopers and Lybrand in London. . . reported . . . that over 90% of all spreadsheets with more than 150 rows contained at least one significant formula mistake."

Category 21.2 *Security product QA failures*

1997-07-18 **DSN QA**

RISKS 19 25

On 97.07.17, reported Daniel Pouzzner, the .com and .net domains disappeared from the DNS due to propagation of corrupt namerserver databases. Peter G. Neumann added, "[The problem apparently began around 11:30pm 16 Jul EDT, during the autogeneration of the NSI top-level domain zone files, and resulted from the failure of a program converting Ingres data into the DNS tables, corrupting the .COM and .NET files. Quality-assurance alarms were evidently ignored and the corrupted files were released at 2:30am EDT — with widespread effects. Other servers copied the corrupted files from the NSI version. Corrected files were issued four hours later, although there were still some lingering problems. . . .]

Category 21.2 *Security product QA failures*

1997-07-18 **Internet availability disaster backhoe fiber**

AP, Newsbytes, Reuter, Independent

On 1997.07.17 at 02:45 EDT, an operator at Network Solutions Inc. ignored alarms and released corrupted DNS table updates to the Net; as a result of the corruption, the entire .com and .net domains disappeared for half a day, disrupting worldwide access to e-mail and Web access in those sectors (mostly located in the United States and Canada). A few hours later, a backhoe operator sliced through a fiber-optic cable in Laurel, MD, near Washington, DC and shut down several phone trunks and elements of the Internet backbone, causing massive rerouting of Internet traffic and considerable congestion on the backup routes. The Net was back to normal by around 15:00 the same day. Members of the London Internet Exchange (LINKS) complained about what they described as inadequate accountability at Network Solutions.

Category 21.2 *Security product QA failures*

1997-07-26 **QA satellite porn**

RISKS 19 26

When a France Telecom operator inadvertently beamed 20 minutes of hard-core pornography into Saudi Arabia instead of general news, the scandal resulted in cancellation of the Saudi government's contract with the French service and a diplomatic flap whose repercussions lasted for weeks.

Category 21.2 *Security product QA failures*

1997-08-19 **QA harassment**

RISKS 19 31

According to reports from Britain, people are being harassed by auto-dialers on various machines such as vending machines, oil tanks, and even public toilets. The problem is that a single mis-typed phone number in the programming can cause hundreds of calls to innocent victims who cannot respond, don't know where the call is originating, and can't shut the calls off. About 8,000 people a month report such nuisance phone calls.

Category 21.2 *Security product QA failures*

1997-08-27 **PGP virtual memory pass phrase cache superzap QA quality assurance**

C|NET http://www.news.com/News/Item/0,4,13853,00.html

Australian Christopher Drake discovered that under Windows95, PGP 5.0 allows its passphrase to be stored in virtual memory. It is possible to recover the passphrase from at least five places on disk. The workaround: enable password caching with a small delay (e.g., a second).

Category 21.2 *Security product QA failures*

1997-08-29 **Netscape bug JavaScript**

Newsbytes

Netscape confirmed that Andre dos Santos of University of California at Santa Barbara correctly identified a problem with JavaScript in Navigator 4.01a and 4.02. Until the patches were installed, a user opening a second window at a rogue site might transmit confidential information through an insecure link.

Category 21.2 *Security product QA failures*

1997-09-13 **QA browsers**

San Jose Mercury News

Netscape technicians were embarrassed to find that their newly-enhanced Web site was a mess when viewed with the intended browsers: the latest versions of their own Communicator and Navigator software. Fancy features caused strings of error messages and did not work properly. Another investigation is being initiated to find out why it took the company a week to discover the blunder after it put up the defective pages.

Category 21.2 *Security product QA failures*

1997-09-17 **QA**

RISKS 19 39

Lauren Weinstein, editor of the Privacy Forum, noted a dangerous problem with the widely-used Quicken / Checkfree system for paperless banking. Seems that if a user forgets to update banking records before the (typically) 45-day period after which many banks delete online records of customer transactions, the program has no indication that the records have been removed. So from the point of the next (late) update, all the banking statements spit out by the Quicken / Checkfree programs are wrong. Moral: (1) Update your Quicken / Checkfree records frequently; (2) periodically verify your electronic statements against your paper statements.

Category 21.2 *Security product QA failures*

1997-09-17 **telco QA area code**

RISKS 19 38

A bug in the new software for DMS-100 central switches caused billing errors for 167,000 Californians who were billed for long distance calls instead of for local calls. The buggy software got confused by multi-area-code local calling areas.

Category 21.2 *Security product QA failures*

1997-09-17 **telecommunications denial of service disaster QA**

RISKS 19 39, 40

When a technician uploaded the wrong Routing and Translation tables to an AT&T SS7 switch, the entire 800-number service of AT&T went down for 90 minutes on 97.09.03. Robert Perillo, writing in RISKS, said that such tables should be verified offline before being installed; that an expert system should validate the tables; and that quality assurance requires pre-testing before installation on the production systems.

Category 21.2 *Security product QA failures*

1997-09-21 **QA**

RISKS 19 39

After Microsoft and PBS announced their collaboration to create Barney dolls that would interact with children under the instructions of an "ActiMates" transceiver synchronized with a new TV show, I suggested that there might be spinoffs: I can see it now: a new genre of horror movie in which animated figures controlled by TV shows take on a sinister glamour and throttle, eviscerate and otherwise harm infants while under the control of the TV set. This development will rejuvenate the Evil Dummy theme and give succor to all the mind-control freaks who already think that TV is a nefarious plot to damage the collective intelligence of the human race.

Come to think of it, they may have a point.

On a more practical note, think about the damage caused by dolls that ate their little owner's hair — and then think about _computer-controlled_ dolls — and then think about _hacked_ computer-control programs for little robots being cuddled by infants. Be afraid. Be very afraid.

Mua-ha-ha-ha. . . . [add reverb effect]

Category 21.2 *Security product QA failures*

1997-10-01 **QA**

RISKS 19 40

In Britain, over 800 students who had been accepted by universities were informed that they had lost their places because of "computer errors" in transmitting their A-level exam scores. Other students (number unknown) may have been initially refused because of the false scores sent to universities.

Category 21.2 *Security product QA failures*

1997-10-17 **QA**

RISKS 19 41

Bad Corsican drivers have not been charged with driving offences in Paris since 1990 because the Paris computer system rejected their postal code. The anomaly was detected only after manual verification of the records.

Category 21.2 *Security product QA failures*

1997-11-11 **QA hardware chips**

RISKS 19 45

Pentium and Pentium MMX chips were discovered to be susceptible to assembly-code that could halt them with a single instruction. Combined with an Internet Explorer flaw, it would be possible to append the fatal machine code to an excessively long URL to cause a Windows95 system to halt simply by attempting to link to a dangerous URL.

Category 21.2 *Security product QA failures*

1997-12-11 **QA spelling checker**

RISKS 19 50

Martin Bonner, writing in RISKS, contributed this case: >Cambridge City Council (England) wrote to a number of residents. Being careful people, they spell-checked the letter before sending it. The problem was that the spell checker couldn't see anything wrong with a letter that began "Dear Sir or Madman...".<

Category 21.2 *Security product QA failures*

1998-05-16 **encryption QA quality assurance ciphertext cleartext**

RISKS 19 74

The MS-Outlook 98 e-mail program was reported to behave counter-intuitively when a user attempted to cancel an encryption process on outbound e-mail. Instead of cancelling the encryption and returning to the READY state, the program cancelled the encryption but immediately mailed the unencrypted text. Furthermore, REPLYing to such an erroneously unencrypted message also disabled the automatic encryption that the recipient expects to use. All of this would occur without notification to the users, who could cheerfully assume that their correpondence was encrypted. See <http://www.wired.com/news/news/technology/story/12249.html>.

Category 21.2 *Security product QA failures*

1998-10-19 **antivirus product support amalgmation merger QA quality assurance**

Network World http://www.nwfusion.com/news/1019virus.html

Network Associates Inc., the megalithic company that has been gobbling up smaller firms in the last year or so, ran into trouble with its antivirus product customers. The company experienced serious problems with its servers, causing many customers to lose their connections during all-important downloads of update files for their virus-scanning software. In addition to problems apparently stemming from NAI's upgrade of server software, some of its antivirus programs didn't work with Windows98. The company experienced a massive rise in the number of calls to its support lines, with consequent long delays in reaching help.

Category 21.2 *Security product QA failures*

2000-01-09 **Web privacy programming error data leakage**

RISKS, AP, SecurityPortal, ZDNet 20 74
http://www.zdnet.com/zdnn/stories/newsbursts/0,7407,2419486,00.html

Northwest Airlines warned customers who placed orders on its Frequent Flier Web site that their transactions had been transmitted through the Net in the clear. Seems that Secure Sockets Layer (SSL) was not turned on again after system maintenance in mid-December. An observant customer noticed the unlocked lock symbol in his browser and alerted the company to the problem. No one knows if any credit card numbers or personal data were compromised.

Category 21.2 *Security product QA failures*

2000-02-21 **fraud separation of duties automatic processing QA quality assurance design liability**

RISKS 20 81

Banks in California announced that they would no longer honor requirements for dual-signature accounts. Claiming that automated recognition equipment could not handle dual signatures, the banks refused any liability for allowing unauthorized single-signature withdrawals. The banks thus put many organizations at risk of fraud, especially non-profit groups.

Category 21.2 *Security product QA failures*

2000-02-23 **Web software QA quality assurance failure password script**

RISKS 20 87

When a user entered an invalid request on the Palm Store (palmorder.modusmedia.com), he received an error message that included the system administrator password for the server involved.

Category 21.2 *Security product QA failures*

2000-03-19 **anti-piracy software QA quality assurance beta failure error bug reboot loop**

RISKS 20 85

Malcolm Park, writing in the RISKS Forum, reported on a quality assurance failure in the software for reading "free" books downloaded from the Internet. The only format that he was able to receive was the GlassBook, requiring a 7Mb free software download of the appropriate reader. Upon installing this reader, Park's Windows NT4 SP6a operating system went into an endless loop of reboots. By examining his NT partition for a good two hours, Park determined that the fault lay in the InterLok anti-piracy software. As he wrote, "My PC had been crippled by anti-piracy measures applied to a "free" software product I'd installed to read a "free" book. It is entirely feasible that others were locked out of their systems for good by this software." [Moral: before installing software, be sure you have the necessary recovery tools to reinstate a known-good version of the operating system.]

Category 21.2 *Security product QA failures*

2000-04-14 **QA quality assurance Trojan horse unauthorized code Easter egg vulnerability backdoor**

NewsScan, San Jose Mercury News 20 88
http://www.sjmercury.com/svtech/news/breaking/ap/docs/4267471.htm; RISKS

A three-year-old piece of Microsoft software includes a secret password that could be used to gain illegal access to hundreds of thousands of Web sites, including site management files that could lead to customers' credit card numbers. The code was discovered by two security experts who found within the code the following message: "Netscape engineers are weenies!" Microsoft is urging customers to delete the file, titled "dvwssr.dll," and plans to send out an e-mail bulletin and post a warning on its Web site describing the security hole. (AP/San Jose Mercury News 14 Apr 2000) However, Russ Cooper of Bugtraq wrote in RISKS, " the public has been overly warned against an extremely limited threat... while the real threat from the dvwssr.dll has been largely ignored by the media." Cooper explained that the more important issues were that (1) analysts were able to exploit the dll for buffer overflows; and (2) "While this particular program had minimal use in its lifetime, the fact that a static password (used for obfuscation, not entry) was even present should not be understated. This program has survived numerous Q&A cycles and, if we believe that source code for NT has been available at some 30+ U.S. Universities for years, numerous code reviews."

Category 21.2 *Security product QA failures*

2000-05-19 **antivirus false positives QA quality assurance**

RISKS 20 89

The Norton AntiVirus signature file dated 2000-05-18 caused many false positive identifications of the VBS.NewLove.A e-mail enabled worm.

Category 21.2 *Security product QA failures*

2000-05-25 **antivirus QA quality assurance confidentiality**

RISKS 20 89

A home-grown anti-virus scanner at a company accidentally converted all e-mail file access attributes to world-readable while it scanned in-boxes for suspect files. The breach of control was discovered only after about 10 days of vulnerability.

Category 21.2 *Security product QA failures*

2000-05-30 **antivirus quarantine QA quality assurance technical support**

RISKS 20 90

Richard Thieme, a regular contributor to the RISKS Forum, reported that Symantec's Systemworks 2000 Anti-Virus program reacted to the source code for the network.vbs worm by quarantining an entire Eudora Pro e-mail box where filters automatically stored incoming e-mail from a security list. That entire folder remained permanently inaccessible. When he finally reached a human being in technical support after hours of trying to get a meaningful response on how to recover the quarantined e-mail messages, he was told that no one had ever requested that particular function before. Given that the messages were not, in fact, infected, the anti-virus product actually caused harm instead of preventing it.

Category 21.2 *Security product QA failures*

2000-07-06 **QA quality assurance**

RISKS 20 94

CTS, the company that supplies automated barriers for access control to trains in Surrey, England, upgraded the software in June. Instead of improving the response speed, the newly programmed barriers erased the information on valid tickets, causing immense tie-ups for manual restitution to furious customers as well as for manual verification of unerased tickets. [Comment: how could any software firm test so poorly that such a drastic error could slip through quality assurance?]

Category 21.2 *Security product QA failures*

2000-07-18 **access control QA quality assurance design flaw danger emergency**

RISKS 20 95

The designers of subway access-control systems have justifiably introduced antipassback timers so that a magnetic ticket cannot be used immediately after someone has entered the restricted area of a station. However, Boyd Roberts reported to RISKS that the London Underground engineers foolishly introduced a timer for egress as well as ingress. Roberts wrote, "This is atrocious design" and pointed out that in an unmanned station, such restrictions on egress could be catastrophic in an emergency.

In a follow-up posting, Clive D. W. Feather explained that the barrier system is controllable by staff, who can analyze the situation and override any blockage. In addition, all Tube stations must be manned all the time, and if staff leave they are required by policy and procedure to disable the barriers.

Category 21.2 *Security product QA failures*

2000-08-25 **QA quality assurance encryption bug key escrow**

RISKS. PoliTech http://www.politechbot.com/p-00067.html, Wired http://www.wired.com/news/print/0,1294,16219,00.html 21 03

The popular PGP encryption and digital-signature software was shown to include a bug in the key escrow functions that allowed unauthorized access to improperly-encrypted ciphertext.

Category 21.2 *Security product QA failures*

2000-10-16 **access control software canonical passwords hard-coded cleartext crack**

RISKS 21 09

WinU software from Bardon was claimed to lock down computers using Windows; the company's Web site included a list of large customers using the software. Someone posted a list of hard-coded, cleartext canonical backdoor passwords ("emergency passwords") obtained from the executable files, thus at once rendering the product useless and indirectly helping to supply a list of companies ripe for attack.

Category 21.2 *Security product QA failures*

2000-12-03 **antivirus signature files QA quality assurance operating system crash**

RISKS 21 13

Peter G. Neumann wrote, "Windows 95, 98, and NT all seem to have crashed under McAfee virus definition file version 4.0.4102. It includes a driver that actually imitates the virus. Network Associates recommended starting in Safe Mode and disabling VirusScan's startup scan."

Category 21.2 *Security product QA failures*

2001-04-23 **hacker challenge firewall QA quality assurance promotion gimmick backfire failure penetration**

RISKS 21 36

Jay Anantharaman reported in RISKS on a hacker challenge gone wrong: "A team of computer hackers has gained 35,000 pounds for hacking into a computer system just twenty-four hours after the competition began. Argus Systems organised the competition -- to break into a Web server locked down using its security product called PitBull -- to promote its products and to coincide with the start of Infosec, the UK's premier computer security event. Undeniably, the stunt backfired and is an embarrassment for Argus Systems Group, as well for as security consultant firm Integralis and hardware vendor Fujitsu Siemens, which helped organise the stunt and have coordinated three similar competitions in the US and Germany without suffering setbacks."

Category 21.2 *Security product QA failures*

2001-04-29 **virus operations security production software infection QA quality assurance embarrassment**

RISKS 21 37

Dave Stringer-Calvert reported in RISKS that Microsoft security fixes were infected with FunLove virus upon release. "A virus infection of security fix files on Microsoft's partner and premier support Web sites has forced the software giant to suspend certain downloads for more than a fortnight. Microsoft issued an alert on Monday, which states that various Hotfix files on its Premier Support and Microsoft Gold Certified Partners Web sites are infected with the FunLove virus. A copy of the notice said Microsoft has stopped access 'in order to protect customers' to an unspecified number of files, and expects to be able to restore access later today [29 Apr 2001]. Customers were advised to contact their technical account manager in the interim."

Category 21.2 *Security product QA failures*

2001-06-13 **bug tracking database error QA quality assurance incorrect data corruption transcription dissemination validation validity integrity**

RISKS 21 49

Uwe Ohse was able to compare his original bug posting about a particular problem with the version of his report in the SecurityFocus Vulnerability Database; to his distaste, he "found a number of errors in the database entry. The vulnerability in question is a local one, not a remotely exploitable bug. The bug database got it exactly the other way round. The database entry states the bug exists in version 1.0, but not in 1.0.1 to .3. This is wrong - the bug exists in version 1.1.0 (i don't know about older versions). There are other minor incorrect information."

Category 21.2 *Security product QA failures*

2001-07-20 **password change programming design error rejection false negative logic**

RISKS 21 53

A RISKS correspondent reported on a flaw with general applicability for all security systems: don't change the rules on password composition when _receiving_ existing passwords.

Philip Bragg explained that the original password for a digital certificate allowed non-alphanumeric characters; however, after a software change, the Web site form that asks users to log on with their old (or new) passwords explicitly forbids non-alphanumeric characters in the input field. Interestingingly, entering a bad password leads to an error message, whereas entering the correct password leads to "a mostly blank and useless page." Mr Bragg notes, "If the system knows I am using the correct passphrase why won't it let me renew my certificate?"

Web designers take note.

Category 21.2 *Security product QA failures*

2002-01-04 **QA quality assurance bug date javascript display**

RISKS 21 85

William Colburn, writing in RISKS, noted an embarrassing date problem on the Web page showing McAfee virus alerts: the date was missing in the sentence, "This page current as of." With javascript enabled, the date shown was January 4, 1971. Worse still, it turned out that the 1971 date was pulled from his own computer, which had the wrong date set. Finally, he pointed out that the current date was inserted by javascript into a cached copy of the page, producing the risk that an old page with inaccurate information could mislead someone into thinking it was up to date.

Category 21.2 *Security product QA failures*

2002-01-20 **antivirus anti-malware flaw quality assurance QA denial-of-service DoS crash Windows patch**

Security Wire Digest 4 5

F-SECURE REPAIRS GLITCH
F-Secure last week fixed a problem in its Anti-Virus 5.30 that caused some Windows systems to crash. The flaw affects systems using Windows 9x/ME/NT/2000 and is caused by the way F-Secure Anti-Virus 5.30 deals with "certain combinations of strange or unusual characters." Though the problem affects very few customers, according to published reports, users who experience "occasional system crashes with complex and long hyperlinks, random blue screens on Microsoft Windows NT 4.0/2000 and false virus alarms" are encouraged to read the F-Secure advisory.
http://www.f-secure.com/support/top-issues/avwrks-top-issues-page_2002011000.shtml

---

Category 21.2 *Security product QA failures*

2002-03-10 **buffer overflows vulnerabilities ICAT CVE**

ICAT Metabase

The ICAT Metabase < http://icat.nist.gov/icat.cfm > for the Common Vulnerabilities and Exposures (CVE) database reported 240 vulnerabilities involving buffer overflows out of a total of 1241 for the period from 1 Jan 2001 to 10 Mar 2002. This represents about 19% of all vulnerabilities logged for that period. Overall, for the entire period since the CVE began recording vulnerabilities in 1995, buffer overflows are named in 737 of the 3677 vulnerabilities or about 20% of the total.

Category 21.2 *Security product QA failures*

2002-04-22 **privacy confidentiality design disclosure flaw QA quality assurance identity theft SSN**

RISKS 22 04

Ted Lee reported this astounding blunder in RISKS:

>I had reason to question the denial of a claim on our dental insurance. I called the appropriate 800 number and ended up choosing the menu item for their "automated services." The first thing they asked for was my subscriber identification number, which the voice then said "is usually your social security number." I punched it in. The voice repeated it back to me -- and then went on to spell out my name (yes, they had it correct; OK, no middle initials, but first and last name were fine) *and* give my birthdate. Need I say more?<

[MK adds: For those puzzled by the implications, this system allows anyone who has picked up a potential identity-theft victim's SSN and knows they do business with this insurance company to determine the victim's birthdate -- very helpful in developing the stolen identity.

MORAL: don't program automated systems to divulge confidential information unnecessarily.]

Category 21.2 *Security product QA failures*

2003-02-07 **Microsoft problematic patch pulled Windows NT XP uninstall**

NIPC/DHS

February 05, eSecurity Planet — Problematic Windows NT patch pulled.

Microsoft has pulled the security patch for Microsoft Security Bulletin MS02-071: Flaw in Windows WM_TIMER Message Handling Could Enable Privilege Elevation. The patch, which was first issued on December 11, actually introduces an error that may cause systems to fail. While the Slammer worm inflicted its damage on copies of Microsoft SQL Server 2000, the latest problem revolves around a security patch for Windows NT 4.0 systems. But it comes at a time when sysadmins are being scolded for not updating systems with the necessary patches in the first place. (The patch for Slammer has been around since July.) The security vulnerability was found in the WM_TIMER Message Handling in NT 4.0 and could enable privilege elevation. Patches for Windows 2000 and Windows XP were unaffected by the latest withdrawal, Microsoft said. In the updated advisory, Microsoft said it was investigating the cause of the problematic patch and promised to release an updated fix soon. The company urged Windows NT 4.0 administrators to uninstall the patch until a new fix is issued. This vulnerability has a severity rating of "Important". The updated advisory may be found on the Microsoft website:
http://www.microsoft.com/technet/treeview/default.asp?url=/t echnet/security/bulletin/MS02-071.asp

---

Category 21.2 *Security product QA failures*

2003-03-04 **new vulnerablility snort buffer overflow NIPC advisory execute arbitrary code**

NIPC/DHS

March 03, Department of Homeland Security, National Infrastructure Protection Center — NIPC Advisory 03-003: "Snort buffer overflow Vulnerability".

There is a buffer overflow in the Snort Remote Procedure Call normalization routines which can cause Snort to execute arbitrary code embedded within sniffed network packets. Depending upon the particular implementation of Snort this may give local and remote users almost complete control of a vulnerable machine. The vulnerability is enabled by default. Snort is a widely used Intrusion Detection System from Sourcefire. The affected Snort versions include all version of Snort from version 1.8 through current. Snort 1.9.1 has been released to resolve this issue. More information can be found on the Sourcefire website:
http://www.sourcefire.com/services/advisories/sa022503.html.

Category 21.2 *Security product QA failures*

2003-03-20 **new vulnerability Microsoft security bulletin ISA DNS Intruction Detection Filter denial-of-service**

NIPC/DHS

March 19, Microsoft — Microsoft Security Bulletin MS03-009: Flaw In ISA Server DNS Intrusion Detection Filter Can Cause Denial Of Service.

Microsoft Internet Security and Acceleration (ISA) Server 2000 contains the ability to apply application filters to incoming traffic. A flaw exists in the ISA Server DNS intrusion detection application filter, and results because the filter does not properly handle a specific type of request when scanning incoming DNS requests. An attacker could exploit the vulnerability by sending a specially formed request to an ISA Server computer that is publishing a DNS server, which could then result in a denial of service to the published DNS server. DNS requests arriving at the ISA Server would be stopped at the firewall, and not passed through to the internal DNS server. All other ISA Server functionality would be unaffected. By default, no DNS servers are published. DNS server publishing must be manually enabled. The vulnerability would not enable an attacker to gain any privileges on an affected ISA Server or the published DNS server or to compromise any cached content on the server. It is strictly a denial of service vulnerability. Microsoft has assigned a risk rating of "Moderate" to this vulnerability. A patch is available at the Microsoft website.

Category 21.2 *Security product QA failures*

2003-04-10 **new vulnerability Microsoft security bulletin Winsock ISA firewall flaw patch exploit fix**

NIPC/DHS

April 09, Microsoft — Microsoft Security Bulletin MS03-012: Flaw In Winsock Proxy Service And ISA Firewall.

There is a flaw in the Winsock Proxy service in Microsoft Proxy Server 2.0, and the Microsoft Firewall service in ISA Server 2000, that would allow an attacker on the internal network to send a specially crafted packet that would cause the server to stop responding to internal and external requests. Receipt of such a packet would cause CPU utilization on the server to reach 100%, and thus make the server unresponsive. The Winsock Proxy service and Microsoft Firewall service work with FTP, telnet, mail, news, Internet Relay Chat (IRC), or other client applications that are compatible with Windows Sockets (Winsock). These services allow these applications to perform as if they were directly connected to the Internet. They redirect the necessary communications functions to a Proxy Server 2.0 or ISA Server computer, thus establishing a communication path from the internal application to the Internet through it. Microsoft has assigned a risk rating of "Important" to this vulnerability. A patch is available at the Microsoft website.

Category 21.2 *Security product QA failures*

2003-04-18 **CERT CC advisory Snort IDS intrusion detection system new vulnerability exploit patch fix**

NIPC/DHS

April 17, CERT/CC — CERT Advisory CA-2003-13: Multiple Vulnerabilities in Snort Preprocessors.

The Snort intrusion detection system ships with a variety of preprocessor modules that allow the user to selectively include additional functionality. There are vulnerabilities in two of these modules. CORE Security Technologies has discovered a remotely exploitable heap overflow in the Snort "stream4" preprocessor module. To exploit this vulnerability, an attacker must disrupt the state tracking mechanism of the preprocessor module by sending a series of packets with crafted sequence numbers. This causes the module to bypass a check for buffer overflow attempts and allows the attacker to insert arbitrary code into the heap. This vulnerability affects Snort versions 1.8.x, 1.9.x, and 2.0 prior to RC1. Internet Security Systems has discovered a remotely exploitable buffer overflow in the Snort RPC preprocessor module. When the RPC decoder normalizes fragmented RPC records, it incorrectly checks the lengths of what is being normalized against the current packet size, leading to an overflow condition. The RPC preprocessor is enabled by default. This vulnerability affects Snort versions 1.8.x through 1.9.1 and version 2.0 Beta. Both issues are addressed in Snort version 2.0, which is available at the Snort website: http://www.snort.org/.

Category 21.2 *Security product QA failures*

2003-04-24 **patch fix slow Microsoft Windows XP security bulletin**

NIPC/DHS

April 24, IDG News Service — Microsoft fixing patch that can slow Windows XP.

Microsoft is revising a security patch for Windows XP systems with Service Pack 1 installed after customers complained that installing the patch slowed their systems down to a crawl. Removing the patch brings system speed back to normal. Originally released on April 16, Security Bulletin MS03-013 addressed a buffer overrun vulnerability in the Windows kernel, which manages core services for the operating system such as allocating processor time and memory, as well as error handling. Microsoft is working on a revised patch which will be re-issued when it has been completed and fully tested. Microsoft said that customers running Windows XP Service Pack 1 should still consider applying the flawed patch as protection until a new version is released. The revised bulletin is available at the Microsoft Website: http://www.microsoft.com/technet/treeview/default.asp?url=/t echnet/security/bulletin/MS03-013.asp.

Category 21.2 *Security product QA failures*

2003-05-08 **VPN vulnerabilities Cisco 3002 hardware client DoS Attack ICMP packets performance degradation**

NIPC/DHS

May 08, IDG News Service — Cisco reports VPN vulnerabilities.

Cisco on Wednesday warned customers of three vulnerabilities in its Cisco 3005, 3015, 3030, 3060 and 3080 VPN (virtual private network) Concentrators and the Cisco VPN 3002 Hardware Client. In one of the vulnerabilities, an interloper could access systems on a private network from a workstation on the public network without any form of authentication. Another vulnerability can be exploited to carry out a DOS attack on the VPN concentrator. In the third vulnerability a flood of malformed ICMP (Internet Control Message Protocol) packets could cause a performance degradation on the concentrator or cause it to restart. Workarounds and an upgrade are available on the Cisco Website: http://www.cisco.com/warp/public/707/cisco-sa-20030507-vpn3k.shtml

---

Category 21.2 *Security product QA failures*

2003-05-08 **microsoft security flaw intenret passport hackers consumer accounts vulnerability**

NewsScan; NIPC/DHS

MICROSOFT SCRAMBLES TO FIX SECURITY FLAW

Microsoft says it has fixed a security glitch in its Internet Passport service that left 200 million consumer accounts vulnerable to hackers. Product manager Adam Sohn said the flaw apparently had existed since at least September 2002, but investigators found no evidence that anyone had tried to exploit it before last month. The flaw was discovered by Pakistani researcher Muhammed Faisal Rauf Danka after hackers repeatedly hijacked Passport accounts belonging to him and a friend. Danka says it took him only about four minutes to find the problem. The embarrassing security lapse could leave Microsoft open to sanctions by the Federal Trade Commission, as well as a possible hefty fine. Under a settlement last summer, the government had accused Microsoft of deceptive claims about Passport's security, and in response the company had pledged to beef up its safeguards and submit to audits every two years for the next 20 years, or risk fines of up to $11,000 per violation. "If we were to find that they didn't take reasonable safeguards to protect the information, that could be an order violation," says an FTC official. Meanwhile, Microsoft is currently touting its "trustworthy computing initiative," which is intended to improve security for all its software products and services. (AP 8 May 2003)

May 08, Associated Press — Microsoft admits Passport was vulnerable.

Computer researcher Muhammad Faisal Rauf Danka of Pakistan discovered how to breach Microsoft Corp.'s security procedures for its Internet Passport service. The service is designed to protect customers visiting some retail Web sites, sending e-mails and in some cases making credit-card purchases. Microsoft acknowledged the flaw affected all its 200 million Passport accounts but said it fixed the problem early Thursday, after details were published on the Internet Wednesday night. Under a settlement with the Federal Trade Commission (FTC) last year over lapsed Passport security, Microsoft pledged to take reasonable safeguards to protect personal consumer information during the next two decades or risk fines up to $11,000 per violation. The FTC's Jessica Rich said Thursday that each vulnerable account could constitute a separate violation - raising the maximum fine that could be assessed against Microsoft to $2.2 trillion.

Category 21.2 *Security product QA failures*

2003-05-13 **security flaws virtual machines random bit change cosmic rays IEEE physical access**

NewsScan

May 13, CNET News — Security flaws exposed in virtual machines. Princeton University student Sudhakar Govindavajhala has found security flaws in Java and .Net virtual machines. The technique relies on the ability of energy to "flip bits" in memory. While cosmic rays can very occasionally cause a random bit in memory to change value, from 0 to 1 or from 1 to 0, Govindavajhala decided not to wait. He used a lamp to heat up the chips inside a computer and cause one or more bits of memory to change. By doing so, the researcher broke the security model that virtual machine's rely on—that the computer faithfully executes its instruction set. An attack requires physical access to the computer, so the technique poses little threat to virtual machines running on PCs and servers. But it could be used to steal data from smart cards, Govindavajhala said Tuesday at the Institute of Electrical and Electronic Engineers (IEEE) Symposium on Security and Privacy in Berkeley, CA. He also pointed out that as processors and memory get faster, the energy needed to induce bit flips becomes smaller, suggesting that his technique will only become more effective.

Category 21.2 *Security product QA failures*

2003-06-25 **Symantec Security Check activeX control holes buggy code attack operating system**

NIPC/DHS

June 25, IDG News Service — Serious security holes, buggy code found in Symantec products.

On Monday, anti-virus software company Symantec acknowledged a report about a serious security flaw in Symantec Security Check, an online service that enables users to scan their computer's vulnerability to a number of security threats. An ActiveX control installed by the Security Check service contains a buffer overflow vulnerability that could enable a remote attacker to crash or run malicious code on systems that had the control installed. Symantec updated the ActiveX control in the Security Check service, but security researchers monitoring the issue noted attackers who have a copy of the flawed ActiveX code with a valid Symantec digital signature could trick a Microsoft Windows system into accepting the control, opening that system to attack. Also on Monday customers using Symantec AntiVirus Corporate Edition reported that an automated anti-virus definition update from the company caused the anti-virus software to fail. Symantec subsequently provided instructions on how to repair systems that had downloaded the faulty update.

Category 21.2 *Security product QA failures*

2003-10-20 **Windows security problems fix Microsoft operating systems vulnerabilities**

NewsScan

MICROSOFT VOWS TO FIX WINDOWS SECURITY PROBLEMS

Microsoft CEO Steve Ballmer has admitted the inadequacy the company's current collection of security software patches for the Windows operating system and says the company will modify them in the coming year. Customers have complained that the company's system of frequently issuing new patches is too time-consuming and difficult, so Microsoft is now designing technology to shield Windows from malicious e-mail messages, viruses and worms. The changes will include shipping Windows with an Internet firewall turned on by default, which would have blocked the recent "Blaster" virus, and will prevent attachments from executing commands — a common method network vandals use to hijack computers. (San Jose Mercury News 10 Oct 2003)

Category 21.2 *Security product QA failures*

2003-10-23 **revisions Microsoft Security Bulletin MS03-047 045 Outlook Web Access OWA language versions patches exchange third-party software**

NIPC/DHS

October 23, Computerworld — Microsoft posts 'revisions' to security bulletins.

Microsoft issued "major revisions" to two patches last week, MS03-045 and MS03-047, after they caused problems on foreign language versions of the Windows operating system and Exchange e-mail server. Security bulletin MS03-045, rated "Important," concerns a buffer overrun vulnerability in a component of most supported versions of Windows. Microsoft discovered compatibility problems between the patch and third-party software on systems running foreign language editions of Windows 2000 with Service Pack 4. Russian, Spanish and Italian versions of Windows 2000 were affected, in addition to versions in a number of other languages, including Czech, Finnish and Turkish. Security bulletin MS03-047, rated "Moderate," described a cross-site scripting vulnerability in Exchange Server 5.5, Service Pack 4. The patch did not work for some customers who installed foreign language versions of Outlook Web Access (OWA), an Exchange service that enables e-mail users to access their Exchange mailboxes using a Web browser instead of the Outlook mail client. While customers running English, German, French and Japanese versions of OWA were covered by the original patch, those running OWA in other languages need to apply the rereleased version, Microsoft said. The patches are available on the Microsoft Website: http://www.microsoft.com/technet/treeview/default.asp?url=/t echnet/security/current.asp

---

Category 21.2 *Security product QA failures*

2003-11-03 **security patch fix exploit vulnerability Microsoft buffer overflow Messenger Service**

NIPC/DHS

October 30, eSecurity Planet — Microsoft revises critical patches.

Microsoft has issued major revisions to several 'critical' security patches because of problems associated with Debug Programs. The "major revisions" issued on October 30 have been released to correct problems in the MS03-042, MS03-043, and MS03-045 patches. The MS03-042 patch, which plugs a 'critical' buffer overflow issue in the Windows Troubleshooter ActiveX Control, has been re-issued because of problems related to CPU resource usage. The Debug Problems afflict all three faulty patches—MS03-043, which is a buffer overrun in Messenger Service that could lead to code execution and MS03-044, which could allow PC takeover because of buffer overflows in the ListBox and ComboBox Control. Additional information is available on the Microsoft Website:
http://www.microsoft.com/technet/treeview/default.asp?url=/t echnet/security/bulletin/winoct03.asp

---

Category 21.2 *Security product QA failures*

2003-11-03 **digital signature forgery naïve security**

RISKS 23 1

Duh! An electronic signature!

Prof. Geoff Kuenning was recommending a student to the Hertz Foundation, and had to sign his reference electronically. The "digital signature" was collected on a Webpage as:

I certify that I am the person named below:
(type name in box)

Given the lack of security in this method of collecting a digital signature, Prof. Kuenning suggests having an additional checkbox in the recommendation form labeled, "This recommendation is forged."

Category 21.2 *Security product QA failures*

2003-12-23 **fix patch vulnerability flaw buffer overflow Internet Explorer browser software third-party Microsoft**

NIPC/DHS

December 22, CNET News.com — New open-source patch released for IE. A Website that published a third-party patch to fix a security hole in Microsoft's Internet Explorer (IE) has had to re-issue the patch Saturday, December 20, after the original was found to contain a buffer overflow exploit. This exploit, which allowed an attacker to take control of the patched PC, might have been far more damaging than the flaw that the patch was trying to fix. According to Openwares, only about 6,500 people downloaded the original patch. Security experts warned people against installing it last week, saying that aside from trust issues, the patch author would not have had access to IE source code and so the patch could interfere with future updates from Microsoft. The IE vulnerability, which was first reported in late November, allows a browser to display one URL in the address bar while the page being viewed is actually hosted elsewhere, making the user more susceptible to ruses like "phishing." However, Openwares' first fix, which worked by filtering out any URLs containing suspicious characters, would work only with addresses that had less than 256 bytes. Larger addresses produced a buffer overflow. Microsoft has still not released a fix for the IE problem or given any indication as to when one might be available.

Category 21.2 *Security product QA failures*

2004-01-09 **password protection MS Word document bug failure weakness flaw**

RISKS; 23 12
http://news.zdnet.co.uk/software/windows/0,39020396,39118935,00.htm=20

'UNFIXABLE' WORD PASSWORD HOLE EXPOSED

Brett McCarron reports as follows:

The password used to "protect" a Microsoft Word form can be revealed with a simple text editor, according to a recent BugTraq article. The RISK in this case goes beyond the ability to edit a protected document (you can bypass this anyway with Edit > Select All > Copy, open a new document and Paste). The real RISK is that the user's password is so easy to discover. Ideally, users would protect a form with a password that is different from their network authentication password(s). But in the real word …

News Story
http://news.zdnet.co.uk/software/windows/0,39020396,39118935,00.htm=20

BugTraq Article
http://www.securityfocus.com/archive/1/348692/2004-01-02/2004-01-08/0

Category 21.2 *Security product QA failures*

2004-01-14 **Microsoft security bulletin patch flaw vulnerability fix**

NIPC/DHS;
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS04−001.asp

January 13, Microsoft — Microsoft Security Bulletin MS04-001: Vulnerability in Microsoft Internet Security and Acceleration Server 2000 H.323 Filter Can Allow Remote Code Execution.

A security vulnerability exists in the H.323 filter for Microsoft Internet Security and Acceleration Server 2000 that could allow an attacker to overflow a buffer in the Microsoft Firewall Service in Microsoft Internet Security and Acceleration Server 2000. An attacker who successfully exploited this vulnerability could try to run code of their choice in the security context of the Microsoft Firewall Service. This would give the attacker complete control over the system. The H.323 filter is enabled by default on servers running ISA Server 2000 computers that are installed in integrated or firewall mode. ISA Servers running in cache mode are not vulnerable because the Microsoft Firewall Service is disabled by default. Users can prevent the risk of attack by disabling the H.323 filter. Microsoft has assigned a severity rating of "Critical" to this issue.

Category 21.2 *Security product QA failures*

2004-01-28 **US-CERT CERT warning forget operating system OS worm vulnerability**

RISKS 23 15

US-CERT WARNS OF WORM, FORGETS TO MENTION OPERATING SYSTEM

Contributor Kevin Dalley reports that US-CERT published a warning about the MyDoom.B worm but forgot to mention explicitly what the susceptible operating system was: http://www.us-cert.gov/cas/techalerts/TA04-028A.html CERT issued a warning for the Novarg.A worm, titled "Steps for Recovering from a UNIX or NT System Compromise." With warning, says Dalley, at least "one could assume that UNIX is at risk." Dalley finishes: "Chew on these CERTs and you will be lucky to see a spark of light."

Category 21.2 *Security product QA failures*

2004-02-05 **firewalls proxy HTTP request check point Application Intelligence AI update issued**

DHS IAIP Daily; http://www.us−cert.gov/cas/techalerts/TA04−036A.html

February 05, US-CERT — Technical Cyber Security Alert TA04-036A: HTTP Parsing Vulnerabilities in Check Point Firewall-1.

The Application Intelligence (AI) component of Check Point Firewall-1 is an application proxy that scans traffic for application layer attacks once it has passed through the firewall at the network level. Both the AI and HTTP Security Server features contain an HTTP parsing vulnerability that is triggered by sending an invalid HTTP request through the firewall. When Firewall-1 generates an error message in response to the invalid request, a portion of the input supplied by the attacker is included in the format string for a call to sprintf(). It is possible to exploit this format string vulnerability to execute commands on the firewall. This vulnerability can be exploited as a heap overflow, which would allow an attacker to execute arbitrary code. In either case, the commands or code executed by the attacker would run with administrative privileges, typically "SYSTEM" or "root". Additional information and a patch are available on the Check Point Website: http://www.checkpoint.com/techsupport/alerts/security_server .html

---

Category 21.2 *Security product QA failures*

2004-02-05 **VPN ISS firewalls proxy HTTP request check point Application Intelligence AI update issued**

DHS IAIP Daily;
http://www.crn.com/sections/BreakingNews/dailyarchives.asp?A rticleID=47735

February 05, TechWeb — Security flaws found in popular firewall software.

Flaws found late Wednesday in Check Point Software's popular firewall and VPN software could allow an attacker to gain entrance to enterprise networks, Internet Security Systems (ISS) said in a critical alert. The disclosure of the vulnerabilities is yet another sign of a move by hackers to hammer at security software, firewalls, and intrusion detection systems, the very devices and applications enterprises rely on to defend themselves against intruders, said Dan Ingevaldson, the director of ISS's X-Force research team. The first vulnerability is within Check Point Firewall-1, and stems from the HTTP Application Intelligence that's designed to prevent potential attacks or detect protocol anomalies aimed at servers behind the firewall. The flaw also exists in the HTTP Security Server applications proxy that ships with all versions of Firewall-1, including the most recent. On Wednesday, Check Point posted a patch for this vulnerability that it recommended be installed immediately. The second vulnerability lies within Check Point VPN-1 Server and its virtual private networking (VPN) clients, Securemote and SecureClient. The vulnerability exists in the ISAKMP processing in both the server and clients, and if exploited, could result in an attacker gaining access to any client-enabled remote computer, including those in employees' homes.

Category 21.2 *Security product QA failures*

2004-03-02 **security vulnerability flaw hole fix patch Dell OpenManage server HTTP POST**

DHS IAIP Daily;
http://www.techworld.com/news/index.cfm?fuseaction=displaynews&NewsID=1115

February 27, Techworld — Critical security hole in Dell OpenManage.

A security hole in Dell OpenManage server could leave the product open to attack by an unauthorized user. The problem has been identified as high risk by security consultancy Secunia. The vulnerability is caused due to a boundary error in the Web server when handling certain HTTP POST requests. POST is an extremely common HTML method of processing forms but can be exploited by sending a message with a hidden but extremely long variable to cause a heap overflow. The vulnerability can be side-stepped by restricting access to Port 1311/TCP and only allowing trusted IP addresses to connect. However, without that in place, a denial of service or system access are readily achievable. Additional information is available on the Secunia Website: http://secunia.com/advisories/10994/

Category 21.2 *Security product QA failures*

2004-03-22 **security vulnerability flaw hole patch fix Norton Internet software**

DHS IAIP Daily;

March 19, CNET News.com — Flaw stymies Norton Internet Security.

A software component of Norton Internet Security could allow hackers to use the application as a backdoor into a person's computer system, security researchers warned Friday, March 19. The flaw occurs in an ActiveX component used by security firm Symantec's desktop security program, Norton Internet Security, according to research firm NGSSoftware. The security hole could be used to run an attack program that would then take control of the computer that the software was trying to protect. "The attack can be achieved either by encouraging the victim to visit a malicious Web page or placing a script within...an HTML e-mail," the advisory stated. Symantec's Antispam software has a similar issue caused by a different ActiveX component. Fixes for the flaws can be downloaded using Symantec's LiveUpdate.

Category 21.2 *Security product QA failures*

2004-04-06 **software flaw hole vulnerability F-secure patch fix hackers anti-virus rooting owning**

DHS IAIP Daily; http://www.vnunet.com/News/1154100

April 06, vnunet.com (UK) — F-Secure warns on software flaw.

Security vendor F-Secure is urging users to patch their systems after the discovery of two flaws in a version of its anti-virus software that leaves users vulnerable to hackers and virus writers. The first flaw could give hackers complete access to a target PC through a hole that affects F-Secure BackWeb 6.31 and earlier versions. This makes the company's anti-virus, BackWeb and policy management software vulnerable. The second problem is in versions 5.41 and 5.42 of F-Secure's Anti-Virus for MIMEsweeper product. It allows the Sober D worm, which is sent in email-attached Zip files, to bypass the antivirus software and infect PCs. Additional information and a patch available here:
http://secunia.com/advisories/11297/4/2004

Category 21.2 *Security product QA failures*

2004-04-22 **software vulnerabilities Symantec security products testing**

NewsScan

FLAWS FOUND IN SYMANTEC PRODUCTS

The security firm eEye Digital Security has discovered four more critical vulnerabilities in three Symantec products and released basic details about them in its upcoming advisory section, where it maintains a list of flaws its researchers have found in software. As part of its policy of informing the public of upcoming security advisories, eEye normally informs the vendor and then waits for a patch before issuing full details of the flaw in question. The newly reported flaws could result in the execution of remote code. (The Age 22 Apr 2004)

Category 21.2 Security product QA failures

2004-05-12 **vulnerability Symantec DNS NetBIOS**

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1591455,00.asp

May 12, eWEEK — Multiple vulnerabilities found in Symantec client products.

Symantec has acknowledged several serious bugs in several of its client security products in both corporate and consumer editions. The problems involve several functions of the products but one specific file, SYMDNS.SYS. Fixes for all of the problems are available through Symantec's LiveUpdate and technical-support channels. Products affected include Symantec Client Firewall versions 5.0.0 through 5.1.1; Symantec Client Security 1.0.0, 1.1.0 and 2.0.0; Norton AntiSpam 2004; Norton Internet Security 2002 through 2004; and Norton Internet Security Professional Edition 2002 through 2004. DNS response is one of the functions listed as having such an error. A malicious response to a DNS request could cause the program to fail or alter the flow of the program. There are also errors in the processing of NetBIOS Name Service responses that could allow remote code execution or denial of service. Since NetBIOS is not a routable protocol, such attacks would have to come from within a network segment. Additional information is available on the Symantec Website: http://securityresponse.symantec.com/avcenter/security/Conte nt/2004.05.12.html

---

Category 21.2 Security product QA failures

2004-08-03 **Juniper Network NetScreen firewall vulnerability SSHv1 denial of service**

DHS IAIP Daily; http://www.juniper.net/support/security/alerts/screenos−sshv 1 −2.txt

August 03, Juniper Networks — NetScreen DoS Advisory.

The Juniper Networks NetScreen firewall SSHv1 service implementation has a bug which allows an attacker to crash ScreenOS. A malicious person who can connect to the SSHv1 service on a Juniper Networks Netscreen firewall can crash the device before having to authenticate. Upon execution of the attack, the firewall will reboot or hang, which will prevent traffic to flow through the device. Juniper Networks currently has updated versions of ScreenOS available for immediate download.

Category 21.2 Security product QA failures

2004-08-10 **Symantec Clientless VPN Gateway vulnerabilities ActiveX browser hotfix available**

DHS IAIP Daily; http://secunia.com/advisories/12254/

August 10, Secunia — Symantec Clientless VPN Gateway 4400 Series multiple vulnerabilities.

Multiple vulnerabilities have been reported in Symantec Clientless VPN Gateway 4400 Series, where some have an unknown impact and others can be exploited to conduct cross-site scripting attacks or manipulate users' signon information: 1) Various unspecified vulnerabilities affect the ActiveX and HTML file browsers; 2) Various unspecified input validation errors within the end user UI can be exploited to conduct cross-site scripting attacks; 3) An error within the end user UI can be exploited by malicious users to manipulate other users' signon information (including username and password). A hotfix is available from Symantec: ftp://ftp.symantec.com/public/en…_5/updates/SCVG5-20040806-00.tgz

---

Category 21.2 Security product QA failures

2004-08-25 **Cisco Secure Access Control Server ACS vulnerabilities update issued**

DHS IAIP Daily; http://www.cisco.com/warp/public/707/cisco−sa−20040825− acs.s html

August 25, Cisco Security Advisory — Multiple vulnerabilities in Cisco Secure Access Control Server.

Multiple vulnerabilities exist in Cisco's Secure Access Control Server (ACS) that may cause a crash impacting the availability of services on the ACS devices. The device must be rebooted to resolve this Denial of Service. Other vulnerabilities associated with this advisory may allow unauthenticated users to gain access to the ACS Administration GUI. Updates are available from the vendor at the Source link.

Category 21.2 *Security product QA failures*

2004-10-05 **Symantec Norton Anti-Virus MS DOS device name scan failure update issued**

DHS IAIP Daily; http://securityresponse.symantec.com/avcenter/security/Content/2004.10.05.html

October 05, Symantec — Symantec Norton Anti-Virus fails to scan files named with MS DOS device names.

Symantec Norton AntiVirus consumer products do not effectively scan files with MS-DOS reserved device names once the file is resident on a user's system. A remote user can create a file that will not be detected by the application. The vendor has issued a fix for Symantec Norton Anti-Virus 2004, available via LiveUpdate. Fixes for other supported versions will be available through LiveUpdate at a later date.

Category 21.2 *Security product QA failures*

2004-10-18 **software anti-virus detection evasion vulnerability**

DHS IAIP Daily; http://www.idefense.com/application/poi/display?id=153&type=vulnerabilities&flashstatus=true

October 18, iDEFENSE — Multiple vendor anti-virus software detection evasion vulnerability.

Remote exploitation of an exceptional condition error in multiple vendors' anti-virus software allows attackers to bypass security protections by evading virus detection. The problem specifically exists in the parsing of .zip archive headers. This vulnerability affects multiple anti-virus vendors including McAfee, Computer Associates, Kaspersky, Sophos, Eset and RAV. See iDEFENSE Advisory in Source link for vendor fixes.

Category 21.2 *Security product QA failures*

2004-11-03 **F-secure antivirus Microsoft Exchange mail server ZIP archive malicious code update issued**

DHS IAIP Daily; http://securitytracker.com/alerts/2004/Nov/1012057.html

November 03, SecurityTracker — F-Secure Anti-Virus for Microsoft Exchange vulnerability.

A vulnerability was reported in F-Secure Anti-Virus for Microsoft Exchange which could allow a remote user to can send malicious code within a ZIP archive that will pass through the anti-virus function without detection. The vendor reported that some password protected files are not detected inside a ZIP archive. The vendor has released F-Secure Anti-Virus for Microsoft Exchange 6.3x Hotfix 2, available at: ftp://ftp.f-secure.com/support/hotfix/fsav-mse/fsavmse63x-02.zip

---

Category 21.2 *Security product QA failures*

2004-12-15 **Adobe Acrobat Reader buffer overflow vulnerability code execution attack update issued**

DHS IAIP Daily; http://secunia.com/advisories/13474/

December 15, Secunia — Adobe Acrobat Reader "mailListIsPdf()" function buffer overflow.

A vulnerability has been reported in Adobe Acrobat Reader 5.0.9 for Unix, which can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to a boundary error in the "mailListIsPdf()" function when checking input files. This can be exploited to cause a buffer overflow by sending an e-mail with a malicious PDF document attached or a link to one. Successful exploitation allows execution of arbitrary code. Update to version 5.0.10 for Unix: http://www.adobe.com/products/acrobat/readstep2.html

---

Category 21.2 *Security product QA failures*

2004-12-15 **Ethereal network sniffer software vulnerabilities denial of service DoS**

DHS IAIP Daily; http://secunia.com/advisories/13471/

December 15, Secunia — Ethereal multiple vulnerabilities.

Multiple vulnerabilities exist which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a vulnerable system including execution of arbitrary code. Vulnerabilities include errors within the DICOM dissector, the handling of RTP timestamps, the HTTP dissector, and the SMB dissector. Update to version 0.10.8: http://www.ethereal.com/download.html

---

Category 21.2 *Security product QA failures*

2004-12-21 **Kerberos V5 authentication software open source buffer overflow vulnerability update issued**

DHS IAIP Daily; http://secunia.com/advisories/13592

December 21, Secunia — Kerberos V5 "libkadm5srv" buffer overflow vulnerability.

A vulnerability has been reported in Kerberos V5, which potentially can be exploited by malicious users to compromise a vulnerable system. The vulnerability is caused due to a boundary error in the libkadm5srv administration library within the "add_to_history()" function during the password history handling. This can be exploited to cause a heap-based buffer overflow when a principal changes the password and has a certain password history state. The vulnerability is fixed in version 1.4-beta3. The vulnerability will reportedly be fixed in the upcoming krb5-1.4 release and krb5-1.3.6 patch release. Apply patch for version 1.3.5: http://web.mit.edu/kerberos/advisories/2004-004-patch_1.3.5. txt

---

Category 21.2 *Security product QA failures*

2005-01-11 **mpg123 Motion Pictures Experts Group MPEG layer-2 buffer overflow vulnerability code execution attack no update issued**

DHS IAIP Daily; http://secunia.com/advisories/13779/

MPG123 MPEG LAYER-2 BUFFER OVERFLOW VULNERABILITY

A vulnerability has been reported in mpg123, which potentially can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to an error in the parsing of frame headers for layer-2 streams. This may be exploited to cause a heap-based buffer overflow via a specially crafted MP2 or MP3 file. Successful exploitation may allow execution of arbitrary code with the privileges of the user executing mpg123. There is no solution at this time.

Category 21.2 *Security product QA failures*

2005-01-12 **Apple iTunes playlist handling buffer overflow vulnerability code execution attack**

DHS IAIP Daily; http://secunia.com/advisories/13804/

SECUNIA ADVISORY SA13804: APPLE ITUNES PLAYLIST HANDLING BUFFER OVERFLOW VULNERABILITY

A vulnerability in iTunes can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to a boundary error within the handling of .m3u and .pls playlists. This can be exploited to cause a buffer overflow via a specially crafted playlist. Successful exploitation may allow execution of arbitrary code.

Category 21.2 *Security product QA failures*

2005-01-17 **VMWare operating system emulator ESX server sensitive information disclosure vulnerability update issued**

DHS IAIP Daily; http://secunia.com/advisories/13871/

VMWARE ESX SERVER THREE VULNERABILITIES

VMware has acknowledged some vulnerabilities in ESX Server, which can be exploited to disclose sensitive information in kernel memory, bypass certain security restrictions, and potentially compromise a vulnerable system. Update to version 2.5 or apply security update available at: http://www.vmware.com/download/esx/

Category 21.2 *Security product QA failures*

2005-01-17 **MySQL script vulnerability privilege escalation attack update issued**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2005/Jan/1012914.html

MYSQL 'MYSQLACCESS.SH' UNSAFE TEMPORARY FILES MAY LET LOCAL USERS GAIN ELEVATED PRIVILEGES

A vulnerability was reported in MySQL in the 'mysqlaccess.sh' script. A local user may be able to obtain elevated privileges. Mmysqlaccess.sh, creates temporary files in an unsafe manner. A local user can create a symbolic link (symlink) from a critical file on the system to a temporary file to be used by the script. Then, when the script is executed, the sym-linked file may be modified with the privileges of the script. A fix is available via Bitkeeper at: http://lists.mysql.com/internals/20600

Category 21.2 *Security product QA failures*

2005-01-17 **BlackBerry Enterprise Server denial of service DoS vulnerability Wireless Markup Language WML update issued**

DHS IAIP Daily; http://secunia.com/advisories/13861/

BLACKBERRY ENTERPRISE SERVER MOBILE DATA SERVICE DENIAL OF SERVICE.

A vulnerability has been reported in BlackBerry Enterprise Server, which can be exploited by malicious people to cause a DoS (Denial of Service). The vulnerability is caused due to an error in the Mobile Data Service when processing WML (Wireless Markup Language) pages and can be exploited by tricking a user into viewing a malicious WML page containing an URL without space characters in the comment block. The vulnerability has been fixed in the following versions: BlackBerry Enterprise Server for Domino 2.2 Service Pack 4 Hot Fix 2 and BlackBerry Enterprise Server for Microsoft Exchange 3.6 Service Pack 4 Hot Fix 2.

Category 21.2 *Security product QA failures*

2005-01-18 **Unix Linux Xpdf stack based buffer overflow vulnerability code execution attack update issued**

DHS IAIP Daily; http://www.securityfocus.com/archive/1/387583/2005−01−16/200 5−01−22/2

MULTIPLE UNIX/LINUX VENDOR XPDF MAKEFILEKEY2 STACK OVERFLOW

Remote exploitation of a buffer overflow vulnerability in the xpdf PDF viewer included in multiple Unix and Linux distributions could allow for arbitrary code execution as the user viewing a PDF file. Successful exploitation of this vulnerability leads to arbitrary code execution as the user who opened the malicious file. An attacker would have to convince a target to open the provided file in order to exploit this vulnerability. A patch to address this issue is available at: ftp://ftp.foolabs.com/pub/xpdf/xpdf-3.00pl3.patch. Updated binaries (ver. 3.00pl3) to address this issue are available at: http://www.foolabs.com/xpdf/download.html

---

Category 21.2 *Security product QA failures*

2005-01-19 **Oracle products multiple vulnerabilities injection denial of service DoS attack update issued**

DHS IAIP Daily; http://secunia.com/advisories/13862/

ORACLE PRODUCTS HAVE TWENTY-THREE VULNERABILITIES.

Twenty-three vulnerabilities have been reported in various Oracle products. Some have an unknown impact and others can be exploited to disclose sensitive information, gain escalated privileges, conduct PL/SQL injection attacks, manipulate information, or cause a DoS (Denial of Service). Patches are available through the vendor.

Category 21.2 *Security product QA failures*

2005-01-21 **Ethereal network sniffer packet dissector vulnerabilities denial of service DoS update issued**

DHS IAIP Daily; http://secunia.com/advisories/13946/

ETHEREAL MULTIPLE UNSPECIFIED PACKET DISSECTOR VULNERABILITIES

Multiple vulnerabilities have been reported in Ethereal, which can be exploited by malicious people to cause a DoS (Denial of Service) or potentially compromise a vulnerable system. These vulnerabilities include errors in the COPS dissector, the DLSw dissector, the DNP dissector, the Gnutella dissector, the MMSE dissector, and the X11 dissector. Update to version 0.10.9: http://www.ethereal.com/download.html

---

Category 21.2 *Security product QA failures*

2005-01-26 **Avaya products multiple vulnerabilities denial of service DoS privilege escalation attack**

DHS IAIP Daily; http://secunia.com/advisories/14011/

AVAYA PRODUCTS MULTIPLE VULNERABILITIES

Multiple vulnerabilities have been reported in Avaya products, which can be exploited by malicious people to cause a Denial of Service or compromise a vulnerable system. Avaya has multiple vulnerabilities in: libitff / zip / vim / unarj /openmotif / postgresql / lesstif / pine / xpdf ; which potentially can be exploited to cause a DoS (Denial of Service), a user can gain escalated privileges, or compromise a vulnerable system. The vendor recommends the following: restrict local access to the server; do not open or view PDF files, and XPM and TIFF images; do not compress or decompress files from untrusted sources; do not enable modeline or filetype plugins in VIM; do not run the "make_oidjoins_check" script.

Category 21.2 *Security product QA failures*

2005-01-27 **Juniper JUNOS remote denial of service vulnerability DoS**

DHS IAIP Daily; http://secunia.com/advisories/14049/

JUNIPER JUNOS UNSPECIFIED REMOTE DENIAL OF SERVICE VULNERABILITY

A new vulnerability has been identified in Juniper Networks routers running JUNOS software, which can be exploited by attackers to cause a Denial of Service. The vulnerability is caused due to an unspecified error within the processing of certain network packets. This can be exploited to disrupt the operation of a vulnerable device via some specially crafted network packets. According to Juniper, it is not possible to use firewall filters to protect vulnerable routers. The vulnerability affects all releases of JUNOS built prior to 2005-01-07. Users registered at Juniper's support site can view patch information at: https://www.juniper.net/alerts/viewalert.jsp?txtAlertNumber= PSN-2005-01-009&actionBtn=Search

---

Category 21.2 *Security product QA failures*

2005-01-31 **HP VirtualVault TGA Trusted Gateway Agent vulnerability denial of service DoS update issued**

DHS IAIP Daily; http://secunia.com/advisories/14082/

HP VIRTUALVAULT TRUSTED GATEWAY AGENT DENIAL OF SERVICE VULNERABILITY

A vulnerability has been reported in HP Virtualvault, which can be exploited by malicious people to cause a Denial of Service. The vulnerability is caused due to an unspecified error in the TGA (Trusted Gateway Agent) daemon and can be exploited via specially crafted network traffic. Apply patch available through the vendor.

Category 21.2 *Security product QA failures*

2005-02-02 **Cisco Internet Protocol videoconferencing IP/VC product vulnerability remote user access device hijacking workaround issued**

DHS IAIP Daily; http://securitytracker.com/alerts/2005/Feb/1013067.html

CISCO IP/VC HARD-CODED SNMP COMMUNITY STRINGS LET REMOTE USERS ACCESS THE DEVICE

A vulnerability was reported in Cisco's IP/VC videoconferencing products. A remote user can gain access to the system using common default SNMP community strings. A user with knowledge of the community strings can gain full control of the device. Such users can, among other things, create new services, terminate or affect existing sessions, and redirect traffic to a different destination. Cisco has described a workaround in their advisory, available at: http://www.cisco.com/public/technotes/cisco-sa-20050202-ipvc .shtml

---

Category 21.2 *Security product QA failures*

2005-02-03 **Microsoft bulletin patch fix update release critical important Windows operating system Media Player MSN Messenger**

DHS IAIP Daily; http://news.com.com/Windows+glitches+to+get+fixes/2100−1002_ 3−5562678.html

MICROSOFT TO RELEASE 13 UPDATES - AT LEAST ONE CRITICAL

Thirteen Microsoft patches will be released next Tuesday, February 8, including nine fixes for Windows flaws. At least one of the updates for the Windows operating system is rated "critical," its highest rating, Microsoft said Thursday, February 3, in a posting to its TechNet site. The forewarning is part of the company's program to give regular computer users notice of monthly security bulletins before the patches themselves are released. These updates will patch a critical flaw affecting Office and Visual Studio, and another critical flaw involving Windows, Windows Media Player and MSN Messenger. Also on the way are a patch for an "important" vulnerability in .Net Framework and a fix for "moderate" problems with SharePoint Services and Office. Bulletin: http://www.microsoft.com/technet/security/bulletin/advance.m spx

---

Category 21.2 *Security product QA failures*

2005-02-04 **Mozilla application suite Hewlett-Packard HP Tru64 UNIX vulnerability denial of service DoS attack update issued**

DHS IAIP Daily; http://secunia.com/advisories/14133/

MOZILLA APPLICATION SUITE "MSG_UNESCAPESEARCHURL()" BUFFER OVERFLOW

HP has confirmed a vulnerability in Mozilla Application Suite for Tru64 UNIX, which can be exploited by malicious people to cause a Denial of Service and potentially compromise a user's system. The vulnerability is caused due to a boundary error in the "MSG_UnEscapeSearchUrl()" function in "nsNNTPProtocol.cpp" when processing NNTP URIs. Update to Mozilla Application Suite 1.7.5: http://h30097.www3.hp.com/internet/download.htm

---

Category 21.2 *Security product QA failures*

2005-02-07 **Emacs editor open source vulnerability movemail format string Post Office Protocol POP code execution attack**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2005/Feb/1013100.html

EMACS MOVEMAIL FORMAT STRING FLAW MAY LET REMOTE POP SERVERS EXECUTE ARBITRARY CODE

The vendor reported that a remote POP3 mail server can send a specially crafted response to a connected movemail client to trigger a format string flaw and execute arbitrary code on the target client. The code will execute with the privileges of the movemail process. On some systems, movemail is configured with set group id (setgid) 'mail' group privileges. The flaw resides in 'movemail.c'. A fixed version of XEmacs (21.4.17) is available at: ftp://ftp.xemacs.org/pub/xemacs/xemacs-21.4

Category 21.2 *Security product QA failures*

2005-02-08 **SquirrelMail S/MIME Multipurpose Internet Mail Extension vulnerability command injection attack command execution update issued**

DHS IAIP Daily; http://www.k−otik.com/english/advisories/2005/0115

SQUIRRELMAIL S/MIME PLUGIN COMMAND INJECTION VULNERABILITY

A command injection vulnerability was reported in the Squirrelmail S/MIME plugin 0.5, which may be exploited by malicious users to execute arbitrary commands. The problem exists due to a missing input sanitizing error when handling the "cert" [viewcert.php] variable. Update to SquirrelMail S/MIME Plugin version 0.6: http://www.squirrelmail.org/plugin_view.php?id=54

Category 21.2 *Security product QA failures*

2005-02-09 **Symantec UPX heap based buffer overflow vulnerability DEC2EXE parsing engine update issued**

DHS IAIP Daily; http://secunia.com/advisories/14179

SYMANTEC MULTIPLE PRODUCTS UPX PARSING ENGINE BUFFER OVERFLOW

A vulnerability has been reported in multiple Symantec products, which can be exploited by malicious people to execute arbitrary code on a vulnerable system. The vulnerability is caused due to a boundary error in the DEC2EXE parsing engine used by the antivirus scanning functionality when processing UPX compressed files. This can be exploited to cause a heap-based buffer overflow via a specially crafted UPX file. Original advisory and updates: http://www.sarc.com/avcenter/security/Content/2005.02.08.htm l

---

Category 21.2 *Security product QA failures*

2005-02-10 **BrightStor ARCserve Backup discovery service buffer overflow code execution attack update issued**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2005/Feb/1013138.html

BRIGHTSTOR ARCSERVE BACKUP BUFFER OVERFLOW IN DISCOVERY SERVICE LETS REMOTE USERS EXECUTE ARBITRARY CODE

A buffer overflow vulnerability in BrightStor ARCserve Backup may permit a remote user to execute arbitrary code on the target system. A remote user can send a specially crafted UDP probe to the Discovery Service on the target system to trigger a buffer overflow of data returned from the recvfrom() function. Vendor updates are available: http://supportconnect.ca.com

---

Category 21.2 *Security product QA failures*

2005-02-10 **F-Secure security vendor ARJ archive handling vulnerability code execution attack update issued**

DHS IAIP Daily; http://secunia.com/advisories/14216/

F-SECURE MULTIPLE PRODUCTS ARJ ARCHIVE HANDLING VULNERABILITY

A vulnerability has been reported in multiple F-Secure products, which can be exploited by malicious people to compromise a vulnerable system. The vulnerability is caused due to a boundary error in the antivirus scanning functionality when processing ARJ archives. This can be exploited to cause a buffer overflow via a specially crafted ARJ archive. Successful exploitation allows execution of arbitrary code, but requires that the malicious ARJ archive is scanned with archive scanning enabled. Updates and original advisory available: http://www.f-secure.com/security/fsc-2005-1.shtml

---

Category 21.2 *Security product QA failures*

2005-02-11 **BrightStor ARCserve Backup default administrator account unauthorized access code execution attack update issued**

DHS IAIP Daily; http://secunia.com/advisories/14233/

BRIGHTSTOR ARCSERVE BACKUP DEFAULT ADMINISTRATOR ACCOUNT

A security issue has been reported in BrightStor ARCserve/Enterprise Backup, which can be exploited by malicious people to gain unauthorized access. The product contains a hard-coded, undocumented administrative account for the Common Agent component. Successful exploitation grants administrative access to the system and may allow execution of arbitrary code. Apply patches available at: http://supportconnect.ca.com

---

Category 21.2 *Security product QA failures*

2005-02-11 **Barracuda spam firewall 200 vulnerability open mail relay configuration update firmware**

DHS IAIP Daily; http://secunia.com/advisories/14243/

BARRACUDA SPAM FIREWALL 200 OPEN MAIL RELAY VULNERABILITY

A vulnerability exists which can be exploited by white-listed senders to use Barracuda Spam Firewall as an open mail relay regardless of what domains Barracuda Spam Firewall is configured. Update to firmware 3.1.11 or later.

Category 21.2 *Security product QA failures*

2005-02-12 **Advanced Guestbook SQL injection vulnerability administrative access proof of concept exploits update issued**

DHS IAIP Daily; http://www.securityfocus.com/bid/10209/discussion/

ADVANCED GUESTBOOK PASSWORD PARAMETER SQL INJECTION VULNERABILITY

It has been reported that Advanced Guestbook is prone to a SQL injection vulnerability that could allow an attacker to gain administrative access to the application. Proof of Concept exploits indicate that it is possible to trigger this issue by leaving the username or password entry blank and then entering certain strings in the password or username fields. This vulnerability is reportedly fixed in version 2.3.1.

Category 21.2 *Security product QA failures*

2005-02-22 **NTLM Kerberos authentication open source buffer overflow vulnerabilities update issued**

DHS IAIP Daily; http://secunia.com/advisories/14364/

CURL/LIBCURL NTLM AND KERBEROS AUTHENTICATION BUFFER OVERFLOWS

Two vulnerabilities have been reported in cURL/libcURL 7.12.1, which can be exploited by malicious people to compromise a user's system. Boundary errors in the "Curl_input_ntlm()" and the "Curl_krb_kauth()" function can be exploited to cause a stack-based buffer overflow. Updates available at: http://cool.haxx.se/cvs.cgi/curl/lib/http_ntlm.c.diff?r1=1.3 6&r2=1.37

Category 21.2 *Security product QA failures*

2005-02-24 **Trent Micro Antivirus VSAPI ARJ archives vulnerability command execution attack**

DHS IAIP Daily; http://www.k−otik.com/english/advisories/2005/0203

TREND MICRO PRODUCTS VSAPI ARJ ARCHIVES PROCESSING VULNERABILITY

A critical vulnerability was reported in several Trend Micro products, and could be exploited by attackers or worms to execute arbitrary commands. The problem is due to a buffer overflow error in the ARJ archive file format parser when handling a specially crafted file name field in the local header, which could be exploited by attackers to execute arbitrary commands by sending a specially crafted ARJ archive to a vulnerable scanner. Upgrade to VSAPI 7.510: http://www.trendmicro.com/download/engine.asp

---

Category 21.2 *Security product QA failures*

2005-02-24 **ACNS denial of service default password vulnerabilities denial of service DoS attack**

DHS IAIP Daily; http://www.cisco.com/warp/public/707/cisco−sa−20050224−acnsd os.shtml

CISCO — ACNS DENIAL OF SERVICE AND DEFAULT ADMIN PASSWORD VULNERABILITIES.

Devices running Cisco Application and Content Networking System (ACNS) software may be vulnerable to Denial of Service (DoS) attacks and may contain a default password for the administrative account. Devices running ACNS software may be vulnerable to the DoS attacks while configured as a transparent proxy server, forward proxy server, or reverse proxy server. The administrative account default password does not require a software upgrade and can be changed by a configuration command for all affected customers. Vendor solutions available through link below.

Category 21.2 *Security product QA failures*

2005-03-08 **Ethereal network sniffer security software stack based buffer overflow vulnerability remote user code execution attack update issued**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2005/Mar/1013399.html

ETHEREAL BUFFER OVERFLOW IN 3G-A11 DISSECTOR LETS REMOTE USERS EXECUTE ARBITRARY CODE

The Ethereal dissector for processing CDMA2000 A11 RADIUS authentication packets contains a stack-based overflow. The dissect_a11_radius() function in 'packet-3g-a11.c' copies up to 256 bytes of user-supplied data of a size specified by the user into a 16 byte buffer. A remote user can supply a specially crafted packet to trigger the overflow and potentially execute arbitrary code on the target system. A fix is available via SVN at: http://ethereal.com/development.html

---

Category 21.2 *Security product QA failures*

2005-03-15 **Symantec security vendor product multiple vulnerabilities Domain Name System DNS cache poisoning redirection attack update issued**

DHS IAIP Daily; http://securityresponse.symantec.com/avcenter/security/Content/2005.03.15.html

SYMANTEC PRODUCTS MULTIPLE VULNERABILITIES

Multiple vulnerabilities are identified in Symantec products (Enterprise Firewall, VelociRaptor, and Gateway Security) that may be exploited by attackers to conduct DNS cache poisoning and redirection attacks. An updated hot fix was released on March 14 that further hardens the DNS for protection against an additional potential vector identified by Symantec engineers. Symantec recommends customers immediately apply the latest hot fix for their affected product versions to protect against this type of threat. Product specific hot fixes are available via the Symantec Enterprise Support site http://www.symantec.com/techsupp

---

Category 21.2 *Security product QA failures*

2005-03-16 **OpenPGP partial plaintext retrieval vulnerability encrypted message recovery design flaw consult vendor**

DHS IAIP Daily; http://www.securityfocus.com/bid/12529/discussion/

OPENPGP PARTIAL PLAINTEXT RETRIEVAL VULNERABILITY

OpenPGP may theoretically allow attackers to retrieve partial plaintexts from encrypted OpenPGP messages. A cipher text attack method has been developed that exploits a flaw in OpenPGP to retrieve partial plaintexts from OpenPGP messages encrypted with symmetric encryption. Apparently when messages are encrypted with the CFB mode, a design flaw in an integrity check feature can be exploited. Consult your vendor for patch information.

Category 21.2 *Security product QA failures*

2005-03-28 **Symantec security product vulnerabilities denial of service DoS system crash update issued**

DHS IAIP Daily; http://securityresponse.symantec.com/avcenter/security/Content/2005.03.28.html

MULTIPLE SYMANTEC PRODUCTS HAVE DENIAL OF SERVICE VULNERABILITIES

Two vulnerabilities were reported in Symantec's Norton AntiVirus, Internet Security, and System Works in the AutoProtect feature. A user can create a file or modify a filename to cause the target system to crash. When Auto-Protect was invoked to scan a particular file type, e.g., introduced on a CD, copied and pasted into the system, etc., the resultant scan caused the system to hang and generate a general protection fault error, or BSOD requiring a system reboot to clear. When SmartScan enabled, renaming a file stored on a network share can induce a system crash when the modification kicks off SmartScan. Based on the file write for the name change, SmartScan will be invoked to scan the file, which can result in excess CPU consumption and ultimately a system crash. Updates are available via Symantec LiveUpdate.

Category 21.2 *Security product QA failures*

2005-04-25 **Trend Micro antivirus software update problem Windows XP SP2**

DHS IAIP Daily; http://news.zdnet.co.uk/0,39020330,39196220,00.htm

TREND MICRO CUSTOMERS SUFFER WEEKEND PROBLEMS

Trend Micro apologized on Monday, April 25, for distributing a faulty software update that caused IT workers around the world to spend the weekend fixing their systems. The Japan-based antivirus company has promised to compensate customers whose computers running Windows XP SP2 were disabled by the update. The company said the update was only available for ninety minutes and caused "certain performance issues" with CPUs. Trend Micro, which denied rumors that the update included a virus, said it didn't know what had caused the incident but that it had now issued a fix and was working with channel partners to solve the problem. Trend Micro said that most of the businesses affected were located in Japan, and that few complaints had been received from customers in the U.S. and Europe. The update affected versions 7.5 and above of Trend Micro's Scan Engine.

Category 21.2 *Security product QA failures*

2005-05-11 **Cisco Catalyst switches 6500 7600 firewall services module ACL bypass vulnerability update issued**

DHS IAIP Daily; http://www.cisco.com/warp/public/707/cisco−sa−20050511−url.s html

CISCO — CISCO CATALYST 6500/7600 SERIES FIREWALL SERVICES MODULE ACL BYPASS VULNERABILITY.

A new vulnerability was identified in Cisco products, which may be exploited by attackers to bypass the security restrictions. A vulnerability exists in the Cisco Firewall Services Module when URL, FTP, or HTTPS filtering is enabled in which inbound TCP packets can bypass access-list entries intended to explicitly filter them. updates available through Source link below.

Category 21.2 *Security product QA failures*

2005-05-11 **Ethereal network sniffer stack buffer overflow vulnerability update issued**

DHS IAIP Daily; http://www.securityfocus.com/bid/13567/info/

ETHEREAL DISTCC DISSECTION STACK BUFFER OVERFLOW VULNERABILITY

A remote buffer overflow vulnerability exists in Ethereal due to a failure of the application to securely copy network-derived data into sensitive process buffers. The specific issue exists in the DISTCC protocol dissector. An attacker may exploit this issue to execute arbitrary code with the privileges of the user that activated the vulnerable application. This may facilitate unauthorized access or privilege escalation. The vendor has released Ethereal version 0.10.11 to address this and other vulnerabilities.

Category 21.2 *Security product QA failures*

2005-05-19 **ZENworks remote management authentication validation failure no update issued**

DHS IAIP Daily; http://www.zone−h.org/en/advisories/read/id=7524/

ZENWORKS REMOTE MANAGEMENT FAILS TO PROPERLY VALIDATE AUTHENTICATION

This authentication protocol contains several stack and heap overflows that can be triggered by an unauthenticated remote attacker to obtain control of the system that requires authentication. Successful exploitation of ZENworks allows attackers unauthorized control of related data and privileges on the machine and network. It also provides attackers leverage for further network compromise. There is no solution at this time.

Category 21.2 *Security product QA failures*

2005-06-30 **government surveillance counter-terrorism identification authentication I&A travellers visitors Department Homeland Security DHS errors data integrity correctness Freedom of Information Act FOIA**

EPIC Alert; http://www.epic.org/alert/EPIC_Alert_12.13.html 12 13

US-VISIT PROBLEMS CAUSE VISITOR DELAYS AT PORTS OF ENTRY

The Electronic Privacy Information Center (EPIC) obtained information throught the Freedom of Information Act (FOIA) showing that the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) has significant errors in its database, causing "many cases of mistaken identity. Commercial aircrew members, vacationers, and businesspersons have all been delayed by the gaffes. The problems caused unnecessary delays in the visitors' travels and resulted in the improper flagging of crewmembers by government watch lists."

The EPIC summary continues:

>US-VISIT was launched at 115 airports and 14 seaports in January 2004. By the end of 2005, the program will be operational at all of the nations more than 400 ports of entry. US-VISIT requires foreign nationals entering or exiting the country to submit biometric and biographical information. This data collection often begins before a visitor buys her plane ticket, as U.S. Consular offices abroad may, before issuing a U.S. Visa, collect fingerscans from potential visitors and compare them against those in a criminal database. Fingerscans are again collected upon the visitor's arrival in the U.S. For verification and then stored in a government database, as are travelers' arrival and departure records. Failure to be processed through this departure confirmation system could jeopardize a visitor's re-admittance to the U.S., as the government compares the manifest information provided by air and cruise lines to ascertain that visitors have not overstayed their visas.

Last September, US-VISIT expanded to include visitors from the 27 nations who are members of the Visa Waiver Program, thus requiring the screening of an additional 33,000 persons per day. Except for visiting diplomats and officials and persons under 14 or over 79 years old, US-VISIT now applies to virtually all foreign nationals holding nonimmigrant visas, regardless of country of origin.

The documents obtained by EPIC show that some travelers are aware that the US-VISIT database contains erroneous information well before DHS realizes its own mistake and fear that their next visit to the U.S. Will result in misidentification. Visitors reported missing their connecting flights due to errors in the database system, and airline crewmembers reported being delayed up to ninety minutes after a long international flight. Some travelers reported that the operator collecting fingerscans at a port had erroneously reversed their left and right index fingerprints, labeled a husband's fingerprints as his wife's, failed to collect the data required under US-VISIT, or collected data from travelers exempt from the program, such as holders of a G-4 visa.<

Category 21.2 *Security product QA failures*

2005-08-01 **Emergency Alert System data entry error user interface verification software quality assurance QA design input checking verification hardware problem bug glitch flaw**

RISKS; http://www.wired.com/news/technology/0,1282,68363,00.html 23 96

EMERGENCY ALERT SYSTEM ERRORS IN FLORIDA & NEVADA

Kevin Poulson reported in _Wired_ on two errors in the Emergency Alert System (EAS) at the end of July that luckily failed to cause panic.

"The Florida gaffe occurred when an operator at the National Weather Service's Tallahassee forecast office inadvertently entered the code 'RHW' instead of 'RWT,' keying a radiological hazard warning instead of a required weekly test…. Fortunately, it failed to cause panic, in part because the audio accompanying the message still identified it as 'only a test,' and the office moved rapidly to quash the false alarm."

In Las Vegas, radio station "KXTE-FM tried to send out a message canceling an earlier Amber Alert, and instead transmitted an EAN, or emergency action notification -- a special code reserved for the president of the United States to use in the event of a nuclear war or similar extreme national emergency…. The error apparently resulted from a hardware problem in the station's EAS encoder-decoder. 'We think that the internal battery had failed, the programming had scrambled itself,' said [a spokesperson for KXTE]."

Category 21.2 *Security product QA failures*

2005-08-03 **lightning damage lightning-detection system recursion**

RISKS; http://tinyurl.com/7jf8h 24 01

RECURSIVE LIGHTNING PROBLEMS

A bit of light-hearted fun at the expense of the lightning-detection folks:

Klaus Johannes Rusch noted this recursive case of vulnerability to what's being monitored:

>Fortunately there were only a few minor injuries when a plane overshot a runway at Pearson International Airport. According to a CBC report … most operations on the airport had been suspended due to bad weather: "… a spokesperson with the Greater Toronto Airports Authority said lightning was causing technical problems with the airport's lightning-detection system." Why would one expect that lightning-detection systems could cope with lightning?<

Peter G. Neumann chimed in with an amusing recollection of a similar case:

>My favorite meta-lightning event occurred was when I was giving a lecture in my Survivable Systems course at Maryland, and I was talking about the time at Wallops Island where they had several missiles ready to launch because they wanted to study the effects of lightning on the missile controls. As some of you may remember, lightning hit the launch platform and triggered the launching of one of the missiles (which I mentioned most recently in RISKS-20.42). Just at that point in the lecture, lightning hit the lecture room and took down the computer controlling the outfeeds to remote classrooms and our own video monitors. Some of the students wondered how I had managed such a theatrical effect.<

Category 21.2 *Security product QA failures*

2005-08-06 **vulnerability hole Acunetix Web Scanner remote denial-of-service DoS sniffer**

DHS IAIP Daily; http://www.securityfocus.com/bid/14488/info

ACUNETIX WEB VULNERABILITY SCANNER REMOTE DENIAL OF SERVICE VULNERABILITY

Acunetix Web Vulnerability Scanner is affected by a remote denial of service vulnerability. This issue affects the Web sniffer component of the application. An attacker can exploit this issue by gaining control of a server through some means or by sending spoofed traffic to the network. A successful attack can result in a denial of service condition due to resource exhaustion. Acunetix Web Vulnerability Scanner version 2.0 is affected. Other versions may be vulnerable as well. Security Focus is not currently.

Category 21.2 *Security product QA failures*

2005-08-22 **vulnerability Cisco intrusion prevention system IPS privilege escalation update issued**

DHS IAIP Daily; http://www.cisco.com/warp/public/707/cisco−sa−20050824−ips.s html

CISCO INTRUSION PREVENTION SYSTEM VULNERABLE TO PRIVILEGE ESCALATION

Cisco Intrusion Prevention Systems (IPS) are a family of network security devices that provide network based threat prevention services. A user with OPERATOR or VIEWER access privileges may be able to exploit a vulnerability in the command line processing (CLI) logic to gain full administrative control of the IPS device. Vulnerable products are Cisco Intrusion Prevention System version 5.0(1) and 5.0(2). This issue is fixed in IPS version 5.0(3) which is available for download: http://www.cisco.com/pcgi-bin/tablebuild.pl/ips5

Category 21.2 *Security product QA failures*

2005-08-22 **vulnerability hole Cisco IDS Management Software SSL Certificate validation bypass security restrictions Service Pack**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1497

CISCO IDS MANAGEMENT SOFTWARE SSL CERTIFICATE VALIDATION VULNERABILITY

A vulnerability was identified in CiscoWorks Management Center for IDS Sensors (IDSMC) and Monitoring Center for Security (Security Monitor or Secmon), which could be exploited by remote attackers to bypass the security restrictions. This flaw is due to an error in the SSL certificate checking functionality that does not properly validate SSL certificates, which could be exploited by attackers to spoof an IDS or IPS and then gather login credentials, submit false data, and filter legitimate data from. Products affected are IDSMC version 2.0 and 2.1, and CiscoWorks Monitoring Center for Security (Security Monitor or Secmon) version 1.1, 2.0 and 2.1. This vulnerability has been addressed in Service Pack 1 for IPSMC 2.1 and Security Monitor 2.1: http://www.cisco.com/pcgi-bin/tablebuild.pl/mgmt-ctr-ids-app

---

Category 21.2 *Security product QA failures*

2005-08-31 **vulnerability Symantec AntiVirus Corporate Edition local information disclosure no patch issued**

DHS IAIP Daily; http://www.securityfocus.com/bid/14708/info

SYMANTEC ANTIVIRUS CORPORATE EDITION LOCAL INFORMATION DISCLOSURE VULNERABILITY

Symantec AntiVirus Corporate Edition is susceptible to a local information disclosure vulnerability. Sensitive information such as the server name, IP address, subnet, subnet mask, connection protocol, username and password to access the LiveUpdate server are logged in a plain text file. A local attacker can subsequently access the file and disclose authentication credentials to access the server. This may lead to various attacks including the potential compromise of the server. Security Focus is not currently aware of any vendor-supplied patches for this issue.

Category 21.2 *Security product QA failures*

2005-08-31 **insider theft security identification authentication I&A piggybacking overwork disgruntled employees trial judgement theft fraud**

RISKS; http://archiv.tagesspiegel.de/archiv/31.08.2005/2022942.asp#art (in German) 24 03

GERMAN INSIDER-THEFT CASE ILLUSTRATES AWFUL SECURITY

Social services have a money machine set up in which, when a client is given money, instead of having it transferred to their account, a chip card is selected, and the number of the card typed into a computer program that controls payouts. The client takes the card to an ATM-like money machine, puts the card in, key is the secret password which is [I hope you are sitting down … --dww] the *birthday* of the client, and takes out the money. A camera films the transaction, but erases the tapes about 6 weeks later.

The program records the payout in the files of the client, and only people with proper passwords have access to the payout system. This is called security.

About 27.000 Euros (about the same in dollars these days) disappeared about 2 years ago. The revision department nailed down 22 transactions that had been conducted without an entry in the files of a client, and the clients knew nothing of the windfalls.

The accused kept his mouth shut during the process, and it was uncovered that the cards were not kept track of and "flew around the offices", people would log onto their payout computers and remain logged in all day, sometimes leaving the office without locking the door. It would have been trivial for a colleague to quickly use a computer to load up a card, then slip it to an accomplice and have them pick up the cash. In addition, everyone seemed to know everyone else's passwords…

The defence lawyer also noted that the social workers were all mad about the extra work they had to do about the new German dole system, so it really could have been anyone.

Berlin remains out the 27.000 Euros and has to pay court costs, the accused keeps his job (but was transferred, probably to the filing room), and the judge recommends they re-think the security of the payout system. I'm with the judge on this one!

[Abstract by Debora Weber-Wulff]

Category 21.2 *Security product QA failures*

2005-09-05 **vulnerability Barracuda Spam Firewall remote directory traversal code execution update issued**

DHS IAIP Daily; http://www.securiteam.com/securitynews/5OP031FGVU.html

VULNERABILITY IN BARRACUDA SPAM FIREWALL

A remote Directory Traversal and Remote Execution vulnerability exist in Barracuda Spam Firewall appliance from Barracuda Networks. In the script "/cgi-bin/img.pl", used to show graph, the value of the "f" (filename) parameters is not sanitized. No authentication is required to exploit this remote vulnerability Barracuda Spam Firewall firmware v.3.1.16 and v.3.1.17 are affected. Other vulnerabilities exist in the advance utilities section but administrative privileges are needed. Firmware update 3.1.18 fixes this issue (3.3.* is also safe).

Category 21.2 *Security product QA failures*

2005-09-07 **vulnerability Cisco IOS firewall authentication proxy FTP telnet sessions buffer overflow workarounds**

DHS IAIP Daily; http://www.cisco.com/warp/public/707/cisco−sa−20050907−auth_ proxy.shtml

CISCO IOS FIREWALL AUTHENTICATION PROXY FOR FTP AND TELNET SESSIONS BUFFER OVERFLOW

The Cisco IOS Firewall Authentication Proxy for FTP and/or Telnet Sessions feature in specific versions of Cisco IOS software is vulnerable to a remotely-exploitable buffer overflow condition. Only devices running certain versions of Cisco IOS® are affected. Cisco has made free software available to address this vulnerability. There are workarounds available to mitigate the effects of the vulnerability.

Category 21.2 *Security product QA failures*

2005-09-07 **vulnerability Symantec Brightmail AntiSpam denial-of-service DoS antivirus scanning**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1660

SYMANTEC BRIGHTMAIL ANTISPAM DENIAL OF SERVICE VULNERABILITIES

Two vulnerabilities were identified in Symantec Brightmail AntiSpam, which could be exploited by remote attackers to cause a denial of service. The first flaw is due to an unspecified error in the antivirus scanning and cleaning procedures that do not properly handle deeply nested zip files, which could cause the application to process messages for an extended period of time. The second vulnerability is due to an unspecified error in the decomposer that does not properly handle "winmail.dat" objects embedded in MIME files, which could cause the application to crash.

Category 21.2 *Security product QA failures*

2005-09-26 **vulnerability Cisco Security Advisory IOS firewall authentication proxy FTP telnet sessions buffer overflow**

DHS IAIP Daily; http://www.cisco.com/warp/public/707/cisco−sa−20050907−auth_ proxy.shtml

CISCO IOS FIREWALL AUTHENTICATION PROXY FOR FTP AND TELNET SESSIONS BUFFER OVERFLOW

The Cisco IOS Firewall Authentication Proxy for FTP and/or Telnet Sessions feature in specific versions of Cisco IOS software is vulnerable to a remotely exploitable buffer overflow condition. The vulnerability is in the Cisco IOS Firewall Authentication Proxy feature which allows network administrators to apply specific security policies on a per user basis. Cisco IOS Software is vulnerable to a Denial of Service (DoS) and potentially an arbitrary code execution attack when processing the user authentication credentials from an Authentication Proxy Telnet/FTP session. To exploit this vulnerability an attacker must first complete a TCP connection to the IOS device running affected software and receive an auth-proxy authentication prompt.

Category 21.2 *Security product QA failures*

2005-10-13 **automated teller machines ATM banking denial of service DoS failure software quality assurance input error QA design testing**

RISKS; http://www.nu.nl/news.jsp?n=603834&c=122&rss (in Dutch) 24 07

UNLUCKY SEVEN

The Dexia Bank ATM machines are experiencing a curious problem. The machines stop functioning when someone enters the number 7, making it impossible for people with a 7 in their pin (personal identification number) code to perform a cash withdrawal.

The problem has been occurring for a month. To prevent people from running out of cash, they are able to perform cash withdrawals inside. "We are experiencing a problem with the software", a Dexia spokesman admitted last Wednesday in the daily journal Het Laatste Nieuws, "the problems should be solved within three weeks."

[Abstract by Lindsay Marshall]

[MK comments: THREE WEEKS?!?]

Category 21.2 *Security product QA failures*

2005-11-11 **vulnerability Kerio WinRoute firewall disabled account authentication denial-of-service DoS**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2005/Nov/1015194.html

KERIO WINROUTE FIREWALL MAY LET USERS OF DISABLED ACCOUNTS AUTHENTICATE TO THE SYSTEM

A vulnerability was reported in Kerio WinRoute Firewall. A remote previously authorized user may be able to authenticate. A remote user may be able to authenticate to the system even if their account has been disabled. The firewall does not properly process certain RTSP streams. A remote user may be able to cause denial of service conditions. The vendor has issued a fixed version (6.1.3): www.kerio.com/kwf_home.html

---

Category 21.2 *Security product QA failures*

2005-12-03 **vulnerability Cisco OpenSSL protocol negotiation man-in-the-middle attack**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/2710

CISCO PRODUCTS OPENSSL INSECURE PROTOCOL NEGOTIATION VULNERABILITY

A vulnerability has been identified in various Cisco products, which could be exploited by attackers to bypass certain security restrictions. This issue is due to an error in the "SSL_OP_MSIE_SSLV2_RSA_PADDING" option of OpenSSL that does not properly reject SSL 2.0 sessions when a client supports SSL 3.0 or TLS 1.0, which could be exploited by malicious people to conduct MITM (Man in the Middle) attacks and force a client and a server to negotiate the SSL 2.0 protocol instead of SSL 3.0 or TLS 1.0.

Category 21.2 *Security product QA failures*

2005-12-22 **Symantec vulnerability impacts products detection exploits patches code programs bug security RAR compressed files utility titles products Library Norton Internet Security SystemWorks Firewall Symantec**

DHS IAIP Daily; http://www.securitypipeline.com/news/175007890;jsessionid=2AK0KWQB2SDV0QSNDBCSKH0CJUMEKJVN

Symantec says vulnerability impacts 63 products.

Symantec on Wednesday, December 21, named more than 60 of its products as affected by the critical vulnerability disclosed earlier this week, and said it was pushing out a "heuristic" detection that would spot potential exploits. However, no patches have yet been released. The number of impacted products was among the largest ever for a single vulnerability, and demonstrated the risk of reusing code in a large group of programs. The bug, which was made public Tuesday, December 20, by researcher Alex Wheeler, is in how Symantec's AntiVirus Library, part of virtually all the Cupertino, CA,-based security giant's programs, handles RAR compressed files. RAR files are created by the WinRAR compression utility, developed and sold by RarLab. In an advisory released Wednesday, Symantec listed 48 enterprise titles and 15 consumer products that used the flawed Library. On the consumer side, the 2006 versions of Norton AntiVirus, Internet Security, SystemWorks, and Personal Firewall are open to attack. Corporate titles such as Norton AntiVirus for Microsoft Exchange, BrightMail Antispam, and AntiVirus for Handhelds are also on the list. The only protection for the moment is a special detection capability that Symantec is downloading to users' systems.

Category 21.2 *Security product QA failures*

2005-12-22 **McAfee VirusScan privilege escalation vulnerability arbitrary applications quoted paths attackers VirusScan Symantec**

DHS IAIP Daily; http://www.securityfocus.com/bid/16040/references

McAfee VirusScan path specification local privilege escalation vulnerability.

McAfee VirusScan is prone to a vulnerability that could allow an arbitrary file to be executed. The 'naPrdMgr.exe' process calls applications without using properly quoted paths. Successful exploitation may allow local attackers to gain elevated privileges. Solution: It has been reported that McAfee VirusScan Enterprise 8.0i patch 12 is not vulnerable to this issue. This could not be confirmed by Symantec.

Category 21.2 *Security product QA failures*

2005-12-27 **Bugzilla unsafe temporary files gain privileges script temporary files symbolic link critical created overwritten bug tracking vulnerability Security Tracker pending**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2005/Dec/1015411.html

Bugzilla 'syncshadowdb' unsafe temporary files may let local users gain elevated privileges.

A vulnerability was reported in Bugzilla in the 'syncshadowdb' script wherein a local user can obtain elevated privileges. The 'syncshadowdb' script uses temporary files in an unsafe manner. A local user can create a symbolic link (symlink) from a critical file on the system to a temporary file to be used by the script. Then, when the script is executed by the bug tracking system, the symlinked file will be created or overwritten with the privileges of the bug tracking system. The vulnerability can enable a local user to obtain the privileges of the bug tracking system. The vulnerability affects Version(s): 2.6.10 and prior versions. Versions 2.18.* and 2.20.* are not affected. Security Tracker reports that the fix will be included in the pending 2.16.11 version but a solution is currently available. Solution: https://bugzilla.mozilla.org/show_bug.cgi?id=305353

Category 21.2 *Security product QA failures*

2006-01-03 **Cisco Secure ACS vulnerability security bypass fix update**

DHS IAIP Daily; http://www.hackerscenter.com/archive/view.asp?id=21516 23

CISCO SECURE ACCESS CONTROL SERVER DOWNLOADABLE IP

A vulnerability in Cisco Secure ACS (Access Control Server), which potentially can be exploited by malicious people to bypass certain security restrictions. The vulnerability is caused due to a design error in the Downloadable IP ACL (Access Control List) feature. This can be exploited by malicious people who know the name of a Downloadable IP ACL configured on the ACS server to authenticate to the RAS/NAS (Remote Access Server/Network Access Server) by using the name of that ACL as their user name. Solution: The vulnerability has been fixed in the following versions: Cisco Secure ACS Version 4.0.1, PIX version 6.3(5), PIX/ASA 7.0(2), Cisco IOS Software Version 12.3(8)T4, and VPN 3000 versions 4.0.5.B and 4.1.5.B.

Category 21.2 Security product QA failures

2006-01-11 **Symantec Norton System Works rootkit feature malware quality assurance failure**

DHS IAIP Daily; http://www.betanews.com/article/Symantec_Found_Using_Rootkit_Feature/1137029426 23

SYMANTEC FOUND USING ROOTKIT FEATURE [NO, IT'S NOT A ROOTKIT]

Symantec is cleaning up a feature in Norton SystemWorks that uses a rootkit-like technique to hide a system folder from Windows. The technology works similar to Sony BMG's controversial rootkit DRM in the way it masks files and makes them invisible to the operating system. The Norton Protected Recycle Bin feature adds a directory called Nprotect, which stores temporary copies of files that users delete. The idea was to supplement the standard Windows Recycle Bin and enable users to recover files they removed accidentally. However, hiding a directory from Windows can open the door to vulnerabilities, as the Sony DRM rootkit debacle exposed. Malware authors were able to write viruses and worms that hid in the cloaked directory, effectively preventing scanning software from discovering their existence on a PC. Users of Norton SystemWorks can download the patch now through LiveUpdate. The rootkit-like activity was discovered by Mark Russinovich of Sysinternals, who first released details on the Sony XCP software.

[MK notes: this article illustrates an improper use of the word "rootkit." It has never meant "stealth" alone. It is specifically used to denote software that allows an attacker to return to a compromised system and regain root privileges.]

Category 21.2 Security product QA failures

2006-01-12 **canonical password Joe account access control vulnerability root backdoor**

RISKS; http://tinyurl.com/atvlo 24 15

CISCO/CISCO = SILLY/SILLY

Gadi Evron analyzed a Cisco advisory entitled "Default Administrative Password in Cisco Security Monitoring, Analysis and Response System" which revealed a back door to root:

"The security issue is basically a user account on the system that will give you root when accessed.

The account is:
1. Hidden.
2. Default.
3. With a pre-set password."

Evron also noted that many Cisco routers still use a canonical "Joe" account (same string for account and password):

"On the other hand, the most common practice to hack routers today, is still to try and access the devices with the notoriously famous default login/password for Cisco devices: cisco/cisco.

Cisco/cisco is the single most used default password of our time. It got more routers pwned than any exploit in history, and it still does. One would think that a company such as Cisco, especially with this history, would stay away from such 'default' accounts? But the fact that this account is hidden makes it something different."

Category 21.2 Security product QA failures

2006-01-12 **Cisco Aironet Wireless Access Point denial of service DoS vulnerability**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2006/0176 23

CISCO AIRONET WIRELESS ACCESS POINTS DENIAL OF SERVICE VULNERABILITY

A vulnerability has been identified in Cisco Aironet Wireless Access Points (AP) running IOS, which may be exploited by remote attackers to cause a denial of service. This flaw is due to an error in the management interface that does not properly handle spoofed ARP (Address Resolution Protocol) messages, which could be exploited by an attacker who has successfully associated with a vulnerable device to exhaust all available memory resources and cause a denial of service. Solution: Upgrade to Cisco IOS version 12.3-7-JA2: http://www.cisco.com/public/sw-center/sw-wireless.shtml.

Category 21.2 *Security product QA failures*

2006-01-19 **anti-virus software F-Secure archive handling vulnerability**

DHS IAIP Daily; http://secunia.com/advisories/18529/ 23

F-SECURE ANTI-VIRUS ARCHIVE HANDLING VULNERABILITIES.

Some vulnerabilities have been reported in various F-Secure products, which can be exploited by malware to bypass detection to compromise a vulnerable system. A boundary error in the handling of ZIP archives can be exploited via a specially crafted ZIP archive to cause a buffer overflow and execute arbitrary code. In addition, an error in the scanning functionality when processing RAR and ZIP archives can be exploited to prevent malware from being detected. Secunia reports that a patch can be obtained at the vendor website. Patch: http://www.f-secure.com/security/fsc-2006-1.shtml

---

Category 21.2 *Security product QA failures*

2006-02-05 **IBM Tivoli Access Manager vulnerability Web applications directory traversal quality assurance**

DHS IAIP Daily; http://www.securiteam.com/unixfocus/5IP021FHPE.html 23

IBM TIVOLI ACCESS MANAGER DIRECTORY TRAVERSAL.

Tivoli Access Manager for e-business is a versatile solution for authentication and authorization problems. Primarily focused on Web applications, Access Manager implementations vary from simple Single Sign On (SSO) to more complex security infrastructure deployments. IBM Tivoli Access Manager is vulnerable for directory traversal that allows authenticated attackers to retrieve any file from the system. IBM's TAM Plug in contains a logout handler under the root Web path named "pkmslogout." This handler is designed to log out authenticated users. Vendor Status: A generally available fix pack for version 5.1.0 and 6.0 was released by the vendor on February 3, 2006 and available as: Fixpack 5.1.0-TIV-WPI-FP0017 is available at: http://www-1.ibm.com/support/docview.wss?uid=swg24011562 Fixpack 6.0.0-TIV-WPI-FP0001 is available at: http://www-1.ibm.com/support/docview.wss?uid=swg24011561

Category 21.2 *Security product QA failures*

2006-03-22 **Trend Micro InterScan Messaging directory insecure permissions vulnerability**

DHS IAIP Daily; http://www.hackerscenter.com/archive/view.asp?id=23774 23

TREND MICRO INTERSCAN MESSAGING "ISNTSMTP" DIRECTORY INSECURE PERMISSIONS.

A vulnerability has been identified in TrendMicro InterScan Messaging Security Suite, which could be exploited by local attackers to obtain elevated privileges. Analysis: This flaw is due to insecure permissions (Everyone/Full Control) being set on the "ISNTSmtp" directory, which could be exploited by malicious users to delete certain files or replace them with malicious binaries. Affected products: TrendMicro InterScan Messaging Security Suite version 5.5 build 1183 and prior. Solution: Upgrade to TrendMicro InterScan Messaging Security Suite version 5.7.0.1121: http://www.trendmicro.com/en/products/gateway/ismss/evaluate /overview.htm

---

Category 21.2 *Security product QA failures*

2006-04-13 **Microsoft security disclosure vulnerability policy criticism**

DHS IAIP Daily; 23
http://www.eweek.com/article2/0,1759,1949279,00.asp?kc=EWRSS03119TX1K0000594

MICROSOFT'S SECURITY DISCLOSURES COME UNDER FIRE.

Is Microsoft silently fixing security vulnerabilities and deliberately obfuscating details about patches in its monthly security bulletins? Matthew Murphy, a security researcher who has worked closely with the Microsoft Security Response Center in the past, is accusing the software maker of "misleading" customers by not clearly spelling out exactly what is being patched in the MS06-015 bulletin released on April 11. That bulletin, rated "critical," contained patches for a remote code execution hole in Windows Explorer, the embedded file manager that lets Windows users view and manage drives, folders and files. However, as Murphy found out when scouring through the fine print in the bulletin, the update also addressed what Microsoft described as a "publicly disclosed variation" of a flaw that was reported in May 2004. In an entry posted to the SecuriTeam blog, Murphy noted that the vulnerability that is documented was privately reported, but the "variation" that was also patched has been publicly known for 700+ days. "[The] information as published is extremely misleading and Microsoft's choice not to document a publicly reported vulnerability is not one that will be for the benefit of its customers' security," Murphy said.

21.3 Embedded processors

Category 21.3 *Embedded processors*

2005-07-20 **embedded control systems automobile safety shutoff flaw error damage emergency design override**

RISKS 23 95

DOES THE PROGRAMMER ALWAYS KNOW BEST?

Bob Paddock reported in RISKS that his Chrysler Voyager van seems to have been damaged by lightning recently and illustrated a design flaw that affects many other software and firmware systems: the assumption that users are complete idiots who cannot be trusted to override an automated decision no matter what the circumstances.

>Got the van out Friday night. I pulled out of the garage and as soon as I hit the road the Check Engine Light came on and the speedometer dropped to zero, as I continued to gain speed, going up the hill. The automatic transmission was now stuck in 1st-gear. I turned around a few driveways up the street and went back to the house. Made appointment to take it in for servicing the next morning.

Dealer is about four miles down the street. Limped along in 1st-gear to the dealer the next morning until we reached the only major four way intersection in this four mile gauntlet.

Right in the middle of the intersection the engine died like I turned the key off. A good Samaritan pushed the van off the road. The dealer came and towed the van for the last mile of the trip.

The dealer said that a tachometer feedback sensor had gone bad "and the van didn't know what speed it was going so it shut down to be safe".

Now for the Us vs Embedded part of the story: Isn't it sufficient that *I* knew stopping in the middle of a busy four way intersections was a Really Bad Thing to do? *It* thought it knew better than I did.

I'm really glad I did not have to cross any railroad tracks when *it* decided to stop on the crossing because it thought it was safe, rather than listen to my commands.<

* * *

In followup comments in RISKS 23.96, Michael Kohne warned that the dealer's hypothesis might be unfounded -- the reasons for the engine shutdown could have been something else entirely. Or perhaps "Another alternative is that he doesn't mean 'safe' the way you mean safe. He means 'it shut the engine down as an alternative to revving up until it explodes'. Because I guarantee that if the van's CPU let a bad sensor destroy the engine you'd be plenty po'd, and you'd probably be screaming even louder."

Category 21.3 *Embedded processors*

2005-08-13 **system design flaw identification authentication I&A failure collision automobile security**

RISKS 24 03

SINGLE-STATE AUTOMATON*

Last week I watched the chauffeur of a Mercedes car. There was a parking spot left just in front of another Mercedes. Both different types, though fairly new. As I watched by the chauffeur got out of her car and pushed the button on the remote control to close the doors.

The system worked. The doors of the Mercedes closed. The already parked Mercedes responded with a happy 'click' and opened its doors. The chauffeur, confident the click was her car telling everything was fine, didn't pay attention, until I pointed her to the fact that she opened the other Mercedes.

She tried several times. When her car opened the other one closed. And vice versa. But she didn't see it as a problem, she could close the doors of her car and walk away. Until I pointed out the system probably worked the other way round as well ….

[Abstract (lightly edited by MK) from Leon Kunders]

* MK explains: a "single-state automaton" is a device that can be either on or off and cycles between the states without memory. For example, an elevator call-button is a single-state automaton: pressing it multiple times once it is on does nothing to increase the speed of the elevator.

Category 21.3 *Embedded processors*

2006-04-07 **major Intel architecture x86 vulnerability Pentium design issue**

DHS IAIP Daily; http://www.fcw.com/article94004−04−07−06−Web&RSS=yes 23

CYBER ATTACKERS CAN EXPLOIT PENTIUM SELF-DEFENSE.

Your computer could hand itself over to cyber attackers when it's trying to cool off. That warning was issued this week at the CanSecWest/Core06 Conference in Vancouver, British Columbia. Computers with Intel Pentium processors can be hijacked through a built-in mode designed to protect the processor's motherboard, said Loïc Duflot, a security engineer and researcher for the scientific division of France's Central Directorate for Information Systems Security. The vulnerability affects every computer that runs on x86 architecture, including the millions that the U.S. government and industry use, said Dragos Ruiu, the conference's organizer.

21.4 SCADA (supervisory control and data acquisition) systems, vehicle controls

Category 21.4 *SCADA (supervisory control and data acquisition) systems, vehicle controls*

2005-02-08 **car virus embedded computers prediction**

NewsScan; http://news.com.com/A+virus+may+be+in+your+cars+future/2100-7349_3-5568633.html

NEW STUDY WARNS OF CAR VIRUSES

A report by IBM Security Intelligence Services predicts that viruses spreading to mobile phones, PDAs and wireless networks could infect the embedded computers that increasingly are used to run basic automobile functions. The average new car runs 20 computer processors and about 60 megabytes of software code, raising more opportunities for malfunctions. In addition to the threat facing vehicles, the report noted the fastest growing threat last year was phishing -- a method of deceiving computer users into revealing personal information -- and predicted that activity would grow more serious in 2005. (Reuters/CNet.com 8 Feb 2005)

Category 21.4 *SCADA (supervisory control and data acquisition) systems, vehicle controls*

2005-02-13 **software engineering quality assurance QA safety-critical cell-phones mobile Bluetooth virus infection economics damages lawsuits reliability**

RISKS 23 72

INFECTING CARS VIA CELL PHONES -- CONT'D

Peter Ladkin reported on a mild brouhaha about the possibility that Bluetooth-enabled car-control systems might be susceptible to damage from viruses infecting or transmitted via cell-phones. He determined that the original reports (including one in RISKS 23.70) may have been stimulated by a discussion with anti-virus expert Eugene Kaspersky, who discussed _theoretical_ possibilities of infecting car systems in response to specific questions from a reporter.

Ladkin mentioned a cute cartoon he saw in which "A passenger is sitting in an airliner using his laptop, and on the screen appears: Bluetooth: new device found: Airbus A310." He then analyzed the economics of critical failures in automobiles and pointed out how unreliable software tends to be. Given how safety-critical car-control systems are, and given the massive costs of customer damage claims, he commented, "So there is plenty of motivation to make auto critical electronics the most dependable SW-based systems the world has ever seen. We are a long way from it, but I don't think we are going to be seeing critical systems upgraded through gratuitously insecure channels. Except for the exceptions, of course."

He concluded, "If I were to bet today, I'd bet on the cartoon staying a cartoon."

Category 21.4 *SCADA (supervisory control and data acquisition) systems, vehicle controls*

2005-02-14 **quality assurance QA response error tolerance missile interceptor communications failure**

RISKS; http://www.cnn.com/2005/TECH/01/12/missile.defense.ap/index.htm 23 66

MISSILE FAILS TEST? CHANGE THE RULES.

Jeremy Epstein commented on the DoD's response to errors in the missile interceptor system:

As has been widely reported, the DoD's missile interceptor test failed miserably in December [2004], building on a rather impressive history of failures. According to Pentagon brass, the problem was "with an automated pre-launch check of the communications flow between the interceptor and the main flight control computer. Detecting too many missed messages, the system shut down automatically, as designed. [so] the Pentagon will increase the pre-launch tolerance for missed messages. [General] Obering said the tolerance level was set too low; increasing it will not risk a flight guidance failure".

Well, that makes me feel better. The system ran into problems, so it generated errors. Rather than figuring out what the problem was, let's ignore the errors. Not unlike turning up the radio in your car so you can't hear it falling apart.

The general went on to say "Statistically, it's a very rare occurrence and most likely would not happen again."

Gee, I feel safer every minute.

* * *

In RISKS 23.72 he reported on yet another failure:

MISSILE INTERCEPTOR DOESN'T EVEN LEAVE ITS SILO -- AGAIN

As reported in RISKS 23.65 and 23.66, the Dec 15 test of the missile interceptor system failed when it didn't lift off from the launchpad due to a timing problem.

The 14 Feb test didn't do any better. CNN reports that "a spokesman for the [Missile Defense] agency, Rick Lehner, said the early indications was that there was a malfunction with the ground support equipment at the test range on Kwajalein Island in the Marshall Islands, not with the missile interceptor itself. If verified, that would be a relief for program officials because it would mean no new problems had been discovered with the missile."

That's good news?

In case you're keeping score, that's 6 failures out of 9 attempts since the program started. And the three "successes" have been highly scripted.

Your tax dollars at work (at least for Americans).

Category 21.4 *SCADA (supervisory control and data acquisition) systems, vehicle controls*

2005-05-17 **automobile control systems engine failure shutdown speed safety software quality assurance QA**

RISKS; http://tinyurl.com/9u6pt(subscribers only); http://tinyurl.com/dov9m 23 87

SOME PRIUS CARS SHUT DOWN AT SPEED

Peter G. Neumann summarized an article about an upsetting software error:

The U.S. National Highway Transportation Safety Administration has 13 reports of Toyota's Prius gas-electric hybrid cars (2004 and early 2005) stalling or shutting down at highway-driving speeds, which Toyota attributes to software problems.

The original article by Sholnn Freeman from the Wall Stree Journal included this text:

>Toyota spokesman Sam Butto said the auto maker identified a "programming error" in the computer systems of 23,900 Prius cars last year. He said that last May Toyota sent owners of those cars service warnings telling them to go to their dealerships for a software upgrade. But he said he wasn't sure how many people went in to receive the hour-long fix.

He and another Toyota spokesman said the auto maker isn't sure if the latest problems associated with 2004 Prius models involve buyers who never got the upgrade or if an altogether different glitch is shutting the car down.<

Edwin Slonim commented in RISKS:

I have always feared losing power, brakes and steering at high speed - with a helpful dashboard indication of "internal error 687, please reset". Looks like it is starting to happen. Of course we need to put this into proportion - how many cars stall at high speed with a fuel blockage, or swerve with a blowout.

Category 21.4 *SCADA (supervisory control and data acquisition) systems, vehicle controls*

2005-06-23 **denial of service DoS power electricity failure railway paralysis human safety temperature air conditioning single point of failure systems engineering fault tolerance**

RISKS 23 92

SINGLE POINT OF FAILURE PARALYZES SWISS RAILSYSTEM FOR 3 HOURS

On 22 Jun 2005 at 5.08pm, a power short occurred between Amsted (Canton Uri) and Rotkreuz (Canton Zug, which in German means "train") on the Swiss train line. The SBB (Schweizerischen Bundesbahnen) operated their own power lines, and this short circuit caused a sharp drop in voltage, which quickly spread throughout the ENTIRE country of Switzerland.

Trains were stalled in the middle of nowhere, with no air conditioning in the heat of the summer. Some train doors could not be opened. More than 200,000 passengers were affected. It took about two hours to get everyone out of the trains. SBB used busses to transport stranded passengers and diesel locomotives to drag trains to the nearest station.

It took two more hours before enough power was restored in order for the trains to begin moving. But the efficient Swiss worked all night moving trains so that everything moved rather smoothly the next day.

There were allegedly no computers involved, but the single point of failure was a vivid illustration of many RISKS concepts, not the least of which is: don't throw out those diesel locomotives yet!

[Report from Debora Weber-Wulff]

Anthony Thorn added:

>My concern --and arguably the risk-- is the impact of such an incident on passenger trains in the new Gotthard "base"-tunnel which will open in 2011. This will be 57 Km (35 miles) long and run at depths up to 2000 meters (7000 feet) which means that the tunnel temperature will exceed 45 C. (113 F). If a train is stopped in the tunnel a very rapid response would be required to avoid a catastrophe.<

Category 21.4 *SCADA (supervisory control and data acquisition) systems, vehicle controls*

2005-07-06 **supervisory control data acquisition SCADA system failure software quality assurance QA failure bug flaw air pollution human safety health power generator emissions monitor**

RISKS; http://tinyurl.com/dvtga 23 93

SCADA SYSTEM FAILURE CAUSES AIR POLLUTION

Bill Hopkins relays a report from Pennsylvania:

>Our local newspaper reports in print (but not on line) that Exelon Power's Cromby generator in Phoenixville, PA exceeded pollution limits for seven months in 2004 after an unidentified "vendor" programmed an emissions monitor for the wrong standards, and that the company will pay 600 grand. Websites for the company and the PA Dept of Environmental Protection confirm the story. Exelon is the parent company of PECO Energy, formerly Philadelphia Electric Co., which supplies power to the area.

Cromby has two generators, one coal-fired and one switchable between oil and natural gas. The vendor ("a big company" says Exelon) set the monitor for the coal-fired unit to standards for the other unit. (I would guess that the SO2 limits for oil might be higher.) Exelon discovered the problem while aggregating data "for a large use," stopped it and turned itself in. DEP assesses a fine for each day of violation.

Risks for a company: trusting the dials and trusting the vendor when you're on the hook.

Risks for the rest of us: breathing in.<

Category 21.4 *SCADA (supervisory control and data acquisition) systems, vehicle controls*

2005-09-17 **avionics software quality assurance QS glitch error bug flaw disaster control SCADA supervisory control data acquisition**

RISKS; http://tinyurl.com/bkg7d 24 05

SOFTWARE FAILURE HIJACKS MALAYSIAN AIRLINES BOEING 777

The Australian (17 Sep 2005) has a chilling story about the pilots of a Malaysian Airlines 777 flying from Perth to Kuala Lumpur last month battling to regain control after an "unknown computer error" caused the aircraft to pitch violently, and brought it close to stalling.

An Australian Transport Safety Bureau report … released yesterday reveals the pilot in command disconnected the autopilot and lowered the plane's nose to prevent a stall, after incorrect data from a supposedly fail-safe device caused the plane to pitch up and climb 3000ft, cutting its indicated air speed from 500kmh to 292kmh, activating a stall warning and a "stickshaker". [A stickshaker vibrates the aircraft's controls to warn the piot when he is approaching stall speed … which, you know, means the plane is about to fall out of the air.]

The system refused to give up control, however. It increased the power on the automatic throttle, forcing the pilot to counter by pushing the thrust levers to the idle position. The aircraft immediately pitched up again, and climbed 2000ft.

The pilot turned back to Perth under manual control. When he kicked in the two autopilot systems, the plane banked to the right, and the nose pitched down.

On its landing approach, at 3000ft, the flight display gave a low airspeed warning and the auto-throttle increased thrust. The warning system also indicated a dangerous windshear, but the crew landed the jet safely.

According to the report, "investigations are focusing on faulty acceleration figures supplied by a device called the Air Data Inertial Reference Unit". The ADIRU collates aircraft navigation and performance data from other systems and passes the information to the primary flight computer.

What's potentially more disturbing, however -- and neither the Transport Safety Bureau nor The Australian appear to have picked this up -- is that a US FAA directive … in June this year highlighted other problems with the Boeing 777's ADIRU.

Boeing has told operators of the jet -- which by the way has the best safety record of any aircraft … -- to load a previous software version.

[Summary by Charles Wright][

Category 21.4 *SCADA (supervisory control and data acquisition) systems, vehicle controls*

2005-10-18 **automobile control system software engineering design flaw quality assurance QA driving brakes failsafe stupid insane nuts gaga**

RISKS; 24 08
http://www.informationweek.com/story/showArticle.jhtml?articleID=170702055

WHO THINKS OF THESE SYSTEMS? AND WHAT DRUGS ARE THEY ON?

Peter Scott comments on possibly the worst idea in automotive design history:

>Toyota is testing technology meant to keep a driver's eyes on the road, according to The Associated Press. The technology employs a camera attached near the car's steering wheel and image-processing software that recognizes when the driver isn't facing forward. The system flashes a light on the dashboard and beeps when the driver looks away, according to the AP. If the driver doesn't respond, *the brakes are applied automatically*. The feature will be in Lexus luxury models to be sold in Japan next spring.

Well, *that* sounds reliable… I feel safer already.

I hope they paint them a distinctive color so I can recognize them on the road and stay well away…<

Category 21.4 *SCADA (supervisory control and data acquisition) systems, vehicle controls*

2005-11-09 **quality assurance QA fail-safe denial of service DoS safety-critical system design emergency override**

RISKS; http://archiv.tagesspiegel.de/archiv/09.11.2005/2163080.asp (in German) 24 09

FAIL-SAFE DIDN'T: BERLIN TUNNEL TESTS SNARL TRAFFIC

After a night of repairs to one of the autobahn tunnels in Berlin the crew wanted to test the fire alarm system. They tried starting some of the fire alarms, and were worried that the automatic gates that are to keep cars from entering a tunnel with a possible fire weren't closing right. They punched more and more alarms, and the gates on both tunnel tubes (work was going on in only one tube) suddenly banged closed - and the computer regulating them crashed.

The gates failed safe -- but they couldn't be opened again. Not by hand, and not by computer, which just refused to start again. They worked feverishly from 5am to 10am, trying to get the gates open again so that traffic (which is normally very heavy at that time of the morning), could move. [I'm glad I took the train yesterday! -dww]

Police were able to evacuate cars trapped in the tunnel by way of an exit from the tunnel, which was not gated.

A special complication was that the gates on the north end of the tunnel were made by a different company than the gates on the south end of the tunnel, this caused "additional problems". Which ones, are left to the comp.risks readers as an exercise.

It is still not clear how the error happened or why the computer would not re-start, speculation has it that the computer couldn't handle so many fire alarms at the same time.

Moral of the story:

* It was good that the system failed safe.
* It was bad that it did not seem able to handle the number of fire alarms that are installed in the tubes.
* If you have different suppliers for parts, you want to make sure they are still delivering the same stuff.

[Summary by Debora Weber-Wulff]

Category 21.4 *SCADA (supervisory control and data acquisition) systems, vehicle controls*

2006-04-15 **automobile real-time control systems failures problems glitches crashes drive-by-wire**

RISKS; Daily Telegraph http://tinyurl.com/e6668 24 25

RISKS OF DRIVE-BY-WIRE SYSTEMS FOR AUTOMOBILES

In March 2006, British motorist was trapped in his BMW at speeds of 130 mph for 26 minutes when his electronic accelarator linkage jammed at maximum throttle. He called police on his mobile phone and miraculously avoided crashing into any other cars on the heavily-travelled motorway during his terrifying trip up the A1 highway. He flipped the car at a roundabout but walked away uninjured.

Don Norman commented in RISKS,

>Seems that stuck throttles were a continual event with old, mechanical throttles. The electronic throttles have received numerous complaints, but all of the ones I could find were about "unintended acceleration". Doing a web search for "electronic throttle accident" (without the quotes) is quite revealing.

I still don't know enough about this class of potential accidents to offer definitive comment. But from what I can tell, automobile incidents will replace aircraft ones for the RISKS community. The more things change, …

Example:

The National Highway Transportation Safety Administration is investigating complaints that some Toyota Motor Corp. cars may suddenly accelerate or surge, causing one car to strike a pedestrian. The 2002 and 2003 Toyota Camry, Camry Solara and Lexus ES300 vehicles all come equipped with an electronic throttle control system, which the NHTSA said uses sensors to determine how much throttle is being applied.

The NHTSA said 30 crashes have been attributed to the problem, with four accidents resulting in five injuries. The crashes "varied from minor to significant and may have involved other vehicles and/or building structures." The preliminary investigation is the first step in the investigative process. The NHTSA will contact Toyota to ask for documents pertaining to the issue, and could upgrade the investigation to an engineering analysis. More than 1 million Toyotas are covered by this investigation, according to the agency.

Toyota officials could not immediately be reached for comment.<

Category 21.4 *SCADA (supervisory control and data acquisition) systems, vehicle controls*

2006-05-08 **industrial control systems critical infrastructure protection threat national security risk SCADA systems**

DHS IAIP Daily; http://fcw.com/article94273−05−08−06−Print 23

INDUSTRIAL CONTROL SYSTEMS POSE LITTLE-NOTICE SECURITY THREAT.

The electronic control systems that act as the nervous system for all critical infrastructures are insecure and pose disastrous risks to national security, cybersecurity experts warn. Supervisory control and data acquisition and process control systems are two common types of industrial control systems that oversee the operations of everything from nuclear power plants to traffic lights. Their need for a combination of physical security and cybersecurity has largely been ignored, said Scott Borg, director and chief economist at the U.S. Cyber Consequences Unit, an independent research group funded by the Department of Homeland Security. Control systems security is one of six areas of critical vulnerabilities Borg included in a new cybersecurity checklist released in April by the research group. The private-sector owners of critical infrastructure refuse to release data and deny that their aging, inherently insecure systems pose any security risk, said Dragos Ruiu, an information technology security consultant to the U.S. government who runs several hacker conferences. Average hackers can break into the systems, said Robert Graham, chief scientist at Internet Security Systems. He, Borg and other experts fear that major cyberattacks on control systems could have socio-economic effects as severe and far-reaching as Hurricane Katrina.

21.5 Robots, botnets

Category 21.5 *Robots, botnets*

2005-06-15 **robot control failure flaw danger software quality assurance QA**

RISKS; http://tinyurl.com/8c6ct; http://tinyurl.com/cmee5 23 92

WALDO GOES WILD

The Register published this tongue-in-cheek report on a robot gone off its nut:

* Robot runs riot at California hospital *

Staff and patients at San Francisco's UCSF Medical Center were left fearful and shaken last week, when a robotic nurse threw off its shackles and went on the rampage.

"Waldo", a robot used to dispense pills and potions to medical stations at the top notch medical facility, refused to return to the pharmacy to pick up a fresh stash at the end of his rounds, according to the San Francisco Chronicle. Instead, the crazed automaton – reportedly the size of a good-sized TV, which in California means it must be at least the size of the average British garden shed -- careened past the drug depository before barging into a room in the hospital's radiation oncology department where an examination was in progress. The psychotic pill pusher reportedly refused to leave, sending both doctor and patient fleeing for their lives.

"This is the first time anything like this has happened," a hospital spokesman told the paper. "Our technology folks are going to have to take a look." Yeah, if they can find him. The 'bot's clearly gone bad, and is probably even as we speak cruising the city's Tenderloin district pushing purloined prescription pain killers, paying off dirty cops and menacing lost tourists.

Even more worryingly, the spokesman said nothing about shutting down Waldo's two colleagues, dubbed Elvis and Lisa Marie. A terrible accident waiting to happen? We think so.

Category 21.5 *Robots, botnets*

2006-01-20 **computer network botnets difficult trace Symantec Security Response**

DHS IAIP Daily; 23
http://www.techworld.com/security/news/index.cfm?NewsID=5205
&Page=1&pagePos=4&inkc=0

HACKER COMPUTER NETWORKS GETTING HARDER TO FIND.

Hacked computer networks, or botnets, are becoming increasingly difficult to trace as hackers develop new means to hide them, says security experts. Botnets are used to send spam, propagate viruses, and carry out denial of service attacks. Extortion schemes are frequently backed by botnets, and hackers are also renting the use of armadas of computers for illegal purposes through Web advertisements, said Kevin Hogan, senior manager for Symantec Security Response. Three or four years ago, it was easier to connect to botnets and estimate the size of one by noting the number of IP addresses on the network, he said. As legislation emerged cracking down on spammers, those who ran botnets started pursuing more clandestine ways to continue their operations. Rather than deter hardcore spammers, it drove them further underground, said Mark Sunner of MessageLabs. Botnets have an ebb and flow similar to biological behavior, Sunner said. Viruses on an infected computer may download new variants in an attempt to evade anti-virus sweeps. Law enforcement authorities have become more adept at tracking down botnet admins. However, the admins have countered by sticking to smaller groups of around 20,000 machines that are less likely to be detected as quickly, Sunner said.

Category 21.5 *Robots, botnets*

2006-01-23 **hacker guilty plead criminal lawsuit California**

DHS IAIP Daily; 23
http://www.cnn.com/2006/TECH/internet/01/23/hacker.ap/index. Html

BOTNET HACKER PLEADS GUILTY.

A 20-year-old hacker admitted Monday, January 23, to surreptitiously seizing control of thousands of Internet-connected computers, using the zombie network to serve pop-up ads and renting it to people who mounted attacks on Websites and sent out spam. Jeanson James Ancheta, of Downey, CA, pleaded guilty in Los Angeles federal court to four felony charges for crimes, including infecting machines at two U.S. military sites, that earned him more than $61,000, said federal prosecutor James Aquilina. Prosecutors called the case the first to target profits derived from use of "botnets," large numbers of computers that hackers commandeer and marshal for various nefarious deeds. The "zombie" machines' owners are unaware that parasitic programs have been installed on them and are being controlled remotely. Ancheta one-upped his hacking peers by advertising his network of "bots," short for robots, on Internet chat channels. A Website Ancheta maintained included a schedule of prices he charged people who wanted to rent the machines, along with guidelines on how many bots were required to bring down a particular type of Website. Acheta's sentencing is scheduled for May 1.

Category 21.5 *Robots, botnets*

2006-02-08 **McAfee tool anti-bot zombie computer networks Advance Botnet Protection DDoS attacks**

EDUPAGE; 23
http://www.techworld.com/security/news/index.cfm?NewsID=5326&inkc=0

MCAFEE TACKLES BOTS

McAfee has introduced a new tool designed to defend against bots. Most distributed denial-of-service (DDoS) attacks are carried out by networks of computers running automated programs, or bots, that are controlled centrally. So-called botnets typically consist of thousands of computers hijacked by a hacker who can use them to launch DDoS attacks. Most attacks involve bots sending thousands of incomplete packets to the targeted server, which may be overwhelmed by the traffic. Defending against such attacks is difficult because it is not easy to distinguish legitimate traffic from DDoS traffic, and system administrators do not want to inadvertently block legitimate server requests. McAfee said that its new system, called Advanced Botnet Protection, is able to identify traffic that consists of incomplete packets, allowing network operators to separate malicious botnet traffic and avoid DDoS attacks.

Category 21.5 *Robots, botnets*

2006-03-02 **botnet zombie computer network hunt command control malicious hackers**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1933210,00.asp 23

HUNT INTENSIFIES FOR BOTNET COMMAND AND CONTROLS.

A group of high-profile security researchers, which includes international representatives from anti-virus vendors, ISPs, educational institutions and dynamic DNS providers, is ramping up efforts to find and disable the command and control infrastructure that powers millions of zombie drone machines, or bots, hijacked by malicious hackers. The idea is to open up a new reporting mechanism for ISPs and IT administrators to report botnet activity, especially the command and control system that remotely sends instructions to botnets. "If that command-and-control is disabled, all the machines in that botnet become useless to the botmaster. It's an important part of dealing with this problem," said Gadi Evron, a botnet hunter who serves in Israel's Ministry of Finance. Over the last year, the group has done its work quietly on closed, invite-only mailing lists. Now, Evron has launched a public, open mailing list to enlist the general public to help report botnet command and control servers. The new mailing list will serve as a place to discuss detection techniques, report botnets, pass information to the relevant private groups and automatically notify the relevant ISPs of command and control sightings.

Category 21.5 *Robots, botnets*

2006-03-16 **new instant message IM threats botnet networks fraud system FaceTime Security Labs**

DHS IAIP Daily; http://www.finextra.com/fullpr.asp?id=8488 23

FACETIME IDENTIFIES NEW IM BOTNET THREAT.

Research experts at FaceTime Security Labs identified and reported a new threat Thursday, March 16, affecting instant messaging applications. Acting on an anonymous tip, researchers have uncovered two botnet networks that collectively represent up to 150,000 compromised computers, one of which is being used as a vehicle to fraudulently scan desktop and back-end systems to obtain credit card numbers, bank accounts, and personal information, including log-ins and passwords. The operators could potentially launch these scans from any computer on the botnet to mask their actual location. With this new threat, FaceTime has identified more than 40 unique files -- many designed to take advantage of social engineering techniques, stored passwords, auto-complete data and vulnerable payment systems.

Category 21.5 *Robots, botnets*

2006-03-20 **botnet zombie computer network authors phpBB forum attack**

DHS IAIP Daily; http://news.netcraft.com/archives/2006/03/20/bot_authors_targeting_phpbb_forums.html 23

BOT AUTHORS TARGETING PHPBB FORUMS.

A bot by the name of FuntKlakow is registering user accounts on thousands of phpBB forums across the Internet, raising concerns that the bot's authors are laying the groundwork for mass exploitation down the road. FuntKlakow post signatures have included links to proxy surfing and "traffic generator" services, raising the prospect that its goal may be spam rather than exploits.

22.1 DoS attacks

Category 22.1 *DoS attacks*

1997-01-15 **spam flooding denial of service IRC DoS**

Business Wire

Self-named "Reverend White," dedicated to making "America straighter and whiter," launched denial-of-service and harassment attack against the widely-used Internet Relay Chat (IRC) channels called the Undernet. "White" and his cronies emitted forged racist and homophobic hate e-mail, overloaded IRC channels and issued threats against users.

Category 22.1 *DoS attacks*

1997-01-20 **Spam denial of service DoS**

RISKS 18 79

Well-known computer scientist and writer Simson Garfinkel's ISP, VineyardNET, was hijacked by CV Communications on 13 Jan 97. The rogue spammers connected directly to the ISP's SMTP server and sent out 66,000 advertisements for — what cheek — spamming services. Most victims of the spammer were subscribers of CompuServe and AOL. Garfinkel tuned his firewall to reject further input from the rogue to prevent any further abuse and adjusted his two-stage mail delivery software to delete all the junk e-mail already on his system.

Category 22.1 *DoS attacks*

1997-06-16 **hacker anti-spam vandalism information warfare hacktivism**

CNET http://www.news.com/News/Item/0,4,11535,00.html

One or more unknowns calling it/themselves "Bluelister" began attacking critics of unsolicited commercial e-mail by sending large amounts of junk e-mail with forged headers from the host sites where such critics have their e-mail addresses. The resulting floods of messages from outraged recipients, unaware that they are falling into the trap laid by the miscreant(s), frequently bring the ISPs or Web sites down. In addition, at least one case of Web site vandalism was attributed to Bluelister: the NetHomes Web-hosting service went down as a result. An unconfirmed message to some NetHomes subscribers, according to Jeff Pelline of CNET, said "The person allegedly responsible for this is the 'Bluelister,' a hacker who reportedly vandalized the NetHomes system and, according to hacked.net and many Internet sources, has perpetrated many other Internet crimes including harassment, mailbombing, etc."

Category 22.1 *DoS attacks*

1997-09-02 **hacker SYN flooding PING flood ISP denial of service**

Australian

Unknown hackers assailed the Zip Internet ISP in Sydney, Australia using SYN-flooding and PING flooding. The system was unusable during the worst floods, which are thought to be from local assailants. The ISP was working with federal police in an effort to catch the malefactors. Zip and its backbone provider, Connect.com, instituted blocking measures to stem the tide of fraudulent packets.

Category 22.1 *DoS attacks*

1998-10-21 **information warfare DNS domain naming system impersonation**

RISKS, EDUPAGE 20 4

AOL selected low-level security at Network Solutions, thus allowing a vandal to send e-mail that automatically altered the aol.com domain on 16 Oct and sent thousands of e-mail messages to autonet.net. The resulting downtime lasted 12 hours. AOL has about 13 million customers.

Category 22.1 *DoS attacks*

1998-10-28 **spam denial of service e-mail forged header bad address**

Boston Globe

In an unsuccessful denial-of-service attack on the Boston Globe, someone sent out thousands of e-mail messages referring to online pornography. The forged headers named boston.com (the domain belonging to the Boston Globe) as the originating site; the messages were sent to computer-generated e-mail addresses, resulting in thousands of error messages being returned to the e-mail server. Luckily, the servers survived without too much trouble. The FBI was investigating.

Category 22.1 *DoS attacks*

2000-07-03 **criminal hacking denial of service DoS telemetry**

RISKS, BBC 20 93

Peter G. Neumann wrote, "According to the BBC, 3 Jul 2000, a computer hacker endangered shuttle astronauts in 1997 by overloading NASA's communication system after tapping into the NASA system monitoring the astronauts' on-board medical signs while docking with Mir. Apparently, NASA has experienced more than 500,000 cyber attacks in the past year."

In a quick riposte from an alert RISKS reader, the story was debunked by a terse denial from officials at NASA HQ and the Johnson Space Center: "News reports that a computer hacker endangered the lives of Space Shuttle astronauts during a 1997 mission are wrong." Seems there was a brief interruption of medical telemetry by a hacker but no significant effects.

Category 22.1 *DoS attacks*

2000-12-10 **spam unsolicited commercial bulk e-mail UCE denial-of-service attack DoS delay availability bandwidth saturation**

RISKS, InformationWeek http://www.informationweek.com/817/verizon.htm 21 15

In December, 70,000 Verizon ISP customers were significantly slowed (up to several hours) in their access to the Net because of three denial-of-service attacks within two weeks involving millions of unsolicited commercial e-mail ("spam"). Or at least, that's what Verizon _claimed_; however, Steve Wildstrom wrote to RISKS expressing skepticism: "Interestingly, Verizon has failed to come up, at least in public, with any evidence that this was in fact an attack. Given the company's dubious service record, a lot of folks suspect this may be a pretty lame attempt to blame a popular bogeyman for an inability to handle traffic. . . . An attack would almost certainly have involved a large number of messages from a small number of sources and at least the mail relays that the messages were sent through would have been identifiable, if not the ultimate source."

Category 22.1 *DoS attacks*

2001-01-26 **criminal hacker Web vandalism DoS denial of service DNS domain name service colocation**

NewsScan; http://washingtonpost.com/wp-dyn/articles/A47581-2001Jan25.html

NETWORK VANDAL ATTACKS MICROSOFT SITES
Just a day after Microsoft's Web sites were down for an extended period of time because of the "human error" of a technician, they were victimized by the "human malice" of a network vandal who subjected them to a "denial of service" attack that flooded them with bogus communications, causing them to gridlock and reject legitimate communications from their customers. The company has called in the FBI for assistance. Computer security expert Abe Singer of the San Diego Supercomputer Center said that part of Microsoft's vulnerability to attack was due to the fact that its four domain-name servers are linked in a single network. "They had all their eggs in one basket and basically someone knocked down the basket." (Washington Post 26 Jan 2001)
http://washingtonpost.com/wp-dyn/articles/A47581-2001Jan25.html

---

Category 22.1 *DoS attacks*

2001-02-16 **denial of service bandwidth saturation SMS short message service mobile phone Thailand**

Reuters; http://www.joeha.com/wbnfeb162001.htm

Thailand's biggest mobile phone network crashed on Valentine's Day [2001] as thousands of young lovers sent romantic messages to their sweethearts. . . . Advanced Info Service (AIS) said the company's GSM network was flooded with more than 100,000 text messages sent within an hour via mobile phones Wednesday. The deluge of messages paralyzed the short message service (SMS) network, blocking all voice calls. AIS has a capacity for just 72,000 SMS messages per hour.

"The volume of messages sent from mobile phones this Valentine's Day was the highest volume ever -- twice as big as the message traffic sent on New Year's Eve," Wichian Mektrakarn, vice president of AIS's engineering operation, told Reuters. Wichian said many young Thais preferred to send Valentines by SMS because they were too shy to voice their feelings. "Clicking out sweet nothings on the phone is much easier than uttering words, which some still find it difficult to do," he said.

Category 22.1 *DoS attacks*

2001-05-24 **DoS denial-of-service attack routine ho-hum yawn**

NewsScan; http://www.usatoday.com/life/cyber/tech/2001-05-24-cert-hacked.htm

CERT SUBJECTED TO "JUST ANOTHER ATTACK"
The Web site of the federally funded Computer Emergency Response Team (CERT) was clogged by a "denial of service" attack that lasted 30 hours this week. CERT, which is located at Carnegie Mellon University in Pittsburgh, has a mission of providing warnings about computer attacks and viruses. An official of the organization said: "We get attacked every day. This is just another attack. The lesson to be learned here is that no one is immune to these kinds of attacks. They cause operational problems, and it takes time to deal with them." (AP/USA Today, 24 May 2001)
http://www.usatoday.com/life/cyber/tech/2001-05-24-cert-hacked.htm

---

Category 22.1 *DoS attacks*

2001-10-31 **DoS denial of service bandwidth saturation**

NewsScan

DENIAL OF SERVICE ATTACK ON NEW YORK TIMES
Although the company's Web site was unaffected, the New York Times experienced a "huge amount of electronic transmissions on Tuesday" that disrupted operations and denied Times employees access to the Internet for several hours. The company's network administrator says the Times does not know whether or not the "storm of data" it received was sent maliciously, but that "there seems to be no innocent explanation" and that it appears to have been a "deliberate attack." (AP/Washington Post 31 Oct 2001)
http://www.washingtonpost.com/wp-dyn/articles/A16398-2001Oct31.html

---

Category 22.1 *DoS attacks*

2002-01-24 **information warfare DoS denial-of-service attack disaster ISP Internet service provider bankruptcy**

Security Wire Digest; ZDNet News < http://news.zdnet.com/2102-1009_22-820708.html?tag=printthis > 4 6

NO SILVER LINING FOR CLOUD NINE
Citing "a brazen act of cyberterrorism" U.K.-based ISP Cloud Nine ceased operations this week after being hit by a crippling denial-of-service attack. The network needs to be rebuilt as a result of the attack and the company's insurance won't cover the repairs. So, the ISP will either be sold or placed in the hands of administrators, CEO Emeric Miszti said in published reports. Cloud Nine's clients will likely be acquired by ISP V21.

Category 22.1 *DoS attacks*

2002-04-04 **DoS denial-of-service attack malformed packet PKC public key cryptosystem IPSec bug flaw design QA quality assurance**

Security Wire Digest 4 26

The OpenBSD ISAKMPD IPSec keying daemon was found to have a design flaw that allowed a denial-of-service attack through malformed packets. A patch was quickly issues. However, Kurt Seifried of Security Wire Digest pointed out that the test suites used for quality assurance in public key cryptography tend not to include the possibilities of DoS attacks.

Category 22.1 *DoS attacks*

2002-04-25 **malformed packets DoS denial-of-service attack BSOD blue screen of death kernel panic Windows 2000 endless loop default settings TCP/IP**

Security Wire Digest 4 32

PORT 445 ATTACK COULD CAUSE DoS
By Shawna McAlearney

Security researchers are warning users to change default registry settings on Windows 2000 boxes to prevent denial-of-service (DoS) attacks through TCP port 445.

Researcher Peter Grundl of KPMG Denmark says that sending malformed packets to the Microsoft-ds port (TCP 445) can result in kernel resources being allocated by the LAN Manager service, which manages domain access. The consequences of such an attack could vary, from the Windows 2000 host ignoring the attack to users finding the dreaded blue screen of death. Experts say the impact of the attack would likely depend upon which services were running.

Targeting the Windows 2000 Server/Advanced Server/Professional, Grundl says: "An attack could be something as simple as sending a continuous stream of 10K null characters to TCP port 445." According to the advisory, this attack will cause the system service to enter a state where it constantly uses 100 percent of CPU resources.

"Port 445 attacks are a recurring problem for users of Windows 2000," says Steve Gibson, president of Gibson Research Corp. "Luckily, any NAT or firewall will protect against the whole class of port 445 vulnerabilities."

Microsoft says it has confirmed this is a problem. The software giant recommends concerned users follow the Registry Editor instructions provided on its Web site, but warns that using the Editor incorrectly can cause serious problems that may not be fixable.

http://support.microsoft.com/default.aspx?scid=kb;en-us;Q320751

Category 22.1 *DoS attacks*

2002-05-05 **DoS denial of service government information warfare**

NIPC Daily Report

The White House Web site reportedly suffered a brief but crippling denial of service attack that rendered the site inaccessible to users on 4 May. White House spokesperson Jimmy Orr confirmed that the White House site was rendered inaccessible due to a "denial of service" in the morning hours between 9 a.m. and 11:15 a.m. EDT. [Spokespersons could not attribute the denial of] service to an orchestrated attack, but did confirm that the White House was "looking into" the possible causes of the of the shutdown. Technicians were able to "unclog the clog" between Whitehouse.gov and its Internet service provider, making the site accessible to the general public. At no point did any malicious data reach White House servers. Security experts believe the Whitehouse.gov shutdown to be linked to the spate of Web site hacks and defacements launched by Chinese and pro-Chinese Internet vandals over the past few days. (Source: Newsbytes, 5 May)

Category 22.1 *DoS attacks*

2002-08-07 **infowar information warfare international attack Internet denial-of-service DoS ISP Internet service providers**

NewsScan

FAILED ATTACKS ON INTERNET
Attacks on U.S. Internet providers Tuesday morning [Aug 6] turned out to be just a blip on the screen. Bush Administration cybersecurity chief Richard Clarke described the attacks -- which were thought to have come from someplace in Western Europe -- as amounting to not much more than an "unusual" event: "There was a real spike in Internet traffic at odd hours. It was clearly unusual because it was five times and seven times normal, but it didn't take anything down." Internet monitoring group Matrix NetSystems detected a 1% decrease in Internet accessibility within the hours of the attacks, but most U.S. systems managers say the attacks were barely noticeable and caused no damage. (AP/New York Times 6 Aug 2002)
http://www.nytimes.com/2002/08/07/technology/07HACK.htm

Category 22.1 *DoS attacks*

2002-10-23 **criminal hackers attack denial-of-service DoS DNS Domain Name System root servers**

NewsScan

HACKER ATTACK TARGETS ROOT SERVERS
A powerful denial-of-service attack briefly crippled nine of the 13 Internet "root" servers, but traffic routing was able to continue unimpeded, said ICANN VP Louis Touton: "As best we can tell, no user noticed and the attack was dealt with and life goes on." One government official described Monday's attack as the most sophisticated and large-scale assault on these root servers to date. The attack, which began around 4:45 p.m. EDT on Monday, blasted the servers with 30 to 40 times the normal amount of messages, rendering seven computers unable to respond to legitimate Internet traffic. Two others failed intermittently during the attack. The Internet theoretically can run with just one operational root server, but response times would be very slow. (AP 23 Oct 2002)
http://apnews.excite.com/article/20021023/D7MR8PT00.htm

Category 22.1 *DoS attacks*

2002-11-06 **DNS Domain Name System root servers vulnerabilities attacks protection**

NewsScan

VERISIGN TAKES STEPS TO PROTECT ROOT SERVERS
Verisign has taken steps to protect the two root servers that it controls, following last month's attack that briefly crippled nine of the 13 computer servers that manage global Internet traffic. The company says it moved one of its computers to a different building in an unspecified location in northern Virginia and onto a different part of its network. Verisign says the change is designed to ensure that a hardware outage or focused attack targeting part of its network could not disrupt both servers. FBI Director Robert Mueller said last week that the October 21 attacks have been traced back to hacked computers in South Korea and the U.S. (AP/Los Angeles Times 6 Nov 2002)

Category 22.1 *DoS attacks*

2003-01-15 **denial-of-service attack DoS saturation e-mail fraud**

NewsScan

UNIVERSITY BOMBARDED WITH FAKE MESSAGES
Campus police at Ohio State University are evaluating charges against an individual they think is responsible for bombarding the university's computer network last month with 11 million phony e-mail messages over a several-day period, crippling Internet access and delaying e-mail distribution for days. The police have not disclosed the content of the messages, nor identified the suspect, who may be facing charges of illegal tampering with records, theft, unauthorized use of a computer system, and vandalism. (AP/USA Today 15 Jan 2003)

Category 22.1 *DoS attacks*

2003-03-26 **news Iraq war Al-Jazeera denial-of-service hack attack**

NIPC/DHS

March 25, Associated Press — Al-Jazeera site experiences hack attack.

Hackers attacked the Web site of Arab satellite television network Al-Jazeera on Tuesday, rendering it intermittently unavailable, the site's host said. The newly launched English-language page, which went live Monday, was hardest hit in a bombardment of data packets known as a denial-of-service attack. Ayman Arrashid, Internet system administrator at the Horizons Media and Information Services, the site's Web host, said the attack began Tuesday morning local time. The Web host is based in the Persian Gulf state of Qatar. The servers that host the Al-Jazeera site are in France and the United States. Only the U.S. servers were under attack, said Arrashid, so the attackers were likely in the United States. He said technicians were working to thwart the attack, but could not estimate when the site would be fully available again.

Category 22.1 *DoS attacks*

2003-05-15 **denial service attack hole kernel Linux DoS Secunia Red Hat hash collisions spoofed source address 400 packets per sencond**

NIPC/DHS

May 15, internetnews.com — DOS hole found in Linux Kernel.

Security experts Thursday warned of a vulnerability in the Linux Kernel 2.4 branch, which can be exploited to cause denial-of-service (DOS) attacks. "By flooding a Linux system with packets with spoofed source addresses, the handling of the cache will consume large amounts of CPU power. This could potentially bring a Linux system offline with a rate of only 400 packets per second by using carefully chosen source addresses that causes hash collisions in the table," according to a security advisory from computer security firm Secunia. Secunia rated the flaw as "moderately critical" and cautioned that it could be exploited to bring a Linux system offline with a rate of only 400 packets per second by using carefully chosen source addresses that causes hash collisions in the table. Red Hat has issued updated kernel packages to patch Red Hat Linux versions 7.1 through 9: http://rhn.redhat.com/errata/RHSA-2003-172.html.

Category 22.1 *DoS attacks*

2003-06-02 **net attack computers Dan Wallach Scott Crosby internet hash functions offline packets process power Rice University Houston Texas**

NIPC/DHS

June 02, New Scientist — Net attack overwhelms computers with complexity.

Dan Wallach and Scott Crosby, researchers at Rice University in Houston, TX, have found an Internet attack that can knock a web-connected computer offline using specially crafted packets of data. Many programs perform small calculations - called hash functions - on substantial amounts of data to make it easier to sort through. Tables of hashed information can then be referred to, to check that information has not been corrupted or lost en route. Wallach and Crosby calculated that some data would force a program to perform the most intensive hash calculations possible. They tested a number of commercial computer programs and found that sending these types of packets could use up nearly all of a computer's processing power, preventing it from carrying out normal tasks. Wallach and Crosby were able to disrupt target computer program using just a dial-up modem connection. The only way to defend against the attack is to use more efficient, better designed hashing algorithms. A paper outlining the attack will be presented in August at the Usenix Security Symposium in Washington D.C.

Category 22.1 *DoS attacks*

2003-12-11 **SCO Group denial-of-service hacker attack Linux Unix**

NIPC/DHS

December 10, Dow Jones Business News — SCO Group Website disabled by another hacker attack.

The Website of SCO Group Inc. has been temporarily disabled by a hacker attack that began early Wednesday, December 10, the company said. It marks the third time this year the Lindon, UT, software firm's site has been the target of a "denial of service" attack. In such assaults, hackers bombard an Internet site with traffic in an attempt to overwhelm its server computers and shut it down. The latest attack began at 6:20 a.m. EST, and it isn't clear when it will cease, said SCO spokesman Blake Stowell. Past attacks against the company's site have lasted for several days. Stowell said the company has notified law-enforcement authorities. The attack is preventing SCO customers from downloading updates or security fixes to their software.

Category 22.1 *DoS attacks*

2004-01-14 **patch flaw vulnerability fix Sun ONE buffer overflow denial of service DoS**

DHS/IAIP Update

BUFFER OVERFLOW PLUGGED IN SUN ONE WEB SERVER.

Sun Microsystems on Monday, January 12, warned of a buffer overflow vulnerability in its Sun ONE/iPlanet Web Server product. The firm said the flaw could be exploited by a remote user to crash the Web server, which is a type of denial-of-service attack. Independent research firm Secunia has rated the security hole as "moderately critical." The vulnerability affects the Sun ONE/iPlanet Web Server 6.0 Service Pack 5 and earlier versions on the HP-UX platform. Sun has issued a new service pack to fix the flaw, noting that there are no workarounds. The susceptible products are a crucial part of Sun's Web services initiative which falls under Sun Open Net Environment (Sun ONE) brand. The Sun ONE brand includes the Sun ONE Web Server, Sun ONE Portal Server, Sun ONE Application Server, Sun ONE Directory Server, Sun ONE Identity Server, Sun ONE Messaging Server and the Sun ONE Integration Server (all formerly iPlanet products). A service pack is available online: http://wwws.sun.com/software/download/products/3f186391.html

---

Category 22.1 DoS attacks

2004-01-26 **computer network vulnerability Internet security**

NIPC/DHS; http://news.com.com/2100−7355_3−5145863.html?tag=nefd_top

January 22, CNET News.com — Security pros question flaw find.

Two Internet software developers who said they have uncovered a way to cause entire networks of computers to freeze or shut down may have simply rediscovered an old network issue. The network performance issues are described in a series of Web site forum postings recently publicized within the security community. The poster, who uses the alias NT Canuck, said he created a tool, with the help of another developer, that can shut down entire networks. However, security researchers at the Computer Emergency Response Team (CERT) Coordination Center downplayed the issue, saying that the program simply inundates a network with so much data that computers have problems functioning correctly. "We don't see any specific vulnerability being discovered here," said Jason Rafail, an Internet security analyst at the center. According to the Web posts, the programmers found that certain circumstances could be created that would cause a network of computers to freeze, and in some cases fail. The developers contacted Microsoft and the CERT Coordination Center; both organizations confirmed that they were contacted in November. However, Microsoft's Security Response Center (MSRC) has not been able to replicate the discoverers' exact findings, said Stephen Toulouse, senior program manager for the MSRC.

Category 22.1 DoS attacks

2004-02-03 **denial-of-service DoS attack virus work network SCO MyDoom sco.com**

NewsScan

SCO SCRAMBLES TO LAUNCH NEW WEB SITE FOLLOWING ATTACK

SCO Group, which saw its Web site taken out by the MyDoom computer worm, launched a new Web site yesterday (www.thescogroup.com), which will serve as its temporary Web site until the worm's barrage against www.sco.com slacks off. "We expect hundreds of thousands of attacks on www.sco.com because of these viruses. Starting on Feb. 1 and running through Feb. 12, SCO has developed layers of contingency plans to communicate with customers, resellers, developers, partners and shareholders," said the company in a statement. The virulence of the MyDoom worm sent a shudder through the Internet security community. "With such a program you could really take out any major Web site on the Internet," says Raimund Genes, European president of security firm Trend Micro. (Reuters/New York Times 3 Feb 2004)

Category 22.1 DoS attacks

2004-03-19 **vulnerability flaw hole patch fix OpenSSL SSL TLS Internet e-commerce security**

DHS IAIP Daily;

March 18, vnunet.com — OpenSSL patches denial of service flaws.

The OpenSSL Project issued patches Wednesday, March 17, to fix two flaws that could leave secure servers open to denial of service (DoS) attacks. An advisory posted on the site warned that both vulnerabilities could allow a remote attacker, using a carefully crafted Secure Sockets Layer (SSL)/Transport Layer Security (TLS) handshake against a server using the OpenSSL library, to cause OpenSSL to crash. Depending on the application this could lead to a DoS. These vulnerabilities have been fixed in OpenSSL 0.9.6m and 0.9.7d, available from the project's Website: http://www.openssl.org/

Category 22.1 DoS attacks

2004-04-19 **ColdFusion MX Macromedia denial-of-service DoS vulnerability patch**

DHS IAIP Daily; http://www.esecurityplanet.com/trends/article.php/3342061

April 19, eSecurity Planet — ColdFusion MX DoS vulnerability patched.

Graphics design software specialist Macromedia has rolled out a fix for a denial-of-service vulnerability found in its ColdFusion MX 6.1 product suite. The firm said the flaw affected all editions of ColdFusion MX 6.1 and all versions of ColdFusion MX 6.1 J2EE. Macromedia tagged the issue as "important" and recommended that users apply the accompanying patch immediately. ColdFusion MX, formerly known as "Neo," is a key part of Macromedia MX, an integrated collection of tool, server and client technologies developed to function as a single environment. But, security bugs have followed the product around with the latest centering around the way ColdFusion MX handles file uploads. "When file uploads to ColdFusion MX via an HTML form are started, but are interrupted before they complete - disk space on the server may not be reclaimed when the ColdFusion MX template finishes processing," the company explained.

Category 22.1 *DoS attacks*

2004-06-15 **network attack vandalism Websites down denial-of-service Akamai**

NewsScan

ATTACK KNOCKS MAJOR SITES OFFLINE

An attack this week by network vandals struck Akamai Technologies, which provides data services for Microsoft, Yahoo, Federal Express, Xerox, the FBI and other major organizations; the attack brought down many of the world's most-visited Web sites for about 45 minutes. An Akamai executive says the company has "no reason to believe that the attack was directed solely at Akamai." The company manages approximately 15% of the traffic on the Internet. (Washington Post 15 Jun 2004)

Category 22.1 *DoS attacks*

2004-08-24 **Symantec security product vulnerabilities denial of service DoS**

DHS IAIP Daily; http://secunia.com/advisories/12371/

August 24, Secunia — Symantec multiple products ISAKMPd denial of service vulnerability.

A Denial of Service (DoS) vulnerability exists in multiple Symantec products due to an unspecified error within the isakmpd service. Mulitple platforms are affected for VelociRaptor 1.5, Gateway Security 1.0 and 2.0, and Enterprise Firewall/VPN 7.0 and 7.0.4. Vendor updates are available: http://secunia.com/advisories/12371/

Category 22.1 *DoS attacks*

2004-08-25 **denial-of-service DoS attack Novell Bordermanager VPN service**

DHS IAIP Daily; http://www.kb.cert.org/vuls/id/432097

August 25, US-CERT — Vulnerability Note VU#432097: Novell Bordermanager VPN Service denial of service vulnerability.

A Denial of Service (DoS) vulnerability exists in the Novell Bordermanager VPN service that could cause an affected device to crash. The Novell Bordermanager product includes Virtual Private Network (VPN) capabilities, including support for the standard Internet Key Exchange (IKE) protocol. A flaw exists in the way the VPN service handles certain malformed IKE packets which creates a remotely exploitable Denial of Service vulnerability. A vendor solution is available: http://support.novell.com/cgi-bin/search/searchtid.cgi?/1009 3576.htm

---

Category 22.1 *DoS attacks*

2004-08-31 **WS_FTP file transfer protocol server application denial of service DoS vulnerability anonymous usage**

DHS IAIP Daily; http://secunia.com/advisories/12406/

August 31, Secunia — WS_FTP server file path parsing denial of service vulnerability.

According to Secunia Advisory SA12406, vulnerability exists in WS_FTP Server version 5.0.2, which can be exploited by malicious users to cause a DoS (Denial of Service). The problem is caused due to an error in the parsing of file paths and can be exploited to cause a vulnerable system to use a large amount of CPU resources. Successful exploitation requires that the user has been authenticated. There is no vendor solution available at this time. As a workaround, restrict access to the FTP server and disallow anonymous usage.

Category 22.1 *DoS attacks*

2004-09-02 **HP Systems Insight Manager user login denial of service DoS Microsoft security patch update issued**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Sep/1011141.html

September 02, SecurityTracker — HP Systems Insight Manager may not let users login after applying a Microsoft security patch.

The Microsoft security fix described in Microsoft security bulletin MS04-025 prevents users from logging in to HP Systems Insight Manager with Internet Explorer. This issue appears to be more of an incompatibility issue, rather than a security vulnerability. The vendor has issued a fix, available at: http://h18013.www1.hp.com/products/servers/management/hpsim/index.html?jumpid=go/hpsim

---

Category 22.1 DoS attacks

2004-09-06 **gnubiff POP3 mail server buffer overflow denial of service DoS vulnerabilities**

DHS IAIP Daily; http://secunia.com/advisories/12445/

September 06, Secunia — gnubiff POP3 buffer overflow and denial of service vulnerabilities.

Two vulnerabilities exist in gnubiff, which potentially can be exploited to cause a DoS (Denial of Service) or compromise a vulnerable system. An unspecified boundary error exists within the POP3 functionality. This can be exploited to cause a buffer overflow and may potentially allow execution of arbitrary code. Update to version 2.0.0 or later: http://sourceforge.net/project/showfiles.php?group_id=94176

Category 22.1 DoS attacks

2004-11-05 **Symantec LiveUpdate ZIP decompression denial of service DoS no update issued**

DHS IAIP Daily; http://securitytracker.com/alerts/2004/Nov/1012095.html

November 05, SecurityTracker — Symantec LiveUpdate zip decompression routine may let users deny service.

The LiveUpdate decompression routine does not check for uncompressed file sizes before attempting to decompress a downloaded LiveUpdate zip file and does not properly validate directory names before creating the directories on the target system. A user can replace a downloaded zip archive (or spoof the Symantec site) and can cause denial of service conditions if the zip archive is crafted to contain an overly large file. There is no solution at this time

---

Category 22.1 DoS attacks

2005-02-24 **Japanese government Website attack denial of service DoS**

DHS IAIP Daily; http://www.nytimes.com/aponline/technology/AP−Japan−Cyber−At tack.html?

JAPANESE GOVERNMENT HIT BY CYBER ATTACKS

A series of cyber attacks disrupted Japanese government computer networks this week, although no damage was reported, Japan's top government spokesperson said Thursday, February 24. The attacks, three times each on Tuesday and Wednesday, targeted the Prime Minister's Office and the Cabinet Office, causing computers to freeze up under a deluge of data and made it impossible for anyone to access the two Websites, Chief Cabinet Secretary Hiroyuki Hosoda said. There was no significant damage, since the attacks were not designed to destroy key programs, and the government networks have since returned to normal operations, he said. Officials are investigating who launched the attack, but having trouble tracking the data. "We don't know whether the attack came from inside or outside the country," Hosoda said.

Category 22.1 DoS attacks

2005-05-02 **Mtp Target software denial of service DoS vulnerabilities no update issued**

DHS IAIP Daily; http://secunia.com/advisories/15195/

MTP TARGET FORMAT STRING AND DENIAL OF SERVICE VULNERABILITIES

Two vulnerabilities in Mtp Target, which can be exploited to malicious people to cause a DoS (Denial of Service) or compromise a user's system. A format string error in the client code when displaying messages from other users can be exploited to execute arbitrary code on a user's system. A signed error in the server code can be exploited by a client to crash the game via a specially crafted parameter. There is no solution at this time.

Category 22.1 DoS attacks

2005-10-15 **denial of service DoS SMS cellular mobile phone**

Cryptogram

SMS CAUSES A MESS

Bruce Schneier writes:
Turns out you can jam cell phones with SMS messages. Text messages are transmitted on the same channel that is used to set up voice calls, so if you flood the network with one, then the other can't happen. The researchers believe that sending 165 text messages a second is enough to disrupt all the cell phones in Manhattan.

Category 22.1 DoS attacks

2006-01-13 **denial of service DoS attack Million Dollar Homepage botnet**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/content/article/2006/01 /13/AR2006011300210.html 23

MILLION DOLLAR HOMEPAGE TARGETED IN HUGE DENIAL OF SERVICE ATTACK

The Million Dollar Homepage, an ad gimmick created by British college student Alex Tew that brought more than $1 million to its 21-year-old creator, was under a massive denial of service attack Friday, January 13, the Website's hosting company said. Tens of thousands of computers controlled by an unknown group or person overwhelmed the site's servers with requests. The site was up Friday due to the voluntary efforts of the hosting company, InfoRelay Online Systems Inc. Tew drew international attention when his September idea to sell a million pixels on his homepage for a $1 each to advertisers took off. The attack stemmed from a network of computers, called a botnet, that were infected with Trojans or other malicious software distributed over the Internet, Russell Weiss, vice president of technical services for InfoRelay, said. The attack started Wednesday night, January 11, growing by early Thursday, January 12, into a zombie army of possibly as many as 100,000 computers from all over the world, Weiss said. Weiss did not know where the attack originated, or whether it was part of an extortion scheme.

Category 22.1 DoS attacks

2006-03-08 **Xerox WorkCenter Pro PostScript processing error denial-of-service DoS vulnerabilities solution update**

DHS IAIP Daily; http://securitytracker.com/alerts/2006/Mar/1015738.html 23

XEROX WORKCENTER PRO MULTIPLE POSTSCRIPT PROCESSING ERRORS LET REMOTE USERS DENY SERVICE.

Several vulnerabilities were reported in Xerox WorkCenter Pro and Xerox CopyCenter. A remote user can cause denial-of-service conditions. Analysis: A remote user can send a specially crafted PostScript file to the target printer to trigger a buffer overflow in the PostScript file interpreter code and cause denial-of-service conditions on the target system. In addition, a remote user can send a specially crafted PostScript file to traverse the directory and cause denial-of-service conditions on the target system. A remote user can also send a specially crafted PostScript file designed to expose TCP/IP ports to cause denial-of-service conditions on the target system. Additionally, a remote user can trigger a memory error in the Web server code to cause denial-of-service conditions. An unspecified vulnerability exists in the ESS/Network Controller. A user may be able to disconnect power to cause Immediate Image Overwrite to fail without indication. Vulnerable products: The WorkCenter Pro 65, 75, and 90 models and the CopyCenter C65, C75, and C90 models are affected. Solution: The vendor has issued a fixed version (1.001.02.074). This security bulletin supersedes Security Bulletin XRX04-008. The vendor's advisory is available at: http://www.xerox.com/downloads/usa/en/c/cert_XRX06_002.pdf

---

Category 22.1 DoS attacks

2006-03-09 **Sun Solaris denial-of-service vulnerability system hang panic fixes release**

DHS IAIP Daily; http://www.securityfocus.com/bid/16966/references 23

SUN SOLARIS PROC FILESYSTEM PAGEDATA SUBSYSTEM LOCAL DENIAL-OF-SERVICE VULNERABILITY.

A security vulnerability involving the "Pagedata" Subsystem of the Process File System (/proc(4)) may cause the system to hang or panic. Analysis: A local unprivileged user may be able to cause significant performance degradation, hang the system, or panic the system, resulting in a denial-of-service condition. This is due to a security vulnerability involving the Pagedata Subsystem of the process file system "/proc." Vulnerable: Sun Solaris 10.0 _x86; Sun Solaris 10.0; Sun Solaris 9.0 _x86; Sun Solaris 9.0; Sun Solaris 8.0 _x86; Sun Solaris 8.0. Solution: Sun has released an advisory including fixes to address this issue. For more information: http://www.securityfocus.com/bid/16966/solution

---

Category 22.1 DoS attacks

2006-03-22 **Microsoft ASP.NET COM W3WP remote denial-of-service DoS vulnerability**

DHS IAIP Daily; http://www.securityfocus.com/bid/17188/references 23

MICROSOFT ASP.NET COM COMPONENTS W3WP REMOTE DENIAL-OF-SERVICE VULNERABILITY.

Improper access of COM and COM+ components in ASP.NET applications can cause a denial-of-service condition in 'w3wp.exe' processes. Analysis: A remote attacker can exploit this issue to cause denial-of-service conditions in applications using improperly coded ASP.NET, effectively denying service to legitimate users. Vulnerable: Microsoft ASP.NET 1.1 SP1; Microsoft ASP.NET 1.1; Microsoft ASP.NET 1.0 SP2; Microsoft ASP.NET 1.0 SP1; Microsoft ASP.NET 1.0; Microsoft ASP.NET. Solution details: http://www.securityfocus.com/bid/17188/solution

---

Category 22.1 DoS attacks

2006-03-27 **Microsoft Office XP array index denial-of-service DoS vulnerability**

DHS IAIP Daily; http://www.securityfocus.com/bid/17252/references 23

MICROSOFT OFFICE XP ARRAY INDEX DENIAL-OF-SERVICE VULNERABILITY.

Microsoft Office is prone to a denial-of-service condition when handling malformed array indices. Analysis: When an Office application such as Excel, Word, or PowerPoint tries to open a file containing a malformed array index, an exception will be thrown, causing the application to fail. For a complete list of vulnerable products: http://www.securityfocus.com/bid/17252/info Solution: Currently, Security Focus is not aware of any vendor-supplied patches for this issue.

Category 22.1 DoS attacks

2006-04-19 **Cisco IOS MPLS denial-of-service DoS vulnerability solution advisory**

DHS IAIP Daily; http://www.securityfocus.com/bid/17607/discuss 23

CISCO IOS XR MPLS DENIAL-OF-SERVICE VULNERABILITY.

Multiple Multi Protocol Label Switching (MPLS) related vulnerabilities exist on Cisco IOS XR. Only systems that are running Cisco IOS XR and configured for MPLS are affected by these vulnerabilities. Analysis: Upon successful exploitation a Modular Services Card (MSC) on a Cisco Carrier Routing System 1 or a Line Card on a Cisco 12000 series router may reload affecting switched traffic. A successful attack results in a denial-of-service condition for traffic that is being switched on an affected MSC or line card. Vulnerable: Cisco IOS XR for PRP 3.2.3; Cisco IOS XR for CRS-1 3.2.3; Cisco IOS XR 3.2.50; Cisco IOS XR 3.2.4; Cisco IOS XR 3.2.4; Cisco IOS XR 3.2.2; Cisco IOS XR 3.2.1; Cisco IOS XR 3.2. Cisco IOS XR 3.3.0 is not vulnerable to this issue. Solution: Cisco has released an advisory to address this issue: http://www.securityfocus.com/archive/1/431359

Category 22.1 DoS attacks

2006-05-03 **massive denial-of-service DoS TypePad LiveJournal blogging software attacks**

DHS IAIP Daily; http://www.techweb.com/wire/security/187200053 23

MASSIVE DOS ATTACK KNOCKS TYPEPAD, LIVEJOURNAL BLOGS OFFLINE.

Millions of blogs hosted by LiveJournal and TypePad were unavailable throughout Tuesday night, May 2, and into Wednesday morning, May 3, as a massive denial-of-service attack struck their servers. The attack that brought down the servers at Six Apart -- the San Francisco company behind the LiveJournal and TypePad services, and the Moveable Type blogging software -- began at 4 p.m. PDT Tuesday, according to an advisory posted to the firm's Website by Michael Sippey, the vice president of product. According to Sippey, service was interrupted for the following: TypePad, LiveJournal, TypeKey, sixapart.com, movabletype.org and movabletype.com.

22.2 DDoS attacks

Category 22.2 DDoS attacks

1998-03-04 **denial of service Microsoft Windows NT patches update hacker**

Newsbytes

All across the US, system administrators found their Windows NT servers under apparently automated attack. Systems crashed repeatedly until they were updated to the latest patches from Microsoft. There appeared to be no file damage from the attacks, which lasted more than a day. Sites affected included
Carnegie Mellon University (OH)
Massachusetts Institute of Technology
NASA Goddard Space Flight Center (MD)
NASA Dryden Flight Research Center (CA)
NASA Independent Validation and Verification Facility (WV)
NASA Jet Propulsion Laboratory (CA)
NASA Wallops Flight Facility (VA)
NASA Stennis Space Center (MS)
NASA White Sands Test Facility (NM)
NASA Headquarters in Washington (DC)
NASA Langley Research Center (VA)
NASA Ames Research Center (CA)
NASA Marshall Space Flight Center (AL)
NASA Moffett Federal Airfield (CA)
NASA Kennedy Space Center (FL)
NASA Lewis Research Center (OH)
Northwestern University
University of California San Diego
University of California Los Angeles
University of Minnesota
University of California campuses in Berkeley
University of California Irvine
US Navy (unclassified servers)

Category 22.2 DDoS attacks

1999-01-15 **denial of service attack smurf e-mail saturation ISP Internet Service Provider**

RISKS 20 16

According to an article by Tim Barlass in the Daily Telegraph of Australia (12 Jan 1999, p. 9), someone launched a sustained Smurf denial-of-service attack on Ozemail, an important Australian Internet service provider. E-mail service has been disrupted for users in Sydney. A company spokesperson said they were trying to track down the perpetrator and were considering installing filtering software to prevent future attacks.

[Note from MK: a "Smurf" attack uses widely-available software written by criminal hackers to send ping packets with forged origination in the headers to a (usually major) corporate network's broadcast address. Every device — perhaps hundreds or thousands — sends a reply packet to the forged originator address. That system thus receives a flood of packets, often overloading its TCP/IP stacks and resulting in denial of service. See the article by Michael Dillon in ASK THE INFRA EXPERT (Internet World: Apr 20, 1998) for a more detailed explanation.]

Category 22.2 DDoS attacks

1999-12-07 **criminal hackers distributed denial-of-service attacks tools DDoS master slave**

Newsbytes

In August 1999, a new breed of automated attack tools surfaced in the computer underground. Trin00 and TFN were used to install slave programs on unprotected computers using Trojans to insert the unauthorized code. These slave programs, once loaded, wait passively for encrypted instructions from a master program. The slaves can then bombard a specific victim with a flood of spurious communications, causing a denial of service. Because many slaves respond to a single command from the master, the effects on a selected target can be devastating. This is a parallel processor for criminal hackers. Unfortunately, there is no simple fix for the problem; the ideal solution is to prevent the slaves from ever being installed by improving security on all sites on the Net — but don't hold your breath.

Category 22.2 *DDoS attacks*

1999-12-28 **threats operating systems utilities vulnerabilities reports alerts distributed denial-of-service attack DDoS**

FedCIRC Advisory http://www2.fedcirc.gov/advisories/FA-99-23.html 99 23

FedCIRC and CERT-CC cooperated in summarizing the state of distributed denial-of-service tools at the end of December 1999. FedCIRC Advisory FA-99-23 reminded US government agencies that a variety of tools had been released on the Internet to amplify attacks on target systems, including the new TFN2K. In addition, MacOS 9 was vulnerable to serving as an amplifier for unwanted traffic with a ratio of 37.5:1 of output to input.

Category 22.2 *DDoS attacks*

2000-02-07 **Web site attack coordinated distributed denial of service attack connectivity failure outage**

Wired http://www.wired.com/news/print/0,1294,34178,00.html; CNet News

On Monday the 7th of February 2000, a distributed denial-of-service attack starting around 10:15 PST prevented access to the popular Yahoo site. According to the spokesperson for Yahoo's main hosting service, "The Global Center network is not down. There've been no fiber cuts... This is a specific attack on Yahoo by external forces. This affected accessibility to Yahoo, [which] hosts servers for its site at Global Center." In following days, similar attacks disabled eBay, Amazon.com, Buy.com and CNN.com sites.

Category 22.2 *DDoS attacks*

2000-02-08 **distributed denial-of-service attack tools Internet Web download law enforcement investigation**

CNET news.com http://news.cnet.com/category/0-1005-200-1545456.html

Evan Hansen and John Borland of CNET news.com summarized the key issues in the distributed denial-of-service (DDoS) attacks affecting the Web in early February 2000. Trinoo, Tribe Flood Network and Stacheldraht programs use client software illegally installed on poorly-secured systems to amplify commands for coordinated, high-volume bombardment of specific victim sites. Paul Tharp wrote a clear summary of the problem for the New York Post pointing out that the roots of the DDoS lie far back in the development of the Internet — an environment where trust was the norm and a ping (request for information) was never perceived as a threat.

Category 22.2 *DDoS attacks*

2000-02-10 **distributed denial-of-service attacks DDoS perpetrators authors criminal hackers bragging vandalism hactivists**

ZDNet News http://news.excite.com/news/zd/000210/17/hunting-web-attackers

Robert Lemos of ZDNet News reported on the hunt for the perpetrators of the wave of distributed denial-of-service attacks (DDoS) that slowed access to some high-profile sites in February 2000. Criminal hackers such as "Mixter," allegedly the author of the Tribe Flood Network used in DDoS attacks, commented that tracking the attacks is extremely difficult, especially since the backtracking would be likely to find the compromised machines on which slave programs had illegally been implanted by the criminals. One slim hope for finding the perpetrators was bragging; however, several unlikely claims had already been floated by disturbed individuals such as someone calling himself "Captain Zap" who issued an 18-page manifesto claiming responsibility for the attacks and by newly-minted alleged collectivities such as the "Sovereign Anarchist Internet Militia."

Category 22.2 *DDoS attacks*

2000-02-15 **denial-of-service attacks costs consequences estimates**

NewsScan, TechWeb http://www.techweb.com/wire/story/TWB20000214S0006

The Yankee Group [reported] that losses attributable to last week's denial-of-service attacks on major U.S. Web sites could total more than $1.2 billion. The research firm says the attacks resulted in capitalization losses that exceeded $1 billion on the days of the attacks and losses in advertising and sales on those days are expected to exceed $100 million. The report calls for Web sites to beef up their security, and patch holes and vulnerabilities in their systems. It predicts that affected Web sites and their peers will spend an additional $100 million to $200 million on these upgrades. (InformationWeek 14 Feb 2000)

Category 22.2 DDoS attacks

2000-02-17 **law enforcement investigation criminal vandal denial of service**

NewsScan, Washington Post http://www.washingtonpost.com/wp-dyn/business/A59099-2000Feb16.html

Federal Bureau of Investigation director Louis J. Freeh [said] his agency is pursuing "fast-developing leads" to hunt down the vandals who recently made a number of denial-of-service attacks on leading Web sites, and Attorney General Janet Reno is asking Congress for an additional $38 million to fight computer crime by training local police and prosecutors, hiring 100 new FBI computer analysts, and adding 68 lawyers to prosecute computer crimes. Freeh believes that the FBI has gotten excellent cooperation from businesses targeted by the attacks, but security expert Mark Rasch of Global Integrity Corp. says that companies have expressed fear that FBI inquiries will disrupt their business operations: "One of the problems you have is fundamental mistrust between the private sector and the law enforcement community. They're afraid of losing control of the investigation. They are concerned the FBI will ask what computer was hit . . . and walk away with your main server." (Washington Post 17 Feb 2000)

Category 22.2 DDoS attacks

2000-02-17 **denial-of-service attacks investigation law enforcement police ISP**

OTC Newsbytes

The RCMP was investigating the identity of a teenaged criminal hacker calling himself "mafiaboy" who was thought to be one of the perpetrators of the massive distributed denial-of-service (DDoS) attacks on major Web sites in early February. The Canadian federal police were cooperating with the FBI after theLook Communication ISP in Montreal turned over records to help track down the suspect. Security experts warned, however, that copycats were using the same pseudonym as a result of publicity following the DDoS attacks.

Category 22.2 DDoS attacks

2000-02-22 **distributed denial-of-service attacks DDoS vigilantes corporations information secrets sharing government policy**

New Thinking

Gerry McGovern, President of the Irish I.T. consulting company NUA, wrote in his weekly _New Thinking_ column that he was worried about news that US banks were warned about impending distributed denial-of-service (DDoS) attacks but kept the information to a tightly-knit group of financial institutions rather than sharing it with the public and security organizations. He argued that this behavior, as well as being counter-productive in the long run, was anti-social. He accused big business of usurping some of the rights and responsibilities of governments and ended, "Government has flaws; we all know that. But government is our best attempt to create institutions that allow society to be managed in a civilised manner. Without government the choice is chaos or vigilantism. The current search for the hackers behind the major spate of website attacks is a mix of both. Scores of security firms are out looking for the culprits. Their driving objective has nothing to do with law and justice and everything to do with the hoped for PR announcement that their firm caught the nasty hacker. Members of these firms are posing as suspects and friends of suspects in online chat rooms and other areas, to the extent that 'suspects' are turning up all over the place at the same time confusing everybody. . . . Law enforcement on the Internet is becoming a farce, and that's not good for anybody. Internet business will suffer if consumer confidence in the medium declines. As much as we would all like to clean up politics and make government more accountable, today right now - it is still all we've got. I have no problem with big business per se, but I don't want it 'protecting' my privacy and I don't ever want it out 'policing' my streets".

Category 22.2 DDoS attacks

2000-02-22 **DDoS distributed denial-of-service attacks analysis sociology fundamentals community**

Red Rock Eater News

Prof. Phil Agre, owner of the Red Rock Eater News, published a cogent analysis of the distributed denial-of-service (DDoS) attacks that shook the world of e-commerce in early February 2000. Agre said that the fundamental structure of the Internet combined with widespread ignorance by normal users of unsecured computers contributed to the vulnerability of the systems. He predicted that there would be enormous pressure against unsecured sites being used as platforms for the DDoS attacks.

Category 22.2 DDoS attacks

2000-05-01 **criminal hacker tools software denial of service**

NewsScan

Like legitimate software developers, who issue progressively improved versions of their applications, crackers seem to have released an early version of a powerful new tool that attacks and brings down Web sites. The new tool, "Mstream," which is made to launch "distributed denial of service" attacks, is similar to the ones that hosed up Yahoo and other Web sites earlier this year. In a denial of service attack, programmers embed software into hundreds or thousands of computers. Later, on cue, those computers send messages to a targeted server. The volume of Internet messages knocks out the target, rendering it inaccessible to other users. Mstream's core attack engine appears to be more potent than earlier versions and it may be able to carry out its nefarious task with only a handful of computers. Further, it can also damage the network of attacking host computers by overburdening those systems with a protective technique called "egress filtering," in which the hosts try to discard the packets they send. (New York Times 1 May 2000)

Category 22.2 DDoS attacks

2000-05-26 **denial of service DoS Web attack**

RISKS 20

The National Hockey League was down for five days in late May due to a distributed denial-of-service attack.

Category 22.2 DDoS attacks

2000-06-09 **Trojan denial-of-service attacks zombie slave platform**

NewsScan, Wall Street Journal
http://interactive.wsj.com/articles/SB960516256118849978.htm

Network Security Technologies Inc. has warned the FBI that a new "attack" . . . [Trojan] has already been implanted on as many as 2,000 computers worldwide, and could be used to cripple e-commerce and other Web sites. The company discovered the virus, which is hidden in a small video file received in e-mail or found on the Net, when an employee inadvertently downloaded and launched the program. The software can turn a victim's computer into a platform for remote-controlled "denial-of-service" attacks on Web sites. The program is disguised as a video file in the so-called avi format, but actually includes an "exe" extension, which launches the virus. Network Security officials say they've identified two computers and their owners — one in Maine and one in Canada — who appear to be implicated in the plot. (Wall Street Journal 9 Jun 2000)

Category 22.2 DDoS attacks

2001-02-02 **DDoS distributed denial-of-service attack e-mail list**

NewsScan

SECURITY EXPERTS TRICKED INTO HELPING LAUNCH ATTACK
Bugtraq -- an Internet mailing list comprising about 37,000 security industry technicians -- was used as the instrument for launching a denial-of-service attack against Network Associates, one of the world's largest Internet security companies. The bizarre incident began when a hacker sent a disguised string of code to Securityfocus.com, which manages the Bugtraq list. The hacker's message claimed the code was an example of a program that could exploit a recently discovered security hole in corporate security systems, but when Bugtraq members opened the code, it caused their computers to flood Network Associates' Web site with tens of thousands of messages, disabling the Web site for about 90 minutes. In another strange twist, Securityfocus admitted that it had forwarded the infected message to its members -- after getting the code checked and okayed by Network Associates. Industry watchers say the attack could be motivated by revenge against Network Associates, which was the company that first publicized the corporate network vulnerability. (Financial Times 2 Feb 2001)
http://news.ft.com/news/industries/infotechnology

Category 22.2 DDoS attacks

2001-05-03 **information warfare DDoS distributed denial of service firewalls blocking defense**

NIPC Daily Report

Attacks on Croatia's Internet space, particularly Croatian Telekom's (HT) Internet provider HThinet, which started 12 days ago, have been subsiding and are being successfully blocked, according to a HThinet network specialist. HT has been detecting and blocking attacks in cooperation with other Croatian Internet providers and its foreign partners Seabone and Deutsche Telekom. It has been established that the attacks have been coming from more than 1,000 addresses from all over the world. The attacks have been reported to the Croatian Interior Ministry, which cooperates with the Interpol on such cases. (Source: EUP, 3 May)

Category 22.2 *DDoS attacks*

2001-12-20 **distributed denial-of-service attacks DDoS zombie passwords compromise bot eggdrop**

NewsScan

'EGGDROP' VANDAL SETS STAGE FOR DENIAL-OF-SERVICE ATTACKS [20 Dec 2001]
A software robot (or "bot") known as "eggdrop" has been used to invade the customer Web servers of CCBill, a credit card processing company in Tempe, Arizona, and the company has urged all of its customers to change their server passwords and search their systems for malicious software that might have been planted by stealth on their own systems. The fear is that the malicious intrusion could lead to a wider "denial-of-service" attack, in which computer servers are commandeered and then used to generate floods of bogus Internet traffic that denies service to legitimate traffic. (Reuters/New York Times 20 Dec 2001)
http://partners.nytimes.com/reuters/technology/tech-tech-hack.html

---

Category 22.2 *DDoS attacks*

2003-11-03 **spam DDoS distributed denial of service vigilante information warfare**

WP http://www.washingtonpost.com/ac2/wp-dyn/A56072-2003Nov3?language=printer

Spammers retaliated against antispammers by launching DDoS attacks on them that wiped them off the 'Net. Ron Guilmette, an antispam activist, had his DSL Internet access saturated when 4,000 zombies on compromised computers flooded him with unwanted traffic.

Category 22.2 *DDoS attacks*

2005-02-24 **DDoS attacks target Japanese government Web network damage data functioning**

EDUPAGE; http://www.siliconvalley.com/mld/siliconvalley/10980656.htm

DDOS ATTACKS TARGET JAPANESE GOVERNMENT WEB SITES

Distributed denial-of-service attacks targeting the Japanese Prime Minister's Office and Cabinet Office this week caused severe network slowdowns and prevented access to the two Web sites, according to Chief Cabinet Secretary Hiroyuki Hosoda. The cyber attacks caused no significant damage, evidently not having been designed to destroy data, and the affected networks have returned to normal functioning. Similar attacks on several Japanese ministries in August and January 2004 temporarily froze their Web servers. The Japanese government has not yet identified the attackers.

Category 22.2 *DDoS attacks*

2005-03-14 **Internet Storm Center ISC hacking attacks Website hosting servers Domain Name System DNS cache poisoning denial of service DoS virus attacks**

DHS IAIP Daily; http://www.techweb.com/wire/security/159402730

WEEKEND ATTACK INFECTS HOSTING SERVERS

The Internet Storm Center (ISC) tracked a large-scale hack over the weekend that infected site-hosting servers, which in turn transformed all the hosted sites into distributors of malicious code. "We have received reports and evidence that a number of companies that provide shared hosting Web servers have had their servers exploited and all of the customer homepages modified so that visitors are attacked," said the Storm Center's Daniel Wesemann Sunday, March 13, in an online posting. It seems that the attack used both direct and indirect means to infect users, said the ISC. But ICS also found some evidence that a DNS cache poisoning attack was part of the program. "We are not quite sure yet how this is being done, as the files that we've received so far do not seem to contain DNS/DHCP poisoning code." This latest incident of DNS cache poisoning is unrelated to an earlier event this month, which was created by exploiting vulnerabilities in Symantec's gateway products.

Category 22.2 *DDoS attacks*

2005-05-07 **distributed denial-of-service DDoS spam unsolicited commercial e-mail flooding zombies restrictions SMTP servers**

RISKS 23 88

RUMPELSTILTSKIN ATTACK FLOODS NETWORKS

Brett Glass reported on a wave of fraudulent traffic from zombies testing for real e-mail addresses by generating likely candidates. "As described in a paper I wrote several years ago (where I coined the term for lack of a better existing one), it is an e-mail address harvesting attack in which a machine attempts to send e-mail messages to randomly guessed addresses at a domain. It might try common first names -- for example, 'john@domain.com,' 'joe@domain.com,' and 'mike@domain.com' -- and then proceed to common last names and combinations of names and initials. (In some cases, we've seen some very unusual guesses that appear to have been extracted from lists of AOL screen names.) If mail for a guessed address is accepted, the "zombie" machine records the address and sends it back to its 'master' -- a controlling machine which adds it to a database of addresses which will become targets for spam."

Glass concludes with recommendations:

>Because the "zombies" are generally not mail servers, the most effective way to mitigate these attacks -- though it might offend the sensibilities of the "Orthodox End-to-Endians" -- is for ISPs and enterprised to block outgoing port 25 traffic from client computers that are not designated as, or intended to be, mail servers. These computers should send outgoing mail only through a designated mail server, which in turn monitors them for excessive outgoing traffic.

ISPs' firewalls should monitor and log attempts to send such traffic, so that infected machines can be spotted and cleansed of their infections.

As I've mentioned above, there will be some people who are philosophically opposed to the notion of restricting Internet traffic so as to limit abuse. Alas, such idealism is inappropriate for the real world, where spam is now consuming so many resources that it threatens not only to choke off not only legitimate e-mail but to consume the lion's share of ISPs' bandwidth.<

Category 22.2 *DDoS attacks*

2005-05-24 **Federal Trade Commission FTC Internet Service Providers ISP zombies service cutoff hijacked computers China spam**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=8592338

FTC FIGHTING ZOMBIES

The Federal Trade Commission (FTC) will appeal to 3,000 Internet service providers (ISPs) worldwide to help identify and cut off service to hijacked computers. Such "zombies," as they are commonly called, are used by spammers to send millions of unsolicited e-mails. By some accounts, zombie machines send 50 to 80 percent of all spam. Though not requirements, the FTC's recommendations include monitoring subscriber accounts for large amounts of e-mail coming from a particular machine and helping those customers with hijacked computers clean their systems. The FTC said that 25 other countries are participating in the effort, though China--the country believed to be the source of a large percentage of the world's spam--is not one of them. Dave McClure, president of the U.S. Internet Industry Association, said that most U.S. ISPs already do most or all of the things recommended by the FTC. He noted that ISPs are forbidden by law from reading subscriber e-mails, saying that it can be difficult to distinguish between "spam coming across your network and your local charitable organization sending out its monthly newsletter." Reuters, 24 May 2005

Category 22.2 *DDoS attacks*

2006-02-13 **botnet scheme charge indictment zombie computer networks DDoS attacks monetary damages**

EDUPAGE; http://news.com.com/2100-7350_3-6038478.html 23

MEN CHARGED IN BOTNET SCHEME

Three men have been charged by federal authorities in a botnet scheme that reportedly netted the three $100,000 and caused $150,000 in damage. According to the indictment, Christopher Maxwell and two unnamed conspirators created a network of computers by illegally accessing networks at California State University at Northridge, the University of Michigan, and the University of California at Los Angeles. Using the network of zombie machines, the men installed adware on users' computers and also launched a denial-of-service attack on the network of Seattle's Northwest Hospital. The attack on the hospital resulted in the monetary damages cited in the indictment and also shut down the facility's intensive care unit. U.S. Attorney John McKay noted that although botnets are often seen as mere nuisances, this case shows that the repercussions from them can be deadly. If convicted, Maxwell could serve 10 years in prison and be fined $250,000.

Category 22.2 DDoS attacks

2006-03-16 **VeriSign distributed denial-of-service DDoS attack warning zombie botnet networks**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/hacking/story/0,10801,109631,00.html 23

VERISIGN DETAILS MASSIVE DENIAL-OF-SERVICE ATTACKS.

A sudden increase in a particularly dangerous type of distributed denial-of-service (DDoS) attack could portend big trouble for companies, according to VeriSign Inc. The attacks, which started on January 3 and ended in mid-February, were notable because they employed an especially devastating kind of DDoS attack, said Ken Silva, VeriSign's chief security officer. Such an attack typically involves thousands of compromised zombie systems sending torrents of useless data or requests for data to targeted servers or networks -- rendering them inaccessible for legitimate use. In this case, attackers sent spoofed domain-name requests from botnets to Domain Name System servers, which processed the requests and then sent replies to the spoofed victims, according to Silva.

Category 22.2 DDoS attacks

2006-03-20 **domain name system DNS distributed denial-of-service DDoS attack paper release**

DHS IAIP Daily; http://www.securiteam.com/securityreviews/5GP0L00I0W.html 23

PAPER ON DOMAIN NAME SYSTEM AMPLIFICATION ATTACKS RELEASED.

In recent months several attackers massively exploited recursive name servers to amplify distributed denial-of-service (DDoS) attacks against several networks utilizing IP spoofing. Analysis of three of these attacks makes up the bulk of a recent study released Friday, March 17. The paper outlines a DDoS attack which abuses open recursive Domain Name System name servers using spoofed UDP packets. To access the full report: http://www.isotf.org/news/DNS-Amplification-Attacks.pdf

---

22.3 DoS countermeasures

Category 22.3 DoS countermeasures

2000-02-14 **denial-of-service attacks investigation law enforcement LEO police**

NewsScan, Washington Post http://www.washingtonpost.com/wp-dyn/business/A51397-2000Feb14.html

Based on information provided to it by two computer experts, David Brumley of Stanford University and Joel de la Garza of the security firm Securify.com, the FBI [was] preparing to question two hackers nicknamed "Coolio" and "Mafiaboy" to determine whether they were responsible for recent denial-of-service attacks against such major Internet companies as Yahoo, Amazon. Buy.com, eBay, and CNN.com. Another security expert, Michael Lyle, says that Mafiaboy showed up last week on chat groups frequented by hackers and adds: "We entered into a number of conversations with Mafiaboy and we saw him asking for suggestions on what sites to attack and after someone would suggest a site, that site would go down." (Washington Post 15 Feb 2000)

Category 22.3 DoS countermeasures

2000-02-18 **DDoS distributed denial-of-service attacks colloquium discussion university**

Stanford University Computer Systems Laboratory

On 2000-02-23, the Stanford University Computer Systems Laboratory held a colloquium on the recent distributed denial-of-service (DDoS) attacks on Internet sites. Participants included David Brumley, Assistant Computer Security Officer for Stanford University; Joel de la Garza, security consultant for Securify; and Mark Seiden, Director of Securify Labs and Practice Area Head for Physical Security.

Category 22.3 DoS countermeasures

2000-02-19 **DDoS distributed denial-of-service attacks White House meeting government policy President**

Prof. Gene Spafford / CERIAS — Purdue University

Prof. Gene Spafford attended an emergency meeting at the White House on Friday 2000-02-11 to discuss the distributed denial-of-service (DDoS) attacks on major Internet sites that occurred at the beginning of February. He summarized the main points from the discussion as follows (quoting directly):

1) The Internet is international in scope, and most of the companies present have international operations. Thus, we must continue to think globally. US laws and policies won't be enough to address all our problems.

2) Privacy is a big concern for individuals and companies alike. Security concerns should not result in new rules or mechanisms that result in significant losses of privacy.

3) Good administration and security hygiene are critical. The problems of the previous week were caused by many sites (including, allegedly, some government sites) being compromised because they were not maintained and monitored. This, more than any perceived weakness in the Internet, led to the denial of service.

4) There is a great deal of research that yet needs to be done.

5) There are not enough trained personnel to deal with all our security needs.

6) Government needs to set a good example for everyone else, by using good security, employing standard security tools, installing patches, and otherwise practicing good INFOSEC.

7) Rather than new structure or regulation, broadly-based cooperation and information sharing is the near-term approach best suited to solving these kinds of problems.

Category 22.3 *DoS countermeasures*

2000-02-25 **criminal hacker distributed denial-of-service attacks**

CNN

At the end of February, FBI investigators and private security firms continued their search for the perpetrators of the extensive distributed denial-of-service attacks on major Web sites at the start of the month. The investigators were using log files from the affected systems and some of the slave-program-infested sites that were remote-controlled to send the flood of spurious requests to the victims. Some of the router logs show they were swamped with ore than 1 Gb/second of data during the attacks — and it was very important that the routers were the specific targets, since it made defensive measures all but impossible in real time. Some of those slave-infested computers included systems at Stanford University, UCLA, the University of California at Santa Barbara, and home business computers in Oregon. Logs from the #Goonies channel on IRC show someone calling itself "Coolio" (of which there are many, including one in the GlobalHell criminal hacker gang and one that claimed credit for defacing Web sites of DARE (the anti-drug program) and the US Commerce Department's Chemical Weapons Convention site in November 1999. Coolio boasted on IRC about hacking Amazon, the Russian Trek Travel site; it appears the boasting identified the precise time of the attack, something that had not yet been published by the news media. The number of tips, including some from the computer underground, was very high and every field office in the US had agents hunting down the leads.

Category 22.3 *DoS countermeasures*

2000-04-19 **denial-of-service attacks criminal hacker juvenile investigation arrest**

NewsScan, MSNBC http://www.msnbc.com/news/396994.asp

A 15-year-old Canadian boy . . . [was] arrested in connection with the denial-of-service attacks that crippled major Web sites including Yahoo, CNN.com, eBay and Amazon in February. The Montreal-area teenager, who uses "Mafiaboy" as his online moniker, was fingered after investigators were able to trace the attacks to that name by examining the log files of a computer at the University of California-Santa Barbara, one of the servers used in the cyber-assaults. (AP/MSNBC 19 Apr 2000)

Category 22.3 *DoS countermeasures*

2003-08-16 **Blaster worm Sean Sundwall Microsoft spokesman msblaster exploit windows server software redirection disabling**

NIPC/DHS

August 16, Associated Press — Microsoft says no major problems from 'Blaster' worm.

Microsoft spokesman Sean Sundwall said the company had not noticed any extraordinary network congestion Saturday, August 16, from attempts by the "blaster" worm to force thousands of infected computers to target the software company's Website and network. The virus-like infection exploits a flaw in most current versions of Microsoft's Windows operating system for personal computers, laptops and server computers. Although Microsoft posted a software patch on July 16, many users failed to download it, leaving them vulnerable. The exploiters of the Microsoft flaw made a mistake. The worm instructed computers to call up an incorrect address for reaching the actual Microsoft Website that houses the software patch. Although Microsoft has long redirected those who visited that incorrect address to the real site, the company disabled the automatic redirection Thursday. That has helped Microsoft's real Web site stay accessible to users, Sundwall said.

22.4 Accidental availability disruptions

Category 22.4 *Accidental availability disruptions*

1997-01-09 **QA quality assurance loop positive feedback**

Reuters; RISKS 18 75

When an operator keyed in a special code into the SkyTel control system, it caused a half-hour beeping chorus that rang 100,000 beepers with up to 25 erroneous calls. Seems the technician assigned a PIN to a new customer that was actually a secret code used to broadcast news headlines to those 100,000 beepers. So when the customer used the new PIN, it appeared on all the beepers in question — and many of their users promptly called back SkyTel and entered the PIN, causing ever-increasing waves of beeping. The problem was particularly irritating for West coast residents, since the beeping chorus started at 8:16 am Eastern time, which translated to 5:16 am on the Pacific coast.

Category 22.4 *Accidental availability disruptions*

1997-01-10 **availability ISP**

AP

Flat-rate charges for Internet access will eventually be a eliminated, said industry watchers in January. ISPs begin to lose money once their $20/month users reach about 11 hours a month online. As major ISPs such as AOL struggle with the consequences of decoupling usage from cost of usage, niche markets have opened for ISPs charging premium rates but guaranteeing more than busy signals.

Category 22.4 *Accidental availability disruptions*

1997-01-12 **QA quality assurance availability loop positive feedback**

EDUPAGE

A technical glitch on Thursday the 9th of January 1997 caused the SkyTel paging network to send erroneous call-me-back messages to more than 100,000 customers. The problem was exacerbated when some diligent subscribers returned the call and left their phone numbers so that whoever had beeped them could call back. The result was a 26-minute major phone traffic jam as thousands of other SkyTel customers then called those numbers. Apparently, the whole mess started when a customer desiring a new PIN (personal identification number) was mistakenly assigned one linked to a secret code that the company uses to beam Dow Jones News Service information out to 100,000 customers. The PIN, a seven-digit number that looked like a phone number, was zapped to the Dow Jones subscribers, many of whom then tried to dial it as a local call. Others recognized it as a PIN, and called SkyTel to retrieve the "caller's" number, jamming the lines there. "One frequency of our one-way nationwide network experienced an anomaly in the database that caused customers to be paged erroneously," says a spokesman for SkyTel's parent company, MTel, which has apologized for the snafu. (Wall Street Journal 10 Jan 97 A1)

Category 22.4 *Accidental availability disruptions*

1997-01-12 **availability ISP**

EDUPAGE

IBM responded to e-mail delivery problems on its top-ranked Internet Connection by quadrupling its capacity.

Category 22.4 *Accidental availability disruptions*

1997-01-16 **availability telecommunications ISP**

EDUPAGE

Nortel offered LECs and IECs the opportunity to shift Internet data from congested voice networks to the carriers' data networks.

Category 22.4 *Accidental availability disruptions*

1997-01-17 **availability AOL**

AP

By January, AOL's incredibly stupid decision to offer unlimited access for a flat fee of $19.95 had resulted in endless waits because selfish people stayed online for hours — even running special programs to prevent the network from logging them off for inactivity. Furious customers faced endless busy signals; people depending on the network for important e-mail and other services were cut off from the resources they had come to depend on. Many customers launched lawsuits; several state attorneys general launched investigations of possible commercial fraud and misrepresentation. This is an example of the Tragedy of the Commons described by Garrett Hardin twenty years ago; in that case, he described the destruction of English village commons where people could graze their sheep at no cost. Population growth resulted in a perceived economic advantage in the short term by putting as many sheep as possible on the commons even though the animals destroyed the resource. Similarly, AOL violated a prime principle of the market by providing unlimited access to a limited resource without a feedback mechanism to ensure that users would act responsibly. By the last week in January, AOL had agreed in principle to refund fees to anyone affected by the snafu — potentially millions of people.

Category 22.4 *Accidental availability disruptions*

1997-01-19 **availability ISP**

EDUPAGE

AOL's promised expansion would increase its capacity from 10 million to 16 million sessions a day, at a cost of $400M.

Category 22.4 *Accidental availability disruptions*

1997-01-21 **AOL denial of service DoS**

AP

An unfortunate resident of Cleveland has been kept awake by AOL users who mis-key the service's access number, which is one digit away from his home phone number. Royal Anderson has received over 100 calls a night, with the problem intensifying ever since AOL announced unlimited access for a flat fee.

Category 22.4 *Accidental availability disruptions*

1997-01-23 **AOL lawsuit availability**

UPI

Twenty state attorneys general discussed AOL's failure to live up to its claims of unlimited access.

Category 22.4 *Accidental availability disruptions*

1997-01-23 **availability**

AP

The FCC began hearings on how to reduce bandwidth saturation of the Internet resulting in part from AOL and other ISP's decisions to offer unlimited access for a flat fee. LECs and IECs have complained that the ISPs are abusing the public switched telephone network.

Category 22.4 *Accidental availability disruptions*

1997-01-23 **AOL availability**

UPI

Three residents of Ohio asked for a class-action suit for damages against AOL because, they claim, AOL offered unlimited access to the Internet but cannot provide it. AOL said it was spending $350 million to build up its network.

Category 22.4 *Accidental availability disruptions*

1997-01-23 **availability telecommunications**

EDUPAGE

According to the Internet Access Coalition, the telcos' whining about congestion on the voice network is due to the antiquated public switched telephone system, which depends on establishing continuous circuits for data transmission. Instead, said the experts, the phone companies should invest in packet-switching to maximize efficiency of the network. The telcos retorted that with an expected 70-fold increase in data traffic from 1987 to 2001, "Someone has to pay for that usage, the subsequent wear and tear on the network, and the new equipment additions necessitated by this rapid growth."

Category 22.4 *Accidental availability disruptions*

1997-01-25 **AOL availability lawsuits**

AP

NY's attorney general threatened to join the army of other states in suing AOL for commercial fraud unless the company stops promising unlimited access that it cannot supply. Meanwhile, CompuServe broadcast an advertisement during the Superbowl showing 15 seconds of a blank screen accompanied by the sound of a busy signal.

Category 22.4 *Accidental availability disruptions*

1997-02-02 **availability ISP**

EDUPAGE

Some infuriated customers of AOL are claimed to be planning class-action suits for recovery of consequential damages following a series of service outages by the giant ISP. However, AOL Terms of Service contracts specifically exclude liability for such damage.

Category 22.4 *Accidental availability disruptions*

1997-02-06 **AOL availability**

AP, UPI

AOL suffered yet another outage for 2.5 hours on 97.02.05 when technicians upgraded its software starting at 17:00 EST. The system was unavailable again later that night between 04:00 and 07:00 EST.

Category 22.4 *Accidental availability disruptions*

1997-02-06 **availability ISP QA**

EDUPAGE

EDUPAGE reported: >America Online subscribers trying to log on during a two-hour period early Wednesday evening [5 Feb] experienced what a company spokesman called a "hiccup" which gave them the message: "The system is temporarily unavailable. Please try again in 15 minutes." The system malfunction was apparently caused by the installation of a software upgrade. (Atlanta Journal-Constitution 6 Feb 97)<

Category 22.4 *Accidental availability disruptions*

1997-02-06 **Availability ISP AOL**

RISKS 18 81

AOL's spectacular misjudgment in allowing unlimited access without extra charges — and resulting gridlock when some users left their modems hooked up to the ISP 24 hours a day — resulted in an embarrassing climb-down in late January. AOL had to impose a 45-minute limit on all sessions. Anyone trying to stay on-line longer than that was unceremoniously kicked off the system until their next logon.

Category 22.4 *Accidental availability disruptions*

1997-02-13 **Web cache**

RISKS 18 83

At Ontario Hydro, users noticed that they were accessing unexpected and unrequested Web pages; in one case, a user inadvertently brought up someone else's MBANX bank records. The puzzled user accused the owner of the MBANX records of using the finder's PC at night. However, investigation suggested that the server was not forcing users to stop caching forms transmitted under the SSL protocols.

Category 22.4 *Accidental availability disruptions*

1997-03-03 **Explorer browser Web vulnerability**

AP, COMTEX, RISKS 18 85

Student Paul Greene of the Worcester Polytechnic Institute in Worcester, MA announced on his Web page that Microsoft's Internet Explorer 3.0 and 3.01 running under Window95 (only) allow any Web page to include code for execution of any program on a client machine. Microsoft got its patch up within 48 hours.

A week later, Microsoft was hit with two more announcements of Explorer bugs. Version 4.0 was discovered to be susceptible to "hostile links" embedded in newsgroup messages or in e-mail, according to the anti-virus company Eliashim. Then University of Maryland students announced that Explorer version 3.01 would allow an intruder to install executables on a client system (e.g., to infect the victim's computer with viruses).

Category 22.4 *Accidental availability disruptions*

1997-03-17 **Shockwave security e-mail**

RISKS 18 91

Browsers with the Shockwave multimedia plug-in from Macromedia allow a Web server to read e-mail files located on a client (browser's) workstation. A variation of the hole allows a server to access any Web site the client can reach, even if they are on secure intranets. For details, see <http://www.webcomics.com/shockwave/>.

Category 22.4 *Accidental availability disruptions*

1997-03-20 **InterNIC denial of service**

RISKS 18 92

InterNIC lost papers for a company and shut down its DNS entry. Disaster without recovery; took 20 hours to get back online.

Category 22.4 *Accidental availability disruptions*

1997-03-22 **disaster recovery evidence denial of service DoS**

RISKS 18 93

In Austria, court officials seized all computers and backup tapes at the offices of an ISP. As a result, 2,500 customers went off-line without warning. Austrian ISPs rallied to plan a 2-hour shut-down later in the month as a protest against this unprecedented denial of service.

Category 22.4 *Accidental availability disruptions*

1997-03-28 **denial of service ISP Internet DNS domain names DoS**

RISKS 19 1

Michael Miora, NCSA's Director of Consulting, discovered that he no longer had access to the Net. His ISP, Sprynet, suddenly and without notification cut off service to anyone not using an e-mail address ending in "@sprynet.com." This measure was supposed to cut down on fraud. It presumably cut down on clients.

Category 22.4 *Accidental availability disruptions*

1997-03-28 **SSL browser vulnerability Web**

RISKS 18 95 ff

Daniel Klein, a Pittsburgh security consultant, discovered a major hole in both Netscape Navigator and Microsoft Internet Explorer. Servers using the GET command instead of the POST command in Web pages, even those using SSL to encrypt communications. The problem is that improperly written pages allow confidential information resident on the client side to be read by the server for the _next_ Web page loaded: "The information that Web user typed in securely suddenly gets transferred to the logs of the next machine, credit card numbers and all." This bug was confirmed independently by Eric Rescorla and explained in more detail by Anup K. Ghosh, PhD in RISKS 19.02 (97.04.02).

Category 22.4 *Accidental availability disruptions*

1997-05-19 **air traffic electrical power outage backup disaster denial**

AP

A short circuit in backup MCI communications systems at the Air Route Traffic Control Center in Oberlin, OH wiped out most communications among air-traffic control towers and 180 airplanes in Indiana, Michigan, Pennsylvania, New York, Ohio and West Virginia for 67 minutes. A few low-power channels remained functional and ATC relied in part on cellular phones and some non-MCI phone lines. Flights leaving Cleveland, Pittsburgh and Detroit were delayed by an hour; other planes were rerouted around Ohio air space for the duration of the outage.

Category 22.4 *Accidental availability disruptions*

1997-05-23 **denial of service saturation bandwidth ISP**

Newsbytes

On Wednesday 97.05.21, an e-mail server at the Reston, VA facility of the BellAtlantic.net ISP shut down e-mail delivery to its customers. The system was unable to deliver the mail until Friday the 23rd, when all accumulated messages were on their way to their destinations. No messages were lost.

Category 22.4 *Accidental availability disruptions*

1997-05-29 **Internet availability**

EDUPAGE

A study by Inverse Network Technology suggested that most of the delays in e-mail delivery originate in problems on gateways. The study suggested that 88% of all e-mail takes no more than five minutes to deliver; however, some ISPs allow 10% of their deliveries to take longer than an hour.

Category 22.4 *Accidental availability disruptions*

1997-07-17 **Internet power failure outage availability disaster**

Newsbytes

On 08:17 PDT on 1997.07.16, a rectifier failure in a battery room shut down power to the MAE-West switching center, terminating Internet access for major ISPs and their customers. At 11:00 PDT, someone in Los Angeles cut a fiber-optic cable and shut down ATM (asynchronous transfer mode) links carrying 473 T-3 lines (45 Mbps each). The outages affected Internet traffic throughout the United States, with major congestion and outright outages lasting until 13:40 PDT.

Category 22.4 *Accidental availability disruptions*

1997-07-25 **Internet congestion bandwidth availability**

AP

Elizabeth Weise of AP published a fascinating story in late July that reported on research by communications engineers and physicists explaining why the Internet seems to have unpredictable periods of heavy congestion. Some analysts see a "tragedy of the commons" in which users, unaware of the effects of their largely free use of Internet bandwidth, blithely increase their surfing without regard to equitable sharing with the unknown millions of other users. The Net responds acceptably until key "pipes" are saturated with data — and then response can slow to a crawl. In an interesting effect of mass-action, at some point large numbers of users get disgusted and log off, releasing the gridlock suddenly. Some analysts suggest that charging people for their time online will solve the problem; others argue that defining classes of service will help (e.g., charging for high-priority usage and not for low-priority applications). Critics of these proposals deny the validity of the "commons" model, arguing that increased demand can make increased capacity cost-effective.

Category 22.4 *Accidental availability disruptions*

1997-09-10 **telecommunications denial of service QA disaster**

RISKS 19 39

Peter G. Neumann, abstracting a report forwarded by Steve Bellovin, wrote "Around 7pm on the evening of 8 Sep 1997, the main MFS Communications switch (MFS Switch One) failed, downing UK telecommunications links provided by MFS, Worldcom, and First Telecom. The outage also affected most of CompuServe's UK customers, whose access is typically via an MFS phone number."

Category 22.4 *Accidental availability disruptions*

1997-10-09 **denial of service backhoe attack**

AP

In Kansas City in October, an unidentified dump-truck driver forgot to lower his truck's bed before speeding through a street and snagging overhead telephone cables. His carelessness interrupted phone and Net access for 119,000 Sprint users for four hours. Victims included people in Oklahoma, Missouri, and all the way into Florida. This is a new variant of the time-honored "backhoe attack" for causing denial of service.

Category 22.4 *Accidental availability disruptions*

1997-11-11 **QA denial of service power outage e-mail denial of service**

RISKS 19 45

Another glitch hit AOL on Nov 3, 1997, when users lost e-mail service for an hour or so . Worse still, a bug generated a repeating message apologizing for the loss of service and required forcible termination of the AOL client software to stop the automated grovelling. On Nov 18, the e-mail system was unavailable for up to six hours.

Category 22.4 *Accidental availability disruptions*

1997-12-24 **backup disaster recovery**

RISKS 19 53

Sun Valley, ID uses a computerized ticketing system involving a database of authorized skiiers and scanners. After a disk crash in December 1997, the company had to order several thousand skiiers to reregister — including new ID cards and photographs.

Category 22.4 *Accidental availability disruptions*

1998-02-26 **denial of service backhoe telephone cable outage**

EDUPAGE

Another backhoe attack: Illuminet cables were severed in Illinois, causing widespread phone-service outage for customers of AT&T, Teleport, and Bell Atlantic's cellular-phone customers.

Category 22.4 *Accidental availability disruptions*

1998-03-09 **mailstorm positive feedback mailing list server unsubscribe**

RISKS 19 62

In a routine e-mail announcement to about a thousand members, the National Association of Broadcasters included instructions on how to unsubscribe from the list. Unfortunately, the address they gave actually broadcast — how appropriate — the unsubscribe messages to the entire list, causing a growing mailstorm as people replied to the bizarre messages and amplified their responses by a thousand.

Category 22.4 *Accidental availability disruptions*

1998-03-17 **availability capacity Internet bandwidth**

EDUPAGE

If Internet traffic continues doubling every three to six months, the Net will run out of bandwidth, warned ISPs and vendors. Key problems include the rising use of streaming video and other high-volume communications. In April, reported EDUPAGE, "A study by the U.S. Commerce Department <http://ecommerce.gov/> [said] that traffic on the Internet is doubling every hundred days and predicts that electronic commerce will grow to $300 billion a year by 2002. (USA Today 16 Apr 96)"

Category 22.4 *Accidental availability disruptions*

1998-04-14 **availability QA transmission networks fiber optic**

EDUPAGE

In April, software errors at AT&T caused several hours of downtime for customers of the communication giant's fiber optic data network. Later reports indicated that the network failure severely disrupted electronic commerce networks relying on computer communications for financial transactions such as approvals of credit cards.

Category 22.4 *Accidental availability disruptions*

1998-04-14 **availability downtime disaster closing business retail**

RISKS 19 67

Starbucks in Boston, and possibly elsehwere were closed on Tuesday 14 Apr because a central computer crashed and prevented them from opening their cash registers. [Hmm: backup systems? Manual procedures? Free coffee?]

Category 22.4 *Accidental availability disruptions*

1998-04-14 **availability network crash down frame relay telecomm**

RISKS 19 67

On Monday, 13 Apr, the AT&T frame relay network crashed for about a day, depriving an estimated 2500 companies US-wide of computer telecommunications for credit-card validation, inter-bank and inter-branch transactions. Financial losses from lost business were expected to be astronomical. In May, AT&T published an explanation of the events that led to the failure: "AT&T said the problem began when a computer command was issued to upgrade software code in one of the network switch's circuit cards. This created a faulty communications path that generated a large volume of administrative messages to other network switches. As a result, the other switches quickly became overloaded and stopped routing data from customers' applications for periods ranging from six to 26 hours before the network was fully restored."

Category 22.4 *Accidental availability disruptions*

1998-05-07 **single point failure availability disaster backup telecomm**

RISKS 19 72

A single communications tower was taken out of service in Newark, Ohio. RISKS correspondent Matt Curtin reported on the results: "[A Newark friend's] entire network was unreachable, and even his ISP's connection between Columbus and Newark was down. He then told me that since 10:30 a.m., no one in Newark had any telephone service whatsoever. No one could take credit cards. Some stores' POS terminals would not work. No ATMs were working. Even the digital cellular network in Newark became unusable — probably due to overload, as a result of picking up some of the slack."
Complete service was restored only at 18:45. Mr Curtin made the point that single points of failure ought by now to be avoided but they are still widespread.

Category 22.4 *Accidental availability disruptions*

1998-05-16 **mail storm denial of service saturation autoreply**

RISKS 19 74

Yet another mailstorm erupted when an Australian official set autoreply on his e-mail package while he was away. Unfortunately, he inadvertently set his destination for these largely-useless messages to be all 2,000 users on his network — and requested autoconfirmation of delivery of each autoreply — which generated yet another autoreply — and so on ad infinitum and ad nauseam. Within four hours, his endless positive-feedback loop generated 150,000 messages before his autoreply was shut down. The ripples lasted for days, with the perpetrator saddled with 48,000 messages in his in-basket and a stream of 1,500 a day pouring in. [Personally, I detest autoreplies, feeling that a correspondent's lack of reply is self-descriptive. However, if one must use this facility, it's appropriate to regard it as a potential Sorceror's Apprentice, so pay attention to details. In particular, anyone subscribing to e-mail lists (such as RISKS) should never enable autoreply. The danger is exacerbated if the mailing list address is also the address for automatic posting to the list — a guaranteed mailstorm-generator.]

Category 22.4 *Accidental availability disruptions*

1998-05-21 **beeper satellite television TV interruption denial service**

EDUPAGE, RISKS

Over ten million pagers were silenced across the US when the Panamsat Galaxy 4 satellite malfunctioned and began spinning out of control. Other service interruptions affected public radio networks that were unable to transmit some syndicated programs. Carriers switched to other satellites and operations were back to normal within a couple of days.

Category 22.4 *Accidental availability disruptions*

1998-07-07 **availability QA quality assurance software air traffic**

RISKS 19 84

When the American Airlines SABRE computers failed twice in a week at the start of July, hundreds of AA flights were delayed from 8 minutes to several hours.

Category 22.4 *Accidental availability disruptions*

1998-07-14 **QA quality assurance airport baggage traffic control**

RISKS 19 85

In July, both Hong Kong's new airport and Amsterdam's airport were saddled with the consequences of computer problems. The HK airport bagage handling system went haywire, with tons of baggage having to be sent to the old Kai Tak airport when the cargo-handling system lost all its records. In Amsterdam, a malfunction in the air-traffic control software blanked out all screens and caused an emergency hold on all inbound and outbound flights at Schiphol. Although the software was restarted in half an hour, the resulting chaos lasted for the rest of the day. Finally, in Copenhagen, similar baggage-handling software problems were reported in September.

Category 22.4 *Accidental availability disruptions*

1998-08-07 **availability power surges phones fax data**

RISKS 19 90

In Sydney, Australia, a sudden power surge at 12:20 pm on 4 Aug hit Telstra, the main communications service. The sudden outage crashed bank computers, automated banking machines, and phone and fax lines. The power outage lasted one hour but repercussions continued into the night as customers tried to get place phone calls and saturating the bandwidth.

Category 22.4 *Accidental availability disruptions*

1998-08-18 **water supply disaster availability monitoring emergency**

RISKS 19 92

In Lewiston, ME, a computer problem shut down public water-supply chlorination, meaning that 40,000 people had to boil water before drinking it. The water-quality problem lasted 30 hours in part because no one noticed the lack of chlorination until a routine check that occurred 14 hours after the failure. MORAL: frequency of monitoring must reflect the importance of spotting problems.

Category 22.4 *Accidental availability disruptions*

1998-08-19 **air traffic control availability QA quality assurance crash**

RISKS 19 93

Nashua, NH airport experienced over 100 Air Traffic Control system failures in the first eight months of 1998. In the incident on 19 Aug, the system went down for 37 minutes with 350 airplanes having to be managed using verbal commands and slips of paper. Peter Neumann commented, "Do you think the Y2K impact on the ATC system will last only 37 minutes?"

Category 22.4 *Accidental availability disruptions*

1998-09-17 **penetration appropriate diversion resources denial service**

EDUPAGE

Aaron Blosser , a 28-year-old consultant, was accused of misappropriating resources on 2585 computers at his client, U.S. West (a major telephone company). In his attempt to find ever-greater prime numbers, he commandeered over 10 years of processing cycles; as a result of the extra work, directory-assistance operators found the time for retrieval of telephone numbers stretching from the usual 3-5 seconds on into the 5 minute range. Associated Press reported, "The computers were so slow in mid-May that customer calls had to be rerouted to other states, and at one point the delays threatened to close down the Phoenix Service Delivery Center."

Category 22.4 *Accidental availability disruptions*

1998-09-27 **archives data retention media instability incompatibility**

EDUPAGE

The head of the US National Archives failed to meet a deadline for clear policies on government record retention. John W. Carlin explained that all the information technology resources at his disposal were focused on the Y2K problem. He emphasized the complexity of the problem: "How do we identify, manage, preserve and provide ongoing access to e-mail, word processing documents and other kinds of electronic records that are proliferating in formats, mushrooming in quantity and vulnerable to quick deletion, media instability and system obsolescence?"

Category 22.4 *Accidental availability disruptions*

1999-01-03 **archives reference bibliography evanescence instability**

RISKS 20 14

An interesting article in RISKS DIGEST from correspondent Jerry Leichter pointed out that URLs are an unstable form of reference to scholarly work. He cited a case in which interesting papers disappeared from an academic Web site when the sponsoring research was disbanded. He also worried about using commercial sites as repositories for papers, arguing that the vicissitudes of the market make the destiny of such storage uncertain at best.

Category 22.4 *Accidental availability disruptions*

1999-02-01 **emergency phone 911 system crash outage availability**

RISKS 20 19

On 1 Feb 1999, the New York City emergency phone system (911) crashed during a routine backup generator test. It seems the generator did not work and the backup system went down for an hour as technicians worked on getting the power generator running. The main system was down for six hours in all.

Category 22.4 *Accidental availability disruptions*

1999-02-01 **air traffic control critical infrastructure failure backup**

RISKS 20 19

Air traffic controller Paul Cox wrote in RISKS, "On 15 Jan 1999, at 2 PM, the power failed at Seattle Center, an en-route ATC facility that covers nearly 300,000 square miles of the NW United States." He described how the brief interruption in power during some routine tests set in motion catastrophic failure of the ATC in this area. Computers had to be rebooted, radar screens went dead for periods up to an hour and more, and the human controllers were frantic as they tried to shift planes from their normal 5 mile separation to the reequired 20 mile distances prescribed by the FAA. Luckily, the controllers had succeeded after much lobbying in having a backup radio system that did not require computers at all and that therefore worked at once after the power glitch. Mr Cox wrote, "This failure simply drives home yet again that backup systems are only as good as the main systems IF those backups are equally dependent upon a power supply. In fact, our backup communications system and backup radar display systems were essentially worthless to us, because they failed at the same instant as the main system did when the power died. As long as you have a single point of failure in any system, it doesn't matter how many backups you have downstream if they are dependent on that point."

Category 22.4 *Accidental availability disruptions*

1999-02-03 **QA quality software down delay stop halt interruption broker**

Wired via PointCast; Washington Post

Installation of some new software on the ETrade Web-based stock brokerage caused intermittent, serious failures that interrupted electronic trading for several hours on Wednesday 3 February. Some customers interviewed by R. Scott Raynovich, writing for Wired, stated that they would pull their brokerage business out of Etrade for failing to provide consistent service. An anonymous investor reportedly said, "I'm trusting these guys with thousands of dollars of my money, and they can't provide me consistent access to it," said one ETrade customer, who asked to remain unnamed because he feared retribution from ETrade officials as he attempted to transfer money to another service. Hours, sometimes days, go by with me unable to put money into a suddenly hot stock, pull out of one that's tanking, or try to get in on an IPO. I'm disgusted with this company."

Category 22.4 *Accidental availability disruptions*

1999-02-12 **security e-mail public access free**

USA Today

USA Today reported that HotMail and Yahoo, providers of free e-mail, were improving security by shutting down any account subject to several unsuccessful attempt to login. [MK comments: This is one of the oldest mistakes in system management, since it immediately opens each account to a trivially easy denial of service: simply try to logon several times to a victim's account without the right password and VOILA — no further legitimate access until the account is reset.]

Category 22.4 *Accidental availability disruptions*

1999-02-18 **import availability down-time failure crash**

Wall Street Journal

John R. Emshwiller reported in the Wall Street Journal (" Customs Service's Old Computer System Triggers Worry," 1999.02.18) that the U.S. Customs Service's antiquated computers (antiquated in this era of Moore's Law means 14 years old in this case) are causing increasingly frequent failures of availability. Customs Service Commissioner Raymond Kelly said succinctly, "The system is collapsing." Random downtime causes backups in processing the flow of imports ($900B per year involving 19.4 million entry requests) with resulting delays in getting imported products to their destinations on time.

The most serious breakdown to date occurred on 1998.10.01, when hard disk failures caused a chain of system failures resulting in a six-hour downtime. The consequences were dramatic: a backlog of 80,000 requests. In a misguided attempt to stave off further electronic requests, system administrators shut down their modem lines; however, "many importers have automatic dialing systems that just kept resubmitting the requests, each of which was marked as a new entry." The Customs Service decided unilaterally to delete 45,000 of the accumulated requests, forcing resubmission for those shipments.

Currently, the Customs Service has requested financial support for new computer hardware and software, but the Clinton Administration has proposed paying for the $1B expense by levying an import fee — a measure strenuously objected to by the business community, which would prefer funding from general tax revenues.

The article ends on a curious note: "One relative bright spot: Customs Service officials say they don't expect any major Year 2000 computer problems. On the other hand, said Woody Hall, an agency assistant commissioner, `the joke around here is that a lot of good it's going to do you to be Y2K-compliant if the system crashes around you.' "

Category 22.4 *Accidental availability disruptions*

1999-02-24 **availability online trading e-commerce failure crash**

AP

The Charles Schwab online stock brokerage computers went down at 09:37 on 1999-02-24 for about 90 minutes, causing disruption for its clients, who were normally placing an average of 153,000 trades a day online — 28% of the market for online securities trading.

Category 22.4 *Accidental availability disruptions*

1999-03-01 **availability interruption single point of failure downtime**

RISKS 20 23

On 21 Feb 1999, there was a 15 hour period when many ISPs in the UK were down due to (1) a problem on a transatlantic link maintained by Teleglobe and (2) the simultaneous upgrade of a mail server on the Cable Internet ISP. Malcolm Park noted in RISKS that many users of the affected ISPs complained about interference with their Net-dependent business. He pointed out that businesses should know that the Internet has no guarantee of service; at the very least, it would be appropriate for anyone dependent on the Net to have a contract with a backup ISP. [MK comments: here in Vermont, I have two ISPs — and have often had to resort to the secondary one when the first one's local node is saturated or malfunctioning. Unfortunately, I still have only one set of wires between our home out in the boondocks and the central switch — but at least the set includes three different phone numbers.]

Category 22.4 *Accidental availability disruptions*

1999-10-06 **contract fitness tort software license lawsuit date availability**

Financial Times (London)

In Italy, the clothing firm Industrie Zignago S Margherita sued UNISYS for refusing in 1994 to provide an upgrade to its System 1100 that would allow the ancient machines to cross the Jan 1, 1996 date boundary (presumably causing a date counter to roll over). UNISYS did offer a fix, but demanded payment. In October, the court ruled in favor of the client, saying that the supplier had violated its contract to provide software and hardware until 1997.

Category 22.4 *Accidental availability disruptions*

1999-10-20 **availability quality assurance load demand saturation crash encyclopedia reference**

Los Angeles Times

The Encyclopaedia Britannica opened its long-awaited free Web site, <http://www.britannica.com> — and immediately crashed because an order of magnitude more people tried to access the site than expected.

Category 22.4 *Accidental availability disruptions*

1999-10-25 **online file storage vault Web drive drop-box URL**

Wired http://www.wired.com/news/print/0,1294,32051,00.html

About 20 companies have announced free or cheap Web-based file storage for subscribers. One of the most aggressive marketers, i-drive, admits that it takes no responsibility for the security or legality of the materials stored on its servers. Privacy activists and security experts wonder about the safety of storing private information on someone else's systems; others expressed concern about the likely use of these services as ways of sharing stolen intellectual property. On the other hand, those services providing for legal storage and use of MP3 tracks, for example, would have a valuable source of market data for music companies.

Category 22.4 *Accidental availability disruptions*

2000-01-25 **availability terms service level agreement contract**

NewsScan, Los Angeles Times
http://www.latimes.com/business/20000125/t000007795.html

A Microsoft Network subscriber is suing the software giant, claiming that Microsoft overloaded its Internet access service by signing up new subscribers without upgrading its system to accommodate the extra traffic. Microsoft recently ran a promotional campaign promising customers who signed up for three years of MSN service a $400 rebate for purchases at stores such as Office Depot and Best Buy. The lawsuit, which will be filed in federal court in Chicago next week, charges Microsoft with breach of contract and negligence, and will request that the company upgrade its network. (Bloomberg/Los Angeles Times 25 Jan 2000)

Category 22.4 *Accidental availability disruptions*

2000-01-31 **availability production down-time**

Edupage, New York Times

In late January 2000, the National Security Agency's computer systems failed for 72 hours. Not surprisingly, the NSA declined to explain exactly what went wrong, other than to say it was neither a cyberattack nor a Y2K bug.

Category 22.4 *Accidental availability disruptions*

2000-02-21 **Web site availability offline**

RISKS 20 81

Shortly after President Clinton announced, "Our administration has been working for years now to reduce vulnerabilities in government computers and to encourage the private sector to do more," the US Senate's Web site went offline for nine hours on the 14th of February.

Category 22.4 *Accidental availability disruptions*

2000-03-18 **cable back-hoe attack splicing testing cut break availability interruption**

RISKS 20 84

Peter G. Neumann wrote in RISKS: 1,000 phone lines in northeastern San Jose were down for about a week on 10 Mar 2000, when a construction crew accidentally took out four buried cables. ``The repair work is mind-numbingly tedious, with each wire having to be spliced by hand and then tested." [Source: *San Francisco Chronicle*, 14 Mar 2000, A13,18, PGN-ed]

Category 22.4 *Accidental availability disruptions*

2000-03-22 **backhoe attack optic fiber availability outage**

RISKS 20 85 & 86

Tim Dixon wrote as follows in RISKS:
"When will people learn? Computerworld reports that Northwest Airlines had to cancel about 130 flights during a 3.5-hour outage at their Twin Cities hub. It seems a contractor accidentally bored into the cable cluster containing both main and redundant fibre lines. [http://www.computerworld.com/home/print.nsf/CWFlash/000322CBDE]

When will people learn they need to know where their redundancy lies? Cables run through the same conduit are only partially redundant, as events like this will happily take out all the cables in a conduit, making the conduit itself a single point of failure."

Category 22.4 *Accidental availability disruptions*

2000-04-05 **bandwidth technology protocols network broadband consortium**

NewsScan

A group of more than 30 companies, including Nortel, AT&T, NBC Internet, Bertelsmann, Qwest, Sun Microsystems and British Telecom, are working together to design communications architectures for broadband networks. The Broadband Content Delivery Forum hopes to speed up access to high-bandwidth content by using so-called co-location centers near ISPs, which would alleviate bottlenecks in long distance networking traffic. It will also focus on "content mediation" technologies that enable providers to recognize their subscribers and offer them highly personalized content and services. Noticeably absent from the group are Cisco and Lucent, which have been invited to join, but may instead prefer to set their own industry standards. (Financial Times 5 Apr 2000)

Category 22.4 *Accidental availability disruptions*

2000-04-13 **availability backup failure power airport travel disruption air traffic control**

RISKS 20 87

A power failure at 19:50 on 2000-04-10 affected Washington National Airport.. The backup generator failed at 20:41 and power was not restored until ~04:00 the next morning. The outage severely affected travelers and nearby hotels were swamped with stranded would-be passengers. Peter G. Neumann commented in RISKS, "Yes, they needed backup to the backup."

Category 22.4 *Accidental availability disruptions*

2000-05-14 **remote control automobile shutoff risk counterfeit hacking traffic chaos infrastructure protection**

RISKS 20 89

RISKS contributors Serguei Patchkovskii and John Pettitt both remarked on a stupid idea for stopping automobiles: a remote-control device using a receiver in each vehicle that could shut off the electrical system of the car at the push of a button. News reports apparently failed to note (1) the risks to other vehicles from cutting off power to a speeding automobile in a heavily-traveled lane; (2) the risks of counterfeit control devices. Pettitt wrote, "There is so much wrong with this idea it's hard to know where to start; even if the system was designed well enough that only "real" guns would work (very unlikely IMHO) a stolen "gun" could create total gridlock in a city."

Category 22.4 *Accidental availability disruptions*

2000-06-19 **availability bandwidth music trafficking network congestion satellite alternative**

Edupage, NewsScan, Wall Street Journal
http://interactive.wsj.com/articles/SB953765627187819503.htm

In January, Oregon State University administrators banned the Napster program from its networks, saying that the enormous volume of stolen songs was exceeding its bandwidth budget. Calculations showed a doubling time of only three months if the growth in song traffic were to continue unabated.

[In March,] Napster . . . adapted its software to use more "intelligent" search techniques and thus streamline the bandwidth needed to download requested files. The software change, which is the result of an unusual collaboration between the fledgling company and Indiana University, one of the first colleges to block the program, takes advantage of the fact that many colleges are now connected to the high-speed, next-generation Internet2. Now, when a Napster user asks for a file, the software first looks for the file on the user's campus network, then on the high-speed network. Those downloads take much less time than ones from the public network, thus reducing the load on the university networks. As a result, Indiana University . . . [said it was] ready to allow Napster back on campus . . . although network operators . . . [would] continue to monitor its use. (Wall Street Journal 23 Mar 2000)

Ever since MP3 music files took college campuses by storm, the problem of traffic congestion on campus networks has been growing. A typical case is Bucknell University, where 40% of the school's total Internet traffic is attributable to MP3 download services such as Napster. In an effort to resolve the gridlock, Bucknell officials called on alum Jeff Boulter, now a senior director of product development at Launch Media, to come up with a solution. The result is Launch College Direct, a service that uses iBeam Broadcasting's proprietary system to stream Internet content via satellite and put it on a local network that bypasses the school's Internet connection. The new service, which is free, will be deployed first at Bucknell and Georgia Tech. Launch plans to use it to deliver its own collection of music and music videos. (Los Angeles Times 19 Jun 2000)

Category 22.4 *Accidental availability disruptions*

2000-08-25 **availability DNS Domain Name Service servers access**

RISKS 21 03

When four of the 13 root servers at Network Solutions Inc failed, worldwide access, including HTTP, FTP, and SMTP, to all sites in the ".com" domain was interrupted for an hour .

Category 22.4 *Accidental availability disruptions*

2000-09-07 **electric power availability infrastructure protection**

NewsScan

Technology experts Peter Huber and Mark Mills charge that politicians have been ignoring a growing crisis caused by an energy-guzzling computer industry: "A personal computer and its peripherals typically boost power consumption in your home by about 5% per year — more if you run with the Wired crowd. But most of digital infrastructure's burgeoning demand for power occurs out of sight. Almost all the power it takes to deliver a conventional TV picture is used in the den where you watch it. The Web's invisible infrastructure, by contrast, consumes at least twice as much power as the hardware on your desktop. A Palm Pilot sips tiny amounts of power — but connect it to the Web and it can add as much new electric load as a refrigerator, in the servers, routers, and digital transmission systems used to feed it... A year ago we estimated that some 13% of U.S. power output was being used to manufacture and run computers and the sprawling infrastructure. It's more than that today. The country is 'siliconizing' everything — and behind every digital bit stands a bucket of electrons, behind every chip a power supply." Huber and Mills are coauthors of the Digital Power Report, a newsletter. (Wall Street Journal 7 Sep 2000)

Category 22.4 *Accidental availability disruptions*

2000-10-12 **availability electrical power process control bug error failure**

RISKS 21 09

At Eastbourne General Hospital, a computer-controlled backup electrical generator was prevented from cutting in to the circuits when mains power failed because the software appeared to "think" that the backup was already online. Later, when mains power actually was restored, the software prevented it from reaching the operating rooms because it "thought" that the backup generators were still running. As a result of the power interruption, medical staff had to complete a Caesarian section by flashlight ("torchlight" for British readers).

Category 22.4 *Accidental availability disruptions*

2000-12-03 **availability crash mainframe banking financial transactions stoppage outage**

RISKS 21 15

Peter G. Neumann summarized a report by Sam Zuckerman in the _San Francisco Chronicle_ of the 2nd of December: "On 1 Dec 2000, the nationwide Wells Fargo computer network crashed for a few hours, three days after WF had finished merging their computer networks with those of Norwest (which bought WF in 1998). One of four Hitachi Tritium 400 mainframes in the Minneapolis data center shut itself down, apparently after detecting some sort of anomaly. The result stopped all banking operations that depend on real-time interaction."

Category 22.4 *Accidental availability disruptions*

2000-12-28 **availability outage infrastructure**

RISKS 21 18

Glenn C. Lasher Jr. reported in RISKS' "On Thursday, 28 November 2000, 17 of the 21 telephone exchanges in the City of Schenectady NY were taken out of service by a water-main break (for those not familiar with the North American phone system, exchanges uniformly contain a range of 10,000 phone numbers). The Central Office serving downtown Schenectady is located on the block between Franklin and State Streets and Jay and Clinton Streets. The water main break was on Clinton St, and caused the closure of Clinton and State Streets. The break occurred at 3 AM, and the phones went out around 9 AM.

The cellular telephone networks appear to be unable to cope with the additional traffic. I received a frantic call from my wife, who called me at work from her cell phone to tell me the house phone was out. The signal quality was extraordinarily bad, as is the nature of CDMA digital when the cell is overloaded. One is left to assume that users of FDMA and TDMA-based phones may have been cut off completely, especially analog phone users, where the cells have a hard limit of 20 simultaneous calls."

The report continues with more details and an analysis of the situation that includes the following excellent points: "So, where do we begin on this one? Well, here are the RISKS:

1. Placement of mission-critical equipment below ground level leaves it susceptible to flooding. One might assume that an unusually heavy downpour might also have caused problems here.

2. This is a good example of network stress, looking at the behaviour of the cellular networks.

3. This is also a classic demonstration of a single point of failure. A problem in one location has cut off a critical service to an entire (although small) city. It does not matter if your service is through the IBOC (Verizon, in this area) or a CLEC (Sprint, AT&T, Met Tel, to name a few), all fo the equipment is owned and maintained by the IBOC and housed at the corner of Franklin and Clinton.

4. It is also a classic demonstration of diverse paths, as my Internet service continues to run. It does not pass through that same building, but is rather located a mile away on Eastern Parkway (or at least I believe that is the location). "

Category 22.4 *Accidental availability disruptions*

2001-01-04 **availability mystery down time bank crash ATM bank machines**

RISKS 21 18

Ulf Lindqvist reported to RISKS, "As reported in various Swedish news media, The Swedish bank Nordbanken has suffered repeated computer outages during late December and early January. The outages, each with a duration of several hours, shut down ATMs, Internet bank services, debit card purchases and office teller services for Nordbanken's 3.5 million customers.

In an article on the Swedish CNN Web site (cnn.passagen.se) 4 Jan 2001, Nordbanken CEO Magnus Falk says that the bank still does not know what caused the outages, but that they are now able to restart their system faster the next time it crashes... "

Category 22.4 *Accidental availability disruptions*

2001-01-10 **automated teller machines ATM single point failure operations security backup availability financial network**

RISKS 21 20

Andre Oppermann reported in RISKS that "On the day before Christmas Eve, usually the day with the highest turnover of the year in all shops, the whole Swiss debit-card (EC-Card) processing system of Telekurs broke down for more than two hours. Also getting Money from ATM's and the processing of on-line MasterCard credit card payments, which is handled by the same company, was interrupted." The cause: "…[On] Saturday 23 Dec 2000 at 13:15, a tape robot in an automated tape library in the data center of Telekurs, the sole operator of all EC card transactions, drops a tape on the floor which in turn leads to an error propagation which shuts down the whole EC and MasterCard card processing for approximately two and a half hours until 15:25." Oppermann noted that this was another example of a single point of failure and of poor business continuity planning.

Category 22.4 *Accidental availability disruptions*

2001-01-22 **availability power fluctuation outage generators calibration**

NewsScan

CAN SILICON VALLEY SURVIVE ENERGY CRISIS?
Rolling blackouts are wreaking havoc on the high-tech companies that form the bedrock of the Silicon Valley, and some are wondering how long they can rely on emergency back-up generators to keep their enterprises going. The blackouts have prompted talks between the Silicon Valley Manufacturing Group and state and local legislators regarding both short- and long-term fixes for the energy crisis. "What I've heard from many executives is, we want to stay and prosper in Silicon Valley," says Carl Guardino, president and CEO of the SVMG. "Yet at the same time, there's a very real recognition that if you do not have a reliable source of power and your products go down, it becomes extremely difficult to prosper." As one manufacturing firm COO puts it, "The loss of power for a few hours may not be a big problem, but recalibrating the equipment is." (EE Times 19 Jan 2001)
http://www.techweb.com/wire/finance/story/INV20010119S0015

Category 22.4 *Accidental availability disruptions*

2001-01-25 **availability failure operations**

NewsScan

MICROSOFT SITES DOWN 24 HOURS AS RESULT OF 'OPERATIONAL ERROR'
Various Microsoft Web sites, including MSN.com, MSNBC.com, and Microsoft.com, were down about 24 hours beginning Tuesday night, and a company spokesman emphasized that the problem was not with vandalism or with defects in Microsoft systems: "This was an operational error, and not the result of any issue with Microsoft or third-party products, nor the security of our networks." Security consultant Mark Loveless remarked: "If you look at how the Internet works at a really low level, it's a miracle anyone can get to anything. The thing is just so fragile." (Washington Post 25 Jan 2001)
http://washingtonpost.com/wp-dyn/articles/A43208-2001Jan24.html

---

Category 22.4 *Accidental availability disruptions*

2001-03-10 **availability theft backhoe attack single point of failure network**

RISKS 21 27

Gregory Soo reported in RISKS on another network interruption (as abstracted by Peter G. Neumann), "Another copper-theft attempt shut down the Rogers@Home cable Internet service in Canada on 8Mar2001 for over 12 hours, although the thieves wound up only with fiber-optic cable carrying Internet traffic to a U.S. backbone. Over 300,000 Ontario subscribers were affected, because of an outdated backup system and a single-point vulnerability. [Source: Vito Pilieci, *The Ottawa Citizen*, 10Mar2001, Rogers@Home: First cut is the deepest. Rogers admits 'rather outdated' network vulnerable to bumbling thieves."
http://www.ottawacitizen.com/hightech/010310/5075158.html

The RISKS moderator added: " [Coppers, robbers, backups, backbones, backhoes, back to basics. PGN]"

A later report added that exposed communications cables were attacked by unidentified rodents while workers were trying to repair the damage caused by the stupid thieves who couldn't tell the difference between copper cable and fiber-optic cable. Apparently the rodent cut service to some 300,000 network subscribers in the Niagara peninsula.

Category 22.4 *Accidental availability disruptions*

2001-03-21 **undersea cable break availability accident costs**

RISKS 21 30

According to _The Shanghai Daily_ of Mar 21, 2001, Korean-developed fishing nets that use anchors have been wreaking havoc with Chinese cybersurfers' access to the, ah, 'Net. The anchors rip through undersea cables when they are dragged up to several miles during strong tides; such accidents have repeatedly destroyedand then repaired at great expense. An article from _The Australian_, "The first serious break occurred on 9 Feb 2001 about 370km off China's coast, severing the main Internet link between China and the US. Although communications were partially restored during a repair process that stretched over two weeks, 22.5 million customers, including many in Shanghai, suffered slow service, the paper reported. On 9 Mar, the Internet backbone linking Taiwan and Shanghai was cut by a fishing net about 120km south of the city, affecting four million users. When that split was finally repaired on 19 Mar, authorities found another break in the undersea cable that will disrupt Internet services for a further two weeks. Each break costs about six million UN ($1.4 million) to repair, in addition to unknown business losses resulting from the Internet disruptions."

Category 22.4 *Accidental availability disruptions*

2001-03-27 **antivirus software performance degradation operating system design quality assurance**

RISKS 21 32

Joaquim Baptista found that his Windows-based antivirus program was seriously interfering with processing on his Windows 2000 server. For example, "processing involving a 53MB RTF file . . . . consumed after 3 hours of CPU" until he turned off the antivirus. Then the process completed in 15 minutes. He pointed out that running virus-prone Windows and its necessary antivirus products can delay "the computation at least 24 times, and the Pentium 700 becomes less than a Pentium 30! Linux suddenly seems a lot cheaper!"

Category 22.4 *Accidental availability disruptions*

2001-04-01 **wireless communications spectrum shortage availability regulation**

NewsScan

U.S. AGENCIES WARN OF SPECTRUM SHORTAGE
The U.S. Commerce Department, Defense Department and the Federal Communications Commission issued reports last week warning that there isn't enough radio spectrum to readily accommodate companies seeking to develop new wireless Internet services. The reports came in response to a request by the Clinton administration last year to review options for relocating some traditional government and industry uses of the radio spectrum to make way for so-called third generation (3G) wireless services. Officials at the Commerce Department and the Pentagon said they could identify only about 45 megahertz out of the 140 MHz studied, and that it would cost about $2 billion in engineering and other changes to free it up. Meanwhile, the FCC examined 190 MHz now used by schools and fixed wireless providers, but said any change would disrupt those services. Commerce Secretary Donald Evans said he was committed to finding a solution to the spectrum impasse, but a Pentagon official said the wireless industry has yet to prove that it really needs more spectrum. (Wall Street Journal 2 Apr 2001) http://interactive.wsj.com/articles/SB986160719120388594.htm (sub req'd)

Category 22.4 *Accidental availability disruptions*

2001-04-27 **availability artificial intelligence AI**

NewsScan

IBM PROJECT TO DEVELOP SELF-MONITORING SERVERS
IBM will devote one-fourth of its research & development budget to a project called eLiza, aimed at perfecting e-commerce server computers that, without intervention by human operators, will be able to detect and fix system problems, automatically install new software updates, perform load-balancing and security checks, and call on redundant systems to fill in for failing components. The company says that the new servers will be as easy to operate as a kitchen appliance, even though they will have processing power hundreds of times more power than the server computers of today. (AP/Washington Post 27 Apr 2001) http://washingtonpost.com/wp-dyn/business/latestap/A9273-2001Apr27.html

---

Category 22.4 *Accidental availability disruptions*

2001-07-06 **availability network logon failure**

NewsScan

PROBLEMS FOR MSN MESSENGER
Log-on problems were experienced this week by about one third of the more than 18 million people who use Microsoft Messenger, a free service that allows users to send instant text messages via the Internet to communicate individuals in their personal address books or "buddy lists." A Gartner Inc. analyst said philosophically: "They're certainly not the only ones who have had those kinds of problems. Computers and technology are not infallible." (San Jose Mercury News 6 Jul 2001)

Category 22.4 *Accidental availability disruptions*

2001-07-19 **availability accident fiber optic Internet backbone bandwidth throughput traffic**

NewsScan

TUNNEL FIRE DERAILS INTERNET SERVICE
Derailed train cars burning in a Baltimore tunnel have seriously damaged the area's fiber-optic cables, slowing Internet service and other communications traffic in the Mid-Atlantic states, with a ripple effect across the country. WorldCom, PSINet and AboveNet all reported problems with service, but said they had not yet been able to quantify the severity of the problems. Keynote Systems, which measures Web site performance, said the delay experienced by Internet users was the worst it has ever seen. "What we're seeing is a problem in the handshake between the backbones which serve as the Internet's infrastructure," said a Keynote spokeswoman. "These backbone providers hand off traffic to travel between them across the country." Keynote reported major slowdowns as far away as Seattle and Los Angeles that may be attributable to the train wreck. (AP Jul 19 2001) http://news.excite.com/news/ap/010719/18/train-derailment-communications

Category 22.4 *Accidental availability disruptions*

2002-02-15 **availability denial of service quality assurance service level agreement contractual obligation liability e-mail delivery reliability**

NewsScan

COMCAST: 'NOT 100% READY' TO DEAL WITH CUSTOMER PROBLEMS [4 Jan 2002]
Internet service problems were experienced by about 10% of 71,000 Comcast Cable customers in North Jersey who had been transferred to Comcast's own network after the failure of one offered by Excite@Home. "These kinds of problems are very typical when you're launching something new... Our folks were dealing with a large amount of calls at a single point in time. There were some early folks we brought on that were not 100% ready for everything customers were asking," says a company spokesperson. (New York Times 4 Jan 2002)
http://partners.nytimes.com/2002/01/04/technology/04COMC.html

COMCAST PROBLEMS AFFECT DELIVERY OF 300,000 MESSAGES [15 Feb 2002]
Comcast, the cable company and Internet service provider, said yesterday it would "work around the clock" to fix a technical problem that slowed delivery of 300,000 subscriber messages. Industry observers remember that when Excite@Home was on the way to declaring bankruptcy last year it had tried forcefully to make the point that cable companies Comcast and AT&T did not understand the complexity and costs of operating an Internet business. (New York Times 15 Feb 2002)
http://partners.nytimes.com/2002/02/15/technology/15PRIV.html

---

Category 22.4 *Accidental availability disruptions*

2002-02-20 **documentation DNS Domain Name System reserved addresses DoS denial-of-service**

RISKS 21 92ff

Gene Spafford wrote about an interesting problem that occurred in late 2001 when e-mail to one of his friends starting timing out. Investigation revealed that some forbidden origination addresses taken from the IANA list of reserved IP ranges were now being used legitimately. Spafford warned fellow system administrators to keep track of such changes regularly to avoid similar inadvertent self-inflicted denial of service.

James Graves chimed in with a thoughtful comment on the importance of keeping an up-to-date central database of operations knowledge so that problems can be solved once and then later occurrences can be solved immediately simply by looking up the solutions.

Category 22.4 *Accidental availability disruptions*

2002-03-31 **QA quality assurance DoS denial of service disaster availability**

RISKS 22 02

Lindsay Marshall reported in RISKS, >Barclays BACS payment system failed last week, and a large number of people did not get their pay check in their bank account. Normally this would not be a huge problem, but because it is Easter and so has two bank holidays leading up to the last day of the month it is a huge disaster.<

Category 22.4 *Accidental availability disruptions*

2002-04-08 **QA quality assurance operations merger combination bank financial systems failure payments errors debits transactions availability**

RISKS 22 03FF

A series of reports in RISKS noted that the merger of the 12 largest banks in Japan had caused a number of problems, including, "more than 30,000 transaction errors and 2.5 million delayed debits" and "2.5 million of the 3 million automatic debits scheduled to be processed on 1 Apr 2002, including utility and credit card bills, couldn't be made on that day".

Category 22.4 *Accidental availability disruptions*

2002-04-22 **credit card processing disaster recovery outage downtime customer service quality training intelligence stupidity obtuse pig-headed snot-nosed heap parrot droppings**

RISKS 22 04

In April 2002, Citibank VISA experienced a system error that prevented customers from paying their bills on the Web. When Bill Brykczynski tried to pay his bill by phone from his checking account, he found that the phone-based systems were also down, preventing the customer service people from taking his payment. A few days later, still unable to pay his bill using the Web, he called customer service again. This time, the agent asked him for a check number even though there was no check involved. Although Mr Brykczynski tried to explain that giving a check number in this case made no sense, the agent was having none of it. Brykczynski gave up. [MK writes: (1) have a disaster plan in place; (2) train your customer service people to THINK before they refuse an explanation.]

Category 22.4 *Accidental availability disruptions*

2003-01-08 **MSN Messenger instant messaging denial-of-service DoS outage**

NIPC/DHS

January 07, InfoWorld — MSN Messenger outage affects millions.

Microsoft Corporation's MSN Messenger service went down yesterday. According to a Microsoft spokesman, the service went down at approximately 9 a.m. EST, and the root cause of the outage is still unknown. The outage affected all 75 million worldwide users of Microsoft's .Net Messenger Service, including Windows Messenger and MSN Messenger subscribers, according to a statement from Larry Grothaus, lead product manager for MSN. The .Net Messenger Service is the back-end service that powers both the Windows Messenger and the MSN Messenger clients. MSN Hotmail e-mail service and other MSN services weren't affected, he said. Although service was restored for some users by about 2 p.m. EST, some users were still unable to log onto the messaging software later in the afternoon. Microsoft didn't have any more difficulties with the service late yesterday, but some users may still be shut out as the service scales back up, according to Grothaus.

Category 22.4 *Accidental availability disruptions*

2003-03-24 **Iraq war information online newspapers slow down**

NIPC/DHS

March 20, InternetWeek — War information demand slows U.S. military, Arab, alternative news sites.

The Arab news site Al Jazeera, U.S. military sites, and a U.S. alternative press site were among those suffering massive slowdowns and outages in the first day of the war in Iraq, according to Web performance measurement firm Keynote Systems. The slowdowns and outages were presumed to be due to overwhelming demand for access to information, rather than hacker attacks, said Eric Siegel, principle Internet consultant for Keynote. Likewise, British government sites are seeing significant slowdowns and outages. Siegel speculated that the entire online Arab world is turning to Al Jazeera for news, whereas the West has a diversity of sources online.

Category 22.4 *Accidental availability disruptions*

2003-04-22 **Global Positioning System GPS satellite failure denial-of-service risk**

NIPC/DHS

May 01, Wired — What if GPS fails?

Eighteen of the 28 satellites in the GPS constellation are operating past their intended lifespan or suffering from equipment failure. There have been three launch incidents in the past five years, and the Air Force, which maintains the 20-year-old network, is overburdened with competing space priorities. According to John Petersen, director of the Arlington Institute, a scenario-planning outfit in Virginia, "If GPS were to fail completely...civil aviation, trucking, shipping, and telecommunications would be worst hit." Internet activity would slow to a crawl, because many backbone operators rely on precise GPS time stamps to route data. The $12 billion market for GPS devices would be sent reeling, and the arrival of location-based wireless services would be set back years. However, Owen Wormser of the Office of the Assistant Secretary of Defense says GPS can withstand the loss of several satellites before becoming completely dysfunctional. "The system would degrade slightly, rather than seize up," he says.

Category 22.4 *Accidental availability disruptions*

2003-11-28 **cable failure UK Internet traffic affect denial-of-service**

NIPC/DHS

November 26, CNET News.com — Cable failure hits UK Net traffic.

A major failure in one of the key communications links between the United States and Europe appears to have caused widespread disruption to Internet services in the UK. The fault occurred Tuesday, November 25, in the TAT-14 fiber-optic cable system that connects the United States, Denmark, Germany, the Netherlands, France and the UK, and is understood to have left the system unusable for traffic. TAT-14 is a dual, bidirectional ring of cable, so a single serious fault should not be enough to break it, since traffic would still be able to flow between the countries on the ring. But a part of the cable near the U.S. coast had already suffered a technical fault earlier this month, which meant there was no built-in redundancy to cope with Tuesday's failure. According to BT, a member of the consortium of telephone companies that owns TAT-14, the U.S.-side fault should be fixed by the end of this week, which will bring the cable network online again. Tuesday's failure affected BT's voice calls, rather than its data services, but it is understood that a number of Internet service providers experienced faults.

Category 22.4 *Accidental availability disruptions*

2004-02-09 **DNS registration e-mail failure denial of service availability**

RISKS 23 18

WASHPOST REGISTRATION EXPIRED, NEWSROOM HAMPERED

Bill Hopkins wrote: *The New York Times*, 6 Feb 2004, reported (and not *too* smugly) that newsgathering at its rival *The Washington Post* was disrupted when registration lapsed for washpost.com, which the newsroom uses for e-mail.

The renewal notice from Network Solutions was delivered unnoticed to a "dropbox" (whether e-mail or the old-fashioned kind was not clear). However, the registration was renewed soon after the disruption started, before any squatters could jump on it. (Don't dwell on that image.)

Category 22.4 *Accidental availability disruptions*

2004-02-21 **process control sewage hotel Windows complexity availability**

RISKS 23 20

THE BLUE SCREEN OF SEWAGE

Wendy Grossman reports in RISKS that a modern hotel found itself without toilets because its Windows-based computer failed and "…whatever went wrong with it was so obscure that they had to get a technician from the company that supplied it on a plane down from Scotland to fix it and reboot." She asks, "The Blue Screen of Sewage?"

Category 22.4 *Accidental availability disruptions*

2004-03-02 **satellite solar noise availability denial of service outage communications ISP StarBand**

RISKS 23 24

THE SUN IS VERY BRIGHT

StarBand warned its customers of a "sun outage" in the spring and fall of the year when the sun is directly behind one of its communications satellites. The blast of intense radiation overpowers the downlink from the satellite to the home antennas, wiping out ISP access for a few minutes until the and the geosynchronous satellite move away from the sun.

Category 22.4 *Accidental availability disruptions*

2004-03-15 **denial-of-service DoS outage Microsoft Hotmail MSN Messenger**

NIPC/DHS

March 14, PC World — Outage hits Hotmail, MSN Messenger.

Internal technical problems at Microsoft closed down access for many MSN Messenger and Hotmail users, as well as some MSN Internet Access customers, for about eight hours Friday, March 12. Microsoft started receiving reports or problems with its instant messaging, Web based e-mail and dial-up Internet services at about 8:30 a.m. Pacific Time Friday, a company spokesperson says. The issue was identified at around 3 p.m. and solved an hour and a half later, she adds. "The outage was pretty significant in terms of the number of customers it affected, but by now the services should be up and running for everybody," the Microsoft spokesperson confirmed late on Friday afternoon. "It was a completely internal issue," the spokesperson says. The problem had nothing to do with hackers or the security patch for MSN Messenger that Microsoft released earlier this week, she adds. Microsoft did not disclose how many customers were unable to connect to those services in the interim. Service complaints came mostly from the U.S. and Canada, but users outside of North America may also have been affected, the spokesperson says. Users who were already connected to the services were for the most part able to continue using them, the issue primarily affected new log-ons, she says.

Category 22.4 *Accidental availability disruptions*

2004-03-22 **denial-of-service DoS outage Microsoft Hotmail MSN Messenger**

NIPC/DHS

March 19, IDG News Service — Hotmail, MSN Messenger hit with another outage.

Technical problems at Microsoft Corp. for the second time within a week caused trouble for users trying to connect to Hotmail and MSN Messenger, the company said Thursday, March 19. Users around the globe reported that they had problems signing on to the Hotmail and MSN Messenger services during about a three-hour period from 5:00 p.m. GMT until 8:00 p.m. GMT Thursday. Microsoft in a statement said it identified an issue that caused log-on and connectivity issues on some MSN services for a portion of its customers and has since solved it. The company did not specify the scope of the problem. The outage also affected connectivity for MSN Internet Access customers, Microsoft said. The company blames the problems on an unspecified internal problem and said it has no indication of any external causes such as cyberattacks. Although to users the problem was essentially the same, Microsoft said that Thursday's problems are different from those that caused an approximately eight-hour outage last Friday.

Category 22.4 *Accidental availability disruptions*

2004-04-26 **Internet connectivity lost SBC communications DSL subsriber**

DHS IAIP Daily; http://www.stamfordadvocate.com/news/local/state/hc−26154805
.apds.m0421.bc−ct−brf−−apr26,0,7979178.story?coll=hc−headlin es−local−wire

April 26, Associated Press — SBC customers cut off from the Internet.

Connecticut customers who use SBC Communications to reach the Internet were cut off from the World Wide Web much of Monday, April 26, after a fiber optic line was cut, the company said. Beverly Levy, an SBC spokesperson, said the outage had cut service to customers who used SBC Dial-up or the DSL broadband service. Levy said that the vendor whose fiber line was cut Monday morning worked around the problem by routing Connecticut Internet traffic through New Jersey. By 3 p.m. customers had service restored, the company said.

Category 22.4 *Accidental availability disruptions*

2004-05-01 **computer glitch air line testing availability**

DHS IAIP Daily;
http://www.cnn.com/2004/TRAVEL/05/01/delta.delays/index.html

May 01, CNN — Computer glitch grounds Delta flights.

A glitch in a Delta Air Lines computer system grounded flights out of Atlanta on Saturday afternoon, May 1, because data needed for takeoffs was not available, an FAA spokesperson said. Flights in some other cities were affected by the delays. Initially all flights east of Salt Lake City, Utah, were grounded, but within a couple of hours, flights were beginning to take off from airports other than Atlanta, Delta spokesperson Liza Caceres said. By early evening, the delays and cancellations were mostly confined to the Central and Eastern United States, Delta spokesperson Andy McDill said. The Atlanta-based airline uses the computer data in question to calculate weight and balance, and process passenger-related information, said Kathleen Bergen of the FAA. "It's not a safety-related issue," Bergen said.

Category 22.4 *Accidental availability disruptions*

2004-06-03 **confidentiality availability access death posthumous computers documents information wills**

http://www.nytimes.com/2004/06/03/technology/circuits/03data.html?8cir=&pagewanted=print&position=

PUT YOUR PASSWORD IN YOUR WILL?

A growing number of people are storing valuable family information on their computers. Some of them are applying security measures. Unfortunately, many of those people are forgetting to provide appropriate ways of getting into their secured computer systems if they are incapacitated. Other problems once access is gained:

* embarrassing or otherwise confidential information may be revealed inappropriately;
* intellectual property such as book manuscripts may not belong to the people who receive the computers;
* work-related files stored on personal computers may lead to liability for executors if there is a breach of confidentiality;
* important information may be available through Web accounts but the owners may forget to make the passwords available to families.

Category 22.4 *Accidental availability disruptions*

2004-11-26 **UK government computer failure denial of service DoS Department Work Pensions DWP network**

DHS IAIP Daily;
http://www.pcadvisor.co.uk/index.cfm?go=news.view&news=4331

November 26, IDG News Service — UK government hit with another large computer failure.

IT system failures continued to plague the UK government last week, when as many as 80,000 civil servants working for the Department of Work and Pensions (DWP) had to deal with what is being described as the biggest computer crash in government history. The DWP was carrying out a "routine software upgrade" on Monday, November 22, when the system crashed, leaving around 80 percent of the department's 100,000 desk machines disrupted or completely shut down, a DWP spokesperson said Friday, November 26. The problems lasted through most of Thursday, November 25. Microsoft and EDS (Electronic Data Systems) run the DWP's network. The DWP is responsible for providing a variety of state benefits to about 24 million people. It is believed that the crash was caused when an incompatible system was downloaded on to the entire network. The IT failure was only the latest in a string of serious computer system problems experienced by the department.

Category 22.4 *Accidental availability disruptions*

2004-12-08 **interactive games Halo Microsoft Xbox Internet traffic saturation bandwidth**

NewsScan; http://news.bbc.co.uk/1/hi/technology/4079397.stm

THE HALO EFFECT: NETWORK GRIDLOCK

The November 9 launch of Microsoft's Halo 2 Xbox game sparked an Internet traffic explosion that has continued into December and could herald chronic network congestion problems for Internet service providers, warns network monitoring firm Sandvine. "The explosion in Xbox Live traffic attributed to Halo 2 should be seen as a clarion call. ISPs need to enhance the broadband experience for these high-end users by prioritizing or reserving bandwidth for games," says Sandvine CTO Marc Morin. One of the main factors that can disrupt online gaming is "lag," in which there is a noticeable delay between the player's action and the game's response time. Installing software that makes networks more "intelligent" will be key to ISPs' ability to accommodate bandwidth-hungry gamers, says a Yankee Group analyst: "In the competitive broadband environment, operators need to differentiate the way they offer access to services like live-play gaming." (BBC News 8 Dec 2004)

Category 22.4 *Accidental availability disruptions*

2005-02-17 **denial of service DoS wireless mouse batteries**

RISKS 23 73

A BATTERY OF RISKS

Peter Pankonin pointed out yet another denial-of-service problem to worry about:

>This week a user complained that his computer system had locked up. He had typed away on a document for an hour (without saving of course) and couldn't move the mouse. Rebooting didn't fix the problem.

I was summoned to investigate, whereupon I noticed that the mouse pointer was indeed frozen at the center of the screen. Interestingly enough the keyboard still worked. Then I noticed that there was no red light emanating from his wireless optical mouse. After a quick installation of fresh batteries, the system magically recovered. Unfortunately, I was unable to recover the data lost after he rebooted.<

Category 22.4 *Accidental availability disruptions*

2005-04-15 **denial of service disaster recovery failure electric power backup generator automatic cutover alternate center monetary losses**

RISKS 23 84

MAJOR AUSTRALIAN TV STATION SUFFERS CHAIN OF DISASTERS

Peter G. Neumann summarized the sequence of disasters that cost a TV network a great deal of money:

Ch7 is one of the three national commercial TV stations in Australia. On the evening of 13 Apr 2005 they had a power failure and a back-up power failure in Melbourne, the automatic cutover to an alternate broadcast center failed, and the national phone system failed. All national transmissions come from a single center. Almost a million viewers had 41 minutes of the blank screen. Lost ad revenues were estimated at AU$600,000. The cause was apparently not known.

Category 22.4 *Accidental availability disruptions*

2005-06-15 **denial of service DoS software quality assurance QA database error indexing cellular mobile telephone**

RISKS; http://www.aftenposten.no/english/local/article1059215.ece 23 90

DATABASE ERROR MAKES HALF OF NORWAY'S CELLPHONES GO OFFLINE

Customers of Netcom, the second largest cellular provider in Norway, experienced sporadic or close to no service for days earlier this week. Companies that earlier abandoned "normal" phones and went all cellular are now installing land phones and/or IP phones.

>"Hundreds of thousands of customers and a government minister alike remained up in arms Tuesday, after losing use of their mobile telephones in recent days. … NetCom has actively promoted the concept of the "wireless office," and companies from building giant NCC to Aftenposten have made the switch, also as a means of saving money. Instead, it's left them vulnerable to communications breakdown and even dangerous situations."<

Problem? Database indexing issues, after a upgrade the previous week.

[Abstract, excerpt and comment from Olav Langeland]

Category 22.4 *Accidental availability disruptions*

2005-06-20 **denial of service outage cable network cash transactions mobile phone Internet services stock exchange**

RISKS; 23 91
http://www.informationweek.com/story/showArticle.jhtml?articleID=164900973

NEW ZEALAND OUTAGE SHUT DOWN STOCK EXCHANGE

A major outage in New Zealand Telecom Corp.'s cable network Monday disrupted data services, electronic cash transactions, mobile phone, and Internet services, as well as shutting down the nation's stock exchange for hours (the third time in the past nine months that data link failures have halted trading). Widespread disruption to business and private services was caused by two cable breaks on its North Island network. They were repaired by mid-afternoon Monday--at least five hours after they occurred. [Internet service and mobile phones were also out of commission due to two cable breaks. MHS]

The outage was caused by two separate incidents, including a fiber cable break north of the capital, Wellington, and a second cable being cut in Taranaki province on the west coast of North Island, more than 300 kilometers (188 miles) north of Wellington.

[Contributed by Marcus H. Sachs with additional abstracting by Peter G. Neumann]

Category 22.4 *Accidental availability disruptions*

2005-06-21 **Blackberry nationwide cellular network outage blackout denial-of-service DoS**

DHS IAIP Daily; http://www.nytimes.com/aponline/technology/AP−Blackberry−
Out age.html

BLACKBERRY NETWORK DOWN FOR HOURS

The BlackBerry e-mailservice suffered a nationwide outage Friday morning, June 17, but the nearly four-hour disruption only appeared to affect devices connected to certain types of cellular networks. Although Research in Motion Ltd. (RIM), which makes the popular mobile devices and provides a service connecting them to corporate networks, did not respond to phone calls seeking comment, Cingular Wireless, T-Mobile USA, and Nextel Communications Incorporated confirmed the outage. Cingular Wireless said RIM's outage lasted for three hours and 49 minutes, while T-Mobile USA said service was restored by noon EDT. Nextel Communication Incorporated reported that only some customers experienced trouble, and in those cases it was a delay in e-mails rather than a full-fledged service disruption. Both Verizon Wireless and Sprint Corporation said there were no complaints from their customers at all, possibly due to their reliance on cellular networks based on a technology called Code Division Multiple Access (CDMA); the three cellular carriers who experienced the service disruption rely on alternate technology-based cellular networks other than CDMA.

Category 22.4 *Accidental availability disruptions*

2005-06-22 **Blackberry nationwide cellular network outage blackout denial-of-service DoS second week**

DHS IAIP Daily;
http://news.com.com/BlackBerry+endures+another+outage/2100−1 039_3−
5758043.html?tag=nefd.top

BLACKBERRY ENDURES SECOND OUTAGE IN A WEEK

A number of BlackBerry handheld wireless devices experienced service problems on Wednesday, June 22, marking the second time in less than a week that the popular devices lost their data connections. A RIM representative said a hardware failure Wednesday triggered a backup system that operated at a lower capacity "than expected." Service has been restored, she said. BlackBerry customers, including a federal agency in Washington, DC, were told by RIM on Wednesday of an outage affecting accounts nationwide and across all carriers, according to an e-mailfrom RIM. Cell phone operator T-Mobile USA said an undisclosed number of its BlackBerry subscribers in Manhattan had only sporadic e-mailand other kinds of data service Wednesday. These problems were not related to what appears to be a nationwide Blackberry outage, according to a RIM representative.

Category 22.4 *Accidental availability disruptions*

2005-06-28 **Internet crash distributed denial-of-service Pakistan disaster**

DHS IAIP Daily;
http://www.cnn.com/2005/WORLD/asiapcf/06/28/pakistan.internet.reut/index.html

INTERNET CRASHES IN PAKISTAN

An undersea cable carrying data between Pakistan and the outside world has developed a serious fault, virtually crippling data feeds, including the Internet, telecommunications officials said. The system crashed late on Monday, June 27, and was still down on Tuesday evening. Many offices across the country ground to a halt as people realized it was not one of Pakistan's regular, but usually brief, technical hitches. An official at the Karachi stock exchange said Pakistan's main bourse was unaffected as it had its own internal trading system. Fixing it would entail an interruption for other countries using the link, including India, Dubai and Oman, one company official said. But the impact on neighboring countries would be limited and the repairs would begin at 4 a.m. on Wednesday (2300 GMT on Tuesday) to minimize any disruption, he said. Airlines and credit card companies were among the businesses hit by the crash. "It's a total disaster," said Nasir Ali, commercial director of the private Air Blue airline. "We have a Web-based booking system which has totally collapsed."

Category 22.4 *Accidental availability disruptions*

2005-08-08 **usability unexpected consequences bandwidth saturation**

RISKS 24 01

UNEXPECTED CONSEQUENCES OF LIMITED BANDWIDTH

Lauren Weinstein reported that Caltrans has started a 6-month experiment to put real-time travel times on freeway signs. The immediate result is apparently that traffic is tied up all over, as people slow down to read the signs!

[Abstract by Peter G. Neumann]

[MK comments: This is a case of bandwidth saturation of the limited human I/O channel (eyes), processor speed (reading) and computing architecture (lack of data buffer).] If everyone had an eidetic memory that could snap a visual image and then read it later, they wouldn't slow down to read the signs. Maybe we need brain v1.1?]

Category 22.4 *Accidental availability disruptions*

2005-08-31 **hurricane Katrina disaster telephone cable wireless link restoration communication recovery**

DHS IAIP Daily;
http://www.clarionledger.com/apps/pbcs.dll/article?AID=/20050831/NEWS0110/508310392/1260

RESTORING 260,000 LINES TO TAKE DAYS, WEEKS

Telephone and wireless communication could take weeks to restore in areas that took the brunt of Hurricane Katrina's blow. In less severe locations, it will likely only be days. Those time frames parallel how long it will likely take power companies to repair downed lines. Cellular companies report much of their loss of service has resulted from power outages that affected roughly 80 percent of the state. At a minimum, 260,000 telephones lines are down, resulting from uprooted trees that pulled cables as they fell, and water from flooding that seeped into equipment, said Mike Walker, a BellSouth spokesperson. Cingular Wireless said most network disruptions in Mississippi are in Jackson, Biloxi, Pascagoula, Bay St. Louis, Hattiesburg, Gulfport and Brookhaven. Alltel Corp., which has 190,000 Mississippi subscribers, reported 50 percent of its cell sites out of service. "We're moving more than 50 portable generators from Panama City, Florida" said the Arkansas-based company spokesperson Larry White. About 3,500 Alltel landline customers in Florence and Prentiss are also out of service, White said.

Category 22.4 Accidental availability disruptions

2005-09-01 **hurricane Katrina disaster communication restoration New Orleans repair**

DHS IAIP Daily;
http://www.computerworld.com/networkingtopics/networking/voip/story/0,10801,104324,00.html

TELECOMS STRUGGLING TO RESTORE SERVICE IN GULF COAST REGION

Cellular and other communication services have gradually improved in the Gulf Coast region, but service providers said Thursday, September 1, they still can't reach equipment in the flooded city of New Orleans to make needed repairs. Officials at Cingular Wireless LLC, Verizon Wireless, Sprint Corp. and BellSouth Corp. reported that with flooding and power outages in New Orleans, crews can't access cellular sites and switching stations for repairs. Of about 1 million landline phones in Lousiana that were out of service after the storm hit Monday, only 130,000 have been restored so far, said Bill Oliver, BellSouth's president of Lousiana operations Telecommunications have improved, however, in places such as Baton Rouge, Mobile, AL, and Pensacola, FL, company spokespersons said. The carriers are all relying on backup generators and in some cases portable generators and cellular transceivers carried on panel trucks. When possible, the carriers are also increasing power to rooftop cell sites in New Orleans to boost signals, the spokespeople said. "This is much worse than the 9/11 emergency. It is not just a part of a city like New York," said Jeff Kagan, an independent telecommunications analyst in Atlanta, GA. Wireless providers urged callers to use text messaging as an alternative to voice calls, partly because it requires less bandwidth.

Category 22.4 Accidental availability disruptions

2005-09-05 **hurricane Katrina disaster communications cut down satellite phone links**

DHS IAIP Daily; http://www.usatoday.com/tech/wireless/2005−09−05−satellite−phones_x.htm

SATELLITE PHONES PROVIDE CRITICAL LINK TO OUTSIDE WORLD

Satellite phones are serving as critical lifelines in Gulf Coast areas that lack other phone services. The National Guard, the American Red Cross, utility workers, reporters and people in search of relatives are among those using satellite phones to communicate. More than a million customers in Louisiana, Mississippi and Alabama are still without landline phone service, BellSouth says. And cell phone service has been spotty at best along the Gulf Coast. Typically, poles or wires were downed and power outages knocked out service to the digital gear and cell phone towers that are the lynchpins of landline and wireless networks. Satellite phones communicate directly with satellites that hover more than 500 miles high and work virtually everywhere around the globe. U.S. satellite phone providers Globalstar and Iridium note the phone generally must be used outdoors, and its antenna should be pointed skyward and have a clear line of sight to the satellite. Batteries supply about eight hours of talk time but can be recharged using a wall unit or a car's power adaptor.

Category 22.4 Accidental availability disruptions

2005-09-06 **hurricane Katrina disaster communications cut down wireless carriers restore service**

DHS IAIP Daily; http://rcrnews.com/news.cms?newsId=24016

WIRELESS CARRIERS BEGIN TO RESTORE SERVICE

Wireless carriers continued to make progress in re-establishing wireless communications to the Gulf Coast region following Hurricane Katrina. Cingular Wireless L.L.C. reported that as of Monday, September 5, it had fully restored service in Mobile, AL, and Jackson, MS, and that most coverage capacity has been re-established in and around Biloxi, MS. Customers in Meridian, Hattiesburg, and Gulfport, MS, were able to send and receive calls at reduced levels. Cingular also noted that some calls are going through in New Orleans and surrounding areas, but at reduced levels. BellSouth Corp. estimated that 810,000 lines remain impacted in the hardest-hit areas of the Gulf Coast. BellSouth released initial financial estimates of between $400 million and $600 million for both capital and expenses for network restoration. Verizon Wireless said it was providing improved service in areas southwest of New Orleans and was making progress in areas north of Lake Pontchartrain as well as in Baton Rouge and Mississippi. Central New Orleans continues to have widespread outages with limited coverage. Sprint Nextel Corp. reported similar progress in Mississippi, Alabama and Florida. T-Mobile USA Inc. said it had restored wireless service to a "significant level" in New Orleans. Alltel Corp. has restored service in portions of Jackson, MS, and much of Baton Rouge.

Category 22.4 *Accidental availability disruptions*

2005-09-07 **hurricane Katrina disaster communication cut down back on grid FCC**

DHS IAIP Daily;
http://www.wired.com/news/hurricane/0,2904,68779,00.html?tw= wn_tophead_1

GETTING THE GULF COAST BACK ON THE COMMUNICATIONS GRID

Hurricane Katrina wiped out communications systems throughout the Gulf States, and much of the impacted region remains cut off from voice and data service. On Friday, September 2, the Federal Communications Commission (FCC) held a conference call with wireless Internet service providers and infrastructure experts to coordinate volunteer efforts for storm-ravaged areas. FCC staff asked organizers to help gather data from those offering to donate resources -- from satellites to power generators to spare parts -- to help reconnect the effected areas. These improvised networks will initially target the needs of first responders tasked with rescue, relief and security services. FCC chief of staff Daniel Gonzalez says the commission is waiving some red tape to speed things up. Those waivers include permission for volunteers to launch a low-power FM radio station in Louisiana -- an LPFM, which would usually be called "pirate radio."

Category 22.4 *Accidental availability disruptions*

2005-09-19 **hurricane Katrina disaster denial-of-service accidental overwhelmed Red Cross Website online transactions donations**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1860051,00.asp

DONATIONS OVERWHELM RED CROSS STAFF, SITE

In the wake of Hurricane Katrina the Red Cross was faced with an overwhelmed IT infrastructure that was unable to handle the numerous online donations. After the tsunami in Southeast Asia last December, the Red Cross faced a huge number of online donations in which the IT staff worked long hours and offloaded some of the transaction processing to technology partners. However the donation system still wasn't ready for Hurricane Katrina. Dave Clarke, chief technology officer at the Red Cross stated, "As soon as we understood the magnitude of the tragedy, we knew the money would be coming in. When we began to see the initial transaction volume, we determined that if it continued on that growth curve, we would run out of capacity. And we knew we had to get ready."

Category 22.4 *Accidental availability disruptions*

2005-10-19 **Glitch outages California phone Internet Long Beach Hermose Beach Newport Beach Whittier Garden Grove Verizon software error**

DHS IAIP Daily; http://www.latimes.com/news/printedition/la−me−
phones19oct19
,1,4316471.story?ctrack=1&cset=true

GLITCH RESULTS IN PHONE OUTAGES FOR THOUSANDS

At least 150,000 customers in Southern California lost their phone and Internet service for up to 12 hours Tuesday, October 18, because of a computer glitch at a Long Beach central switching plant. The outage struck communities from Hermosa Beach to Newport Beach along the coast and as far inland as Whittier and Garden Grove. According to Verizon, the problem was caused by a software error in a downtown Long Beach office of Verizon Communications Inc. The malfunction corrupted the main software that connects calls and operates the local network.

Category 22.4 *Accidental availability disruptions*

2005-10-21 **disruption Level 3 network Internet availability**

DHS IAIP Daily; http://www.informationweek.com/showArticle.jhtml;jsessionid=
NXVYLVXLHSQCMQSNDBCCKHSCJUMEKJVN?articleID=172303270

MAJOR DISRUPTION IN LEVEL 3 NETWORK SLOWS INTERNET TRAFFIC

The Internet has been slower due to a major disruption of service from tier one carrier Level 3 Communications on October 21. The disruption caused increases in Internet response times and drops in availability. In addition, Websites were unreachable and service was shut off for some users. According to George Roettger, Internet security specialist for NetLink Services Inc, "I don't think I've ever seen an entire backbone network go down like that before."

Category 22.4 Accidental availability disruptions

2005-10-26 **Power outages phone FL batteries cellular Wilma Verizon Wireless**

DHS IAIP Daily;
http://www.palmbeachpost.com/search/content/business/epaper/2005/10/26/a2d_phones_1026.html

POWER OUTAGES DRAG DOWN PHONE SERVICE

Palm Beach County, FL, experienced widespread power outages Tuesday, October 25, after a day without electricity drained backup batteries for cellular and land-line systems in the aftermath of Hurricane Wilma. Most phones were operating Monday morning, October 24, while Hurricane Wilma crossed Palm Beach County and the Treasure Coast. After the power failed, those systems ran on batteries that generally last from four to 10 hours, depending on usage. Phone service was sporadic on Tuesday, as batteries began to fail. Chuck Hamby, spokesperson for Verizon Wireless, said "It worked very well through the storm, but then with the power outages, more and more cell sites dropped out of the network." Many cellular towers have built-in generators that can power the towers for five to seven days. Most providers said Hurricane Wilma did not cause much structural damage to phone lines and towers.

Category 22.4 Accidental availability disruptions

2005-12-01 **Internet Net denial-of-service DoS United Kingdom UK BT**

DHS IAIP Daily; http://news.com.com/Net+outage+hits+Brits/2100−1037_3−597837 4.html?tag=nefd.top

NET OUTAGE HITS UNITED KINGDOM

Internet service providers America Online, Virgin.net, Wanadoo and Zen Internet all confirmed that they had been hit by outages in the United Kingdom (UK) for several hours Wednesday, November 30. BT Group, the UK's telecommunications giant, said the glitches were due to a software problem linked to user authentication. Three servers were the cause of the problem, which affected customers randomly around the UK, according to BT. A BT representative said the outages resulted from increased congestion on the network, preventing fresh users from logging on, although those already connected via BT's broadband network experienced no service interruption. Although none of the ISPs could immediately provide precise information on how many end-users experienced problems, a Zen representative described the outages as "short term but significant," and a representative for Wanadoo said most ISPs had been touched by the problems at BT. AOL estimated that the number of its subscribers who experienced Internet connectivity problems could have reached 100,000. BT's representative said the company has launched an investigation into the problem.

Category 22.4 *Accidental availability disruptions*

2006-01-04 **availability airline reservation system business continuity disaster recovery failure**

RISKS 24 14

UNITED AIRLINES RESERVATION COMPUTER SYSTEM OUTAGE

According to a RISKS correspondent, the AP and Reuters newswire report describing the United Airlines reservation system outage on the 3rd of January 2006 was wrong. Peter Neumann summarized the reports as follows: "Computer Glitch Delays United Air Flights In US, 3 Jan 2006 United Airlines' domestic flights were delayed up to 90 minutes Tuesday night because of an outage in the computer system controlling United's check-ins and reservations, which went down for about five hours around 5 p.m. CST Wednesday. Passengers were checked manually, and flights were delayed up to 90 minutes." However, the corresepondent personally saw delays of far more than 90 minutes at Los Angeles International Airport (LAX). He described the debacle as follows (quoting directly):

* No self-check-in kiosks working, reservationists answering the phone with "our computers are still down", which meant every queue had more than 500 people in it, spilling out on the sidewalk outside the terminal, and they were using "the manual procedure". The people close to the head of the queue had been waiting for more than two hours, they said, and they dispensed with the special queues for premier or 1k, just to spread the pain equally.

* They weren't calling out specific flights to try to fill them.

* They had most of the check-in desks empty. Obviously they don't have enough people trained in the manual procedure to alleviate the bottleneck.

* The woman working the lines (with a megaphone) was apologetic, but wouldn't answer questions, not even frequently asked questions which did not have to with individual problems, such as "if I miss my last flight will you provide a hotel? Or is my ticket now refundable if I fly another carrier?

* some reports are they were flying planes half-empty because people couldn't get to the gates. Of course, they weren't announcing how long they were holding flights to try to board them.

* TSA, not known for their flexibility, was not allowing people to go to the gates directly with a boarding pass. Even an e-ticket receipt with a seat assignment wouldn't get you there.

United stock is down 2% today, trading at around a buck a share. Their earnings are -$43 per share at the moment. I'll bet this was an expensive failure."

Category 22.4 *Accidental availability disruptions*

2006-03-15 **BlackBerry user denial-of-service DoS software upgrade RIM**

DHS IAIP Daily; 23
http://news.com.com/Some+BlackBerry+users+frustrated+by+outa ges/2100−1041_3−6050225.html?tag=nefd.top

SOME BLACKBERRY USERS FRUSTRATED BY OUTAGES.

Research In Motion (RIM) confirmed Wednesday, March 15, that several BlackBerry customers' service experienced outages this week due to a software upgrade, which was the feared outcome if RIM had been forced to implement its workaround technology. Several customers with Cingular, T-Mobile, Verizon Wireless and Sprint's Nextel service reported delays, outages and problems with their BlackBerry Internet Service starting early this week and continuing through Wednesday. RIM confirmed that it was responsible for the problems: "Some BlackBerry Internet Service customers experienced intermittent service earlier this week due to an issue that appears to have stemmed from a software upgrade in RIM's infrastructure. Service appears to be operating at normal levels at this time. RIM continues to monitor the infrastructure closely."

Category 22.4 *Accidental availability disruptions*

2006-03-29 **vulnerability spider bot search engine Javascript cookies bypass design flaw data integrity deletion erasure**

RISKS 24 22

THE SPIDER OF DOOM

Alex Papadimoulis had a fascinating tale of a disappearing Web site. In brief, a government Web site was converted to a content-management system that would allow employees to manage their own Web pages without having to go through a Web designer. It worked fine for five days, but on the sixth day all the content was gone! The entire Website had been erased by an external user that turned out to be the GOOGLE web crawling spider.

>After quite a bit of research (and scrambling around to find a non-corrupt backup), Josh found the problem. A user copied and pasted some content from one page to another, including an "edit" hyperlink to edit the content on the page. Normally, this wouldn't be an issue, since an outside user would need to enter a name and password. But, the CMS authentication subsystem didn't take into account the sophisticated hacking techniques of Google's spider. Whoops.

As it turns out, Google's spider doesn't use cookies, which means that it can easily bypass a check for the "isLoggedOn" cookie to be "false". It also doesn't pay attention to Javascript, which would normally prompt and redirect users who are not logged on. It does, however, follow every hyperlink on every page it finds, including those with "Delete Page" in the title. Whoops.

After all was said and done, Josh was able to restore a fairly older version of the site from backups. He brought up the root cause -- that security could be beaten by disabling cookies and javascript -- but management didn't quite see what was wrong with that. Instead, they told the client to NEVER copy paste content from other pages.<

Steve Summit added in RISKS 24.23

>I can see Joe Loughry's tongue in his cheek pretty clearly from here, but it might not be obvious to a casual reader that this was manifestly *not* a "hacking" attempt by Google. That a simple and naïve traversal of some hyperlinks could cause content to be deleted makes it pretty obvious that something was badly wrong with the site's editing and access-control model.

Needless to say (or, it *ought* to be needless, but is actually pretty needful), security that assumes that visitors *will* have cookies and JavaScript enabled, that can be compromised if these features are disabled, is no security at all. That content could have been inadvertently deleted by any visitor to the vulnerable website; google's spider just happened to get to it all first.<

Category 22.4 *Accidental availability disruptions*

2006-04-06 **Microsoft MSN search denial-of-service DoS outage**

DHS IAIP Daily; 23
http://www.computerworld.com/developmenttopics/websitemgmt/story/0,10801,110305,00.html

MSN SEARCH ENGINE SUFFERS HOURS-LONG OUTAGE.

Microsoft Corporation's MSN search engine, the third most popular in the U.S., suffered an hours-long outage on Thursday, April 6, as queries returned an error message instead of Webpage results. The outage began around 8:30 a.m. PDT and ended around noon, according to a spokesperson for Microsoft. The company is still trying to determine what caused the problem.

---

23 Internet tools

Category 23 *Internet tools*

1997-01-29 **ActiveX diddling**

RISKS 18 80 ff

The CHAOS Computer Club of Germany demonstrated how a rogue ActiveX applet can insert a fraudulent transaction in a victim's stack of pending QUICKEN transfer orders.

Category 23 *Internet tools*

1997-02-21 **ActiveX**

RISKS 18 83

Microsoft responded to the CHAOS Computer Club demonstration of a data diddling attack via ActiveX by saying that the same problem could have occurred using Java and Netscape.

Category 23 *Internet tools*

1997-03-04 **digital signatures Authenticode ActiveX**

RISKS 18 85 ff

Bob Atkinson, chief architect of Microsoft's Authenticode system for signing ActiveX controls, responded to criticism of his company's approach to security of third-party executables. Among the key points: Microsoft has never claimed that it would certify the safety of other people's code; authentication is designed solely to permit identification of the culprits _after_ malicious code is detected; Explorer-based distribution of software is no more risky than conventional purchases through software retailers. Subsequent correspondence chastised Mr Atkinson for omitting several other key points; e.g., interactions among ActiveX controls can violate system security even though individual controls are apparently harmless; there is no precedent in fact for laying liability at the feet of software developers even when you _can_ find them; under attack, evidence of digital signature is likely to evaporate from the system being damaged; latency of execution of harmful payloads will complicate identification of the source of damage; malice is not as important a threat from code as incompetence; Microsoft has a history of including security-threatening options such as automatic execution of macros in Word without offering any way of turning off the feature; a Web site can invoke an ActiveX control that is located on a different site or that has already been downloaded from another site and can pass that control unexpected arguments that could cause harm.

Category 23 *Internet tools*

1997-03-06 **Java ActiveX**

RISKS 18 87

Dr Gary McGraw of Reliable Software Technologies in Sterling, VA reported on some new examples of known security problems in JAVA and ActiveX. A minor JAVA problem concerned the ability to determine a client's IP address without permission. A more serious ActiveX problem allows a server to connect to any arbitrary TCP/IP port on a client system even if a firewall is configured to prevent such connections.

Category 23 *Internet tools*

1997-03-28 **JavaScript denial of service MIME attachment**

RISKS 18 95

A user posted a warning to a USENET group about a Web page that spawns endless windows from within a Web page. The original Web site was designed as a demonstration of a possible denial of service attack. Unfortunately the USENET poster included the actual HTML code for the offending Web page in his USENET posting. Since Netscape Navigator automatically formats such attachments and executes the script, the USENET message had the same effect as the demonstration Web page. Denial of service by remote control. . . .

Category 23 *Internet tools*

1997-04-03 **ActiveX flaw**

Reuters

CEO Scott McNealy of Sun Microsystems, in his keynote address at the JavaOne Conference, showed how when a specially written program containing ActiveX could be downloaded by a remote user and then took over the user's computer and rifled its files for personal financial information. The ActiveX control had been signed but was still malicious.

Category 23 *Internet tools*

1997-04-28 **YAJF Java flaw authentication**

RISKS 19 11

Professor Ed Felten's team at Princeton discovered yet another Java security flaw. This one applies to version 1.1.1 of the Java Development Kit (JDK) and version 1.0 of the HotJava browser from Sun Microsystems. Seems that there are two problems: (1) "If an applet's signer is labeled as trusted by the local system, then the applet is not subject to the normal security restrictions." (2) The current flaw is that an applet can redefine the Java interpreter's perception of who signed it. By searching for the signers trusted by the client system, a hostile applet could bypass all normal security restrictions. The bug was fixed in release 1.1.2 of the JDK.

Category 23 *Internet tools*

1997-05-22 **JAVA ActiveX**

EDUPAGE

Pushing executable files out from servers to client systems is outstripping security provisions in JAVA and ActiveX. JAVA is supposed to integrate some security measures into its code (the "sandbox"), but in contrast, Microsoft's ActiveX relies only on certification of origin to reduce risks of Trojans and just plain programming errors. Prof. Ed Felten of Princeton University's Safe Internet Programming project said, "Once an Active X control is running on your machine, you have no way to constrain what it does."

Category 23 *Internet tools*

1997-08-08 **JAVA applet Microsoft Internet Explorer**

C|Net news.com http://www.news.com/News/Item/0,4,13226,00.html?latest

Ben Mesander, a Java developer with CreativeConcepts in Boulder, Colorado, discovered that Internet Explorer 3.x and 4.0 allows Java applets to open a network connection to a server other than the one from which they were downloaded. Such a bug would permit a Trojan applet to redirect interactions from a legitimate site to a rogue site without notifying the user of the change. For example, a modified applet on a bank site might redirect a user to a pirate site where confidential information could be seized. Because Java normally does not permit such connections, and because Netscape Navigator did not show the same problem, analysts concluded that the bug was in Microsoft Internet Explorer.

Category 23 *Internet tools*

1997-10-01 **JAVA vulnerability**

RISKS 19 40

The Reliable Software Group at University of California Santa Barbara published a new attack on JAVA applications using the CLASSPATH feature. The vulnerability allows a malicious server to spoof an innocent target site, making it look as if the client is communicating with the desired site (e.g., a bank) while actually the data are flowing, unencrypted, to the malicious hijacker site. Check <http://www.cs.ucsb.edu/TRs/> to see if the report makes it to the UCSB Dept of Computer Science compilation of technical reports.

Category 23 *Internet tools*

1997-10-17 **JAVA**

RISKS 19 41

Another JAVA problem surfaced in October when researcher Andre L. Dos Santos at the Reliable Software Group of the University of California Santa Barbara found a new exploit of the CLASSPATH feature. The demonstration program sends confidential data to a rogue site instead of to the bank that requested it.

Category 23 *Internet tools*

1997-11-28 **data diddling e-mail Java HTML Explorer browser**

RISKS 19 49

A RISKS correspondent reported that HTML-enabled e-mail was immediately interpreted by MS Internet Explorer 4.0 because its autopreview mode was active. The e-mail downloaded and executed a Java applet that opened a connection to a foreign Web site and would have gone on to many other sites had the user not interrupted it.

Category 23 *Internet tools*

1998-01-11 **ActiveX security flaw hole registry authentication signature**

BUGTRAQ, http://www.network-security.com/activex/DLLMainAttack.html

A hacker discovered a major security flaw in Internet Explorer and reported it to Microsoft before publishing it on the Net: "Controls that are registered in the Windows registry file become `trusted' and are not subjected to the HIGH / NONE safety level security service. It is possible to use a signed control to introduce an unsigned control onto the desktop. The unsigned control is registered in the Windows registry and can then be activated AT ANY TIME IN THE FUTURE by any HTML page." In other words, a Trojan horse control could allow further controls to be executed regardless of security level. As an aside, the hacker evidently could not wait for a patch before publishing the hole to the world.

Category 23 *Internet tools*

1998-05-14 **intellectual property JAVA Microsoft Sun court injunction**

EDUPAGE

In the continuing legal battle over the purity of JAVA implementations, Sun Microsystems, the owner of the unadulterated product, sued Microsoft for unauthorized modifications to its version of JAVA. The JAVA implementation on Windows98 was alleged to be incompatible with standard JAVA, and Sun argued that these changes constitute a breach of contract. In May, Sun applied for an injunction prohibiting distribution of Windows98 days before its official release. The court hearings began in September.

Category 23 *Internet tools*

1998-07-02 **malicious code applets controls Java ActiveX**

EDUPAGE

ICSA, Inc. organized the Malicious Mobile Code Consortium to fight dangerous Java applets and ActiveX controls. The industry group said it would focus on education, certification and information exchange.

Category 23 *Internet tools*

1998-07-16 **mobile code applet Java Navigator ClassLoader**

RISKS 19 86

The Secure Internet Programming Lab at Princeton University found another flaw in Java that " allows a malicious applet to disable all security controls in Netscape Navigator 4.0x. After disabling the security controls, the applet can do whatever it likes on the victim's machine, including arbitrarily reading, modifying, or deleting files. We have implemented a demonstration applet that deletes a file."

Category 23 *Internet tools*

1998-07-30 **QA virus malicious code applet control e-mail**

EDUPAGE

Several organizations, from CERT-CC to the hacker group L0PHT, issued advisories warning that many popular e-mail programs (e.g., PINE, MS-Outlook versions, and Netscape Mail) were vulnerable to a buffer overflow error that would allow execution of arbitrary code for nefarious purposes.

Category 23 *Internet tools*

1998-09-29 **browser JavaScript quality assurance QA script malicious**

EDUPAGE

Netscape posted patches against a theoretical weakness in its Navigator browser. The flaw would have allowed malicious code written in JavaScript to access data in the Netscape cache (not including SSL pages as long as SSL-caching was disabled).

Category 23 *Internet tools*

1998-12-18 **mobile code Java applet ActiveX control Javascript proxy**

InternetWeek
http://www4.zdnet.com/intweek/stories/news/0,4164,2177494,00.html

Trend Micro Inc. launched its InterScan AppletTrap in January 1999 to identify and block malicious applets and controls written in Java, Javascript and ActiveX.

Category 23 *Internet tools*

1999-01-04 **Java virtual machine applet corrupt crash Windows JVM**

Newsbytes

Fabio Ciucci and the Anfy Java Collective of Italy <http://www.anfyjava.com> warned in 1998 that weaknesses in Microsoft's "corrupt" version of the Java Virtual Machine made it vulnerable to applets that could crash client systems. Although Microsoft published a patch to correct the security hole, it did not publicize the patch. In January, Ciucci and his colleagues warned that the recent revision of the MS JVM [available from <http://www.microsoft.com/java/vm/dl — vm31.htm> or from <http://www.microsoft.com/windows/ie/download/jvm.htm>] were still vulnerable — the company had failed to integrate the former patch in the new system. As a result, malicious applets — increasingly available on the Net — could cause incomprehensible JVM hangs and even outright crashes of the Windows operating system for users unaware of the need for a patch.

Category 23 *Internet tools*

1999-01-06 **flaw spreadsheet Excel weakness HTML Web browser flaw**

InternetWeek
http://www.zdnet.com/intweek/stories/prtfriendly/0,4557,2182861,00.html

A flaw in MS-Excel would allow malicious code written in HTML and downloaded from a Web site to execute arbitrary code secretly downloaded to the user system. The security hole would theoretically allow powerful violations of security such as sending confidential files to the hostile site. MS immediately provided a patch to disable the CALL function within Excel. Padgett Peterson, writing in RISKS 20.15, warned, "What is not well understood is that this exploit is actually multifaceted - there are a number of HTML constructs and a number of applications that can be used. The choke point seems to be in the (Windows) Registry which decides which applications (mostly Microsoft's) are considered "safe", that no warning screen is generated on network download/launch sequences for these applications. EXCEL is just one of these."

Category 23 *Internet tools*

1999-01-15 **Java active content book publication Web mobile code**

RISKS 20 16

Drs Edward Felten and Gary McGraw published a new book about mobile code security. _Securing Java: Getting down to business with mobile code_ was published by John Wiley & Sons in January 1999. In addition to the physical book, these experts put the entire text online at <http://www.securingjava.com>. The hope was that the free edition will not harm sales of the paper book.

Category 23 *Internet tools*

1999-05-01 **mobile active code ActiveX Java malware**

InternetWeek

Several companies announced products for identifying hostile or otherwise dangerous active content pulled from Web pages and executed on client systems. Finjan Software released a new version of its SurfinShield program; Security-7 announced a quarantine server for pre-emptive execution and validation of applets and controls. Experts warned that it is increasingly difficult to justify interdicting all Java, JavaScript and ActiveX execution because so many trading partners are depending on these tools for production Web applications. Rutrell Yasin, writing in InternetWeek, classified mobile code threats as follows:
* System modification: applets can exploit holes in Java, allowing hackers to alter database information;
* Privacy invasion: applets can be used to crack passwords or impersonate e-mail identities;
* Denial of service: applets can shut down a machine;
* Nuisance: applets can launch annoying attacks such as opening multiple windows.

Category 23 *Internet tools*

1999-05-10 **mobile malicious code**

NATIONAL POST (Canada)

Edmonton computer expert Tom Cervenka, member of the vulnerability-tracking "Because We Can" group <http://www.because-we-can.com> identified a vulnerability in the Web site of e-Bay, a major on-line auction site. The vulnerability would allow a criminal hacker to insert harmful JavaScript code on an eBay Web page; the code could then do anything JavaScript allows, including password stealing. Unfortunately, eBay officials dismissed the vulnerability as unimportant.

Category 23 *Internet tools*

1999-08-03 **Internet Explorer browser flaw weakness vulnerability bug macro execution Word Excel Powerpoint load alert patch**

New York Times via EDUPAGE

Because Microsoft believes that word processing, spreadsheet and presentation software should allow automatic execution of macros — thus turning these products into programming languages — they also allowed their Internet Explorer browser to load these programs without alerting users. In August, Microsoft scrambled to issue patches to correct this design flaw so that unwary users would not be subjected to hostile code merely by downloading documents from a hostile Web site or by reading e-mail attachments. The principle still stands: don't double-click attachments of uncertain origin or unvalidated safety.

Category 23 *Internet tools*

1999-09-29 **MS-IE5 Microsoft Internet Explorer browser bug vulnerability ActiveX control download Web firewall**

InfoWorld Electronic, IS/Recon, NTBUGTRAQ

Georgi Guninski, browser-bug discoverer extraordinaire, notified Microsoft of yet more security vulnerabilities in Internet Explorer 5. In August, he found that a malicious ActiveX control could install arbitrary code in the Windows Startup folder. See Guninski's Web site <http://www.nat.bg/~joro> for details but be aware that his demonstration code actually does subvert your security unless you set Internet Zone security setting to "High", or disable the setting "Script ActiveX controls marked safe for scripting." In September, he showed that a malicious JavaScript could download executable code from a Web site (typically allowed by firewalls) and the hostile code could then send itself to any IP address back out through the firewall. Microsoft recommended disabling IE5's active scripting.

23.1 Java

Category 23.1 *Java*

2001-11-15 **Java cookies protocol vulnerability exposure confidentiality penetration patch repair bug QA quality assurance**

RISKS 21 76

A RISKS correspondent reported, "A flaw was discovered in the way Internet Explorer's about: protocol handles javascript requests, enabling a malicious web site to gain access to cookie information on the client's hard drive."
http://www.securityfocus.com/cgi-bin/vulns-item.pl?section=discussion&id=3513
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms01-055.asp

---

Category 23.1 *Java*

2002-03-10 **Java vulnerabilities ICAT CVE CGI**

ICAT Metabase

The ICAT Metabase < http://icat.nist.gov/icat.cfm > for the Common Vulnerabilities and Exposures (CVE) database reported the following vulnerabilities involving Java for the period from 1 Jan 2001 to 10 Mar 2002:

CAN-2000-1117: The Extended Control List (ECL) feature of the Java Virtual Machine (JVM) in Lotus Notes Client R5 allows malicious web site operators to determine the existence of files on the client by measuring delays in the execution of the getSystemResource method. Published Before: 1/9/2001 Severity: Low

CAN-2001-0068: Mac OS Runtime for Java (MRJ) 2.2.3 allows remote attackers to use malicious applets to read files outside of the CODEBASE context via the ARCHIVE applet parameter. Published Before: 2/12/2001 Severity: Medium

CAN-2001-0186: Directory traversal vulnerability in Free Java Web Server 1.0 allows remote attackers to read arbitrary files via a .. (dot dot) attack. Published Before: 5/3/2001 Severity: High

CAN-2001-0297: Directory traversal vulnerability in Simple Server HTTPd 1.0 (originally Free Java Server) allows remote attackers to read arbitrary files via a .. (dot dot) in the URL. Published Before: 5/3/2001 Severity: Low

CAN-2001-0307 Summary: Bajie HTTP JServer 0.78 allows remote attackers to execute arbitrary commands via shell metacharacters in an HTTP request for a CGI program that does not exist. Published Before: 5/3/2001 Severity: Medium

CAN-2001-0308: UploadServlet in Bajie HTTP JServer 0.78 allows remote attackers to execute arbitrary commands by calling the servlet to upload a program, then using a ... (modified ..) to access the file that was created for the program. Published Before: 5/3/2001 Severity: Medium

CAN-2001-0324: Windows 98 and Windows 2000 Java clients allow remote attackers to cause a denial of service via a Java applet that opens a large number of UDP sockets, which prevents the host from establishing any additional UDP connections, and possibly causes a crash. Published Before: 5/3/2001 Severity: High

CAN-2001-0926: SSIFilter in Allaire JRun 3.1, 3.0 and 2.3.3 allows remote attackers to obtain source code for Java server pages (.jsp) and other files in the web root via an HTTP request for a non-existent SSI page, in which the request's body has an #include statement. Published Before: 11/28/2001 Severity: Medium

CAN-2001-1008: Java Plugin 1.4 for JRE 1.3 executes signed applets even if the certificate is expired, which could allow remote attackers to conduct unauthorized activities via an applet that has been signed by an expired certificate. Published Before: 8/31/2001 Severity: High

CVE-2000-1099 : Java Runtime Environment in Java Development Kit (JDK) 1.2.2_05 and earlier can allow an untrusted Java class to call into a disallowed class, which could allow an attacker to escape the Java sandbox and conduct unauthorized activities. Published Before: 1/9/2001 Severity: Medium

CVE-2001-0126: Oracle XSQL servlet 1.0.3.0 and earlier allows remote attackers to execute arbitrary Java code by redirecting the XSQL server to another source via the xml-stylesheet parameter in the xslt stylesheet. Published Before: 3/12/2001 Severity: High

CVE-2001-0137: Windows Media Player 7 allows remote attackers to execute malicious Java applets in Internet Explorer clients by enclosing the applet in a skin file named skin.wmz, then referencing that skin in the codebase parameter to an applet tag. Published Before: 3/12/2001 Severity: High

Category 23.1 *Java*

2003-01-15 **information warfare interoperability intellectual property**

NewsScan

SUN SUES MICROSOFT FOR DAMAGES OVER JAVA
Sun Microsystems has filed a new lawsuit against Microsoft, alleging that Microsoft's business practices damaged the market for Sun's Java programming language. It also alleges that Microsoft kept more than 20 technologies secret, preventing Sun and other server makers from incorporating the features needed to maker their servers work with Microsoft's software. Sun's suit follows an earlier filing in 1997, which focused on a contractual dispute over Microsoft's licensing of Java. The two companies eventually settled out of court. This time around, however, Sun is seeking, potentially, billions of dollars in damages in addition to an injunction that would require Microsoft to distribute the latest version of Java, to disclose technical information so that other companies can write compatible software, and to cease bundling some Microsoft products. The Sun suit follows similar suits recently filed by AOL Time Warner and Be Inc. (Wall Street Journal 11 Mar 2002)
http://online.wsj.com/article/0,,SB1015608994249257320.djm,00.html (sub req'd)

SUN'S CHRISTMAS COMES EARLY IN VICTORY OVER MICROSOFT
A U.S. district court judge ruled Monday that Microsoft had violated Sun Microsystems' copyright for its Java software and ordered the software giant to include Sun's version of Java with its Windows operating system, handing Sun a double-barreled victory over its high-tech rival. The case stems from Sun's claims that Microsoft dropped Sun's Java software in favor of its own variation, which Sun alleges is incompatible with its technology. "Unless Sun is given a fair opportunity to compete in a market untainted by the effects of Microsoft's past antitrust violations, there is a serious risk that in the near future the market will tip in favor of .Net, that it is impossible to ascertain when such tipping might occur in time to prevent it from happening, and that if the market does tip in favor of .Net, Sun could not be adequately compensated in damages," wrote Judge J. Frederick Motz in his decision. Microsoft says it plans to appeal the decision. (CNet News.com 23 Dec 2002)
http://news.com.com/2100-1001-978786.html

SUN AND MICROSOFT GET SET FOR JAVA LEGAL BATTLE
Sun and Microsoft are appearing in federal court to argue their positions before U.S. District Judge J. Frederick Motz, who will be ruling on Sun's request for an injunction requiring Windows to include Sun's latest Java software immediately, pending resolution of the larger Sun lawsuit against Microsoft. Sun claims Microsoft has gained an unfair advantage by shipping Windows with a version of Java that is both outdated and strongly biased toward Windows, even though Java is meant to make it possible for programs to run on all computers, regardless of the operating system. (AP/San Jose Mercury News 15 Jan 2003)

Category 23.1 *Java*

2003-06-10 **sun java everywhere growing market**

NewsScan

SUN PROCLAIMS 'JAVA EVERYWHERE'
Sun Microsystems hopes its new "Java Everywhere" branding effort will be as successful as Intel's "Intel Inside" campaign was, and claims that Java "means a new way of interacting with consumers, giving them new experiences," providing Sun with "a new electrified brand, more market opportunities, more fun, more money." Sun executive vice president Jonathan Schwartz continues: "The opportunity for Java growing the market is everywhere, to create the best sites, devices, games, stores, Web games, smart cards, and security." (EWeek 10 Jun 2003)

Category 23.1 *Java*

2003-06-12 **hp dell java sun microsoft richard green**

NewsScan

HP AND DELL PCs TO INCLUDE JAVA
Hewlett-Packard and Dell will be including Java as a standard component on their personal computers. (Java, a creation of Sun Microsystems, makes it easy to run a program on many different kinds of computers.) Sun, of course, is happy that, as a result of the 1998 Microsoft antitrust trial, computer manufacturers can no longer be pressured by Microsoft to run only that company's products. Sun executive Richard Green says, "The back and forth with Microsoft has limited the success of Java on the personal computer desktop. It is remarkable that the two largest computer makers have committed to Java for their customers." (New York Times 12 Jun 2003)

Category 23.1 *Java*

2003-06-27 **microsoft sun java court windows programming**

NewsScan

COURT OVERTURNS ORDER THAT WINDOWS INCLUDE JAVA
A federal appeals court has overturned a lower-court injunction that would have required Microsoft to incorporate Sun's Java programming language in Microsoft's Windows operating system. On the other hand,, the court also upheld the lower court's ruling that Microsoft had broken a 2001 legal settlement between the two companies and had infringed on Sun's copyrights. The case has been sent back to the district court for further proceedings. (Reuters/USA Today 27 Jun 2003)

Category 23.1 *Java*

2004-02-23 **JAVA virtual machine support vulnerability MS Microsoft**

RISKS 23 20

MICROSOFT DUMPS JAVA VM

Consultant Ferdinand John Reinke wrote in RISKS: "Are you familiar with the MS Java Virtual Machine (MSJVM) issue? After September 30th 2004, Microsoft will no longer be able to support this technology. As a result, customers who have the MSJVM installed after this date will be vulnerable to potential attacks that will attempt to exploit this technology. This problem is compounded by the fact that Microsoft will no longer be able to provide software updates or patches to the MSJVM. This issue is not just a concern for organizations that use Java, but will also impact anyone who has the MSJVM installed. More alarming, many organizations aren't even aware that they have MSJVM installed."

Later, in RISKS 23.23, Jonathan de Boyne Pollard suggested that the change of support would have no immediate effects: "The software is not, after all, magically changing somehow on that date to become more vulnerable." He also denied that the security implications of awareness of what software one has on one's system is in any way related to whether the software is supported or not.

[MK comments: The issue is whether anyone is going to provide patches, and if so, how quickly. As for knowing what one has on one's system, it's very unlikely that a system manager will patch what (s)he doesn't know is being used on the system.]

Category 23.1 *Java*

2004-10-08 **Java Sun Eastman Kodak patent**

NewsScan; http://australianit.news.com.au/articles/0

SUN SETTLES JAVA SUIT FOR $92 MILLION

Eastman Kodak has accepted a $92-million offer by Sun Microsystems to settle a billion-dollar patent-infringement lawsuit over the Java programming language. A U.S. federal jury decided last Friday, after a three-week trial, that Java infringed on patents Kodak acquired when it bought Wang Laboratories' imaging software business for $260 million in 1997. The night before the trial's damages phase, which was to begin Thursday, the companies ended their two-year-old battle in an out-of-court settlement. Without admitting or denying the allegations, Sun Microsystems said it will pay Kodak $92 million to settle all claims in the dispute. In exchange, Sun received a license for Java under all Kodak patents. (The Australian, 8 Oct 2004)

Category 23.1 *Java*

2004-11-01 **Sun Java Web Proxy Server buffer overflow vulnerability denial of service DoS update issued**

DHS IAIP Daily; http://secunia.com/advisories/13036/

November 01, Secunia — Sun Java System Web Proxy Server unspecified buffer overflow vulnerabilities.

Some vulnerabilities have been reported in Sun Java System Web Proxy Server 3.6 Service Pack 4 and prior. These vulnerabilites can be exploited by malicious people to cause a DoS (Denial of Service) or compromise a vulnerable system. The vulnerabilities are caused due to some unspecified boundary errors that can be exploited to cause buffer overflows. Apply Service Pack 5 or later: http://wwws.sun.com/software/download/products/4149bc42.html

---

Category 23.1 *Java*

2004-12-20 **Google Desktop Search local search integration result disclosure remote Java applet exploit update issued**

DHS IAIP Daily; http://securitytracker.com/alerts/2004/Dec/1012624.html

December 20, SecurityTracker — Google Desktop Search discloses local search integration results to remote users.

A remote user can create a Java applet that, when loaded by the target user, will execute queries to the remote server that served the Java applet that appear to the Google Desktop Search application to be valid Google queries, causing the search application to integrate the local search results with the information returned by the remote server that served the Java applet. The applet running on the target user's system will then have access to the integrated local search results and can forward those results to the remote server. The vendor has released a fixed version (121004) as of December 10, 2004.

Category 23.1 *Java*

2005-01-20 **Sun Java plug-in two vulnerabilities security restrictions bypass malicious applet JDK JRE 5.0 not affected**

DHS IAIP Daily; http://secunia.com/advisories/13918/

TWO VULNERABILITIES IN SUN JAVA PLUG-IN

Two vulnerabilities have been discovered in Sun Java Plug-in, which can be exploited by malicious people to bypass certain security restrictions or compromise a user's system. The first vulnerability involves an error in the Java Plug-in within the handling of JavaScript calling into Java code can be exploited by a malicious applet hosted on a Website to access and modify local files or execute local applications. This vulnerability has been fixed in SDK / JRE 1.4.2_01 and later, and SDK / JRE 1.3.1_13 and later. The second vulnerability involves an error in the way applets on the same Web page can interfere with each other can be exploited to load files and Web pages in another applet. This vulnerability has been fixed in SDK / JRE 1.4.2_06 and later, and SDK / JRE 1.3.1_13 and later. For both vulnerabilities, JDK and JRE 5.0 are not affected.

Category 23.1 *Java*

2005-01-28 **HP Tru64 UNIX Java SDK/RTE denial of service DoS vulnerability JVM unresponsive**

DHS IAIP Daily; http://www.k−otik.com/english/advisories/2005/0075

HP TRU64 UNIX JAVA SDK/RTE DENIAL OF SERVICE VULNERABILITY.

A new vulnerability has been identified in HP Tru64 UNIX, which could be exploited by remote attackers to conduct denial of service attacks. The flaw resides in the Java Software Development Kit (SDK) and Run Time Environment (RTE). Object deserialization may allow a remote attacker to cause the Java Virtual Machine to become unresponsive, resulting in denial of service for the Runtime environment and servers that run on the Runtime Environment. Solution available: Java SDK and RTE v1.4.2-4 for HP Tru64 Unix: http://h18012.www1.hp.com/java/download

---

Category 23.1 *Java*

2005-02-14 **International Business Machines IBM Websphere server Java Server Pages source code disclosure sensitive information update issued**

DHS IAIP Daily; http://secunia.com/advisories/14274/

IBM WEBSPHERE APPLICATION SERVER JSP SOURCE CODE DISCLOSURE

A vulnerability has been reported in WebSphere Application Server, which can be exploited by malicious people to gain knowledge of potentially sensitive information. The vulnerability is caused due to an unspecified error allowing the source code of Java Server Pages (".jsp") to be disclosed via a specially crafted URL on the Windows platform. Original advisory and updates available at: http://www-1.ibm.com/support/docview.wss?uid=swg24008814 and http://www-1.ibm.com/support/docview.wss?uid=swg24008815

Category 23.1 *Java*

2005-03-21 **Java Web Start JNLP file command line argument injection vulnerability sandbox JVM disable Windows Solaris Linux update issued**

DHS IAIP Daily; http://secunia.com/advisories/14640/

JAVA WEB START JNLP FILE COMMAND LINE ARGUMENT INJECTION VULNERABILITY

A vulnerability in Java Web Start, which can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to an input validation error when handling property tags in JNLP files. This can be exploited to pass arbitrary command line arguments to the virtual machine by tricking a user into opening a malicious JNLP file. Successful exploitation can lead to the Java "sandbox" being disabled. The vulnerability has been fixed in J2SE releases 1.4.2_07 or later for Windows, Solaris and Linux.

Category 23.1 *Java*

2005-04-20 **Sun Java System Web proxy server buffer overflow vulnerabilities system compromise code execution attack update issued**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/0367

SUN JAVA SYSTEM WEB PROXY SERVER BUFFER OVERFLOW VULNERABILITIES

A new vulnerability was identified in Sun Java System Web Proxy Server, which could be exploited by remote attackers to execute arbitrary commands. This flaw is due to an unspecified buffer overflow error which may allow a remote attacker to compromise a vulnerable system and execute arbitrary code with the privileges of the server process. Note: The default UID for the Web Proxy Server is "nobody". Upgrade to Sun Java System Web Proxy Server 3.6 Service Pack 7 or later: http://www.sun.com/download/index.jsp

---

23.2 Javascript

Category 23.2 Javascript

2001-02-13 **e-mail address capture spyware Web privacy JavaScript**

RISKS 21 24

Stewart C. Russell reported to RISKS on unauthorized e-mail address capture while browsing:
>I was looking at an estate agent's (realtor's) website when I noticed the status line on my browser saying "Contacting <mailserver>" then "Message Sent". I looked through the site's HTML code and there was a little piece of JavaScript which appeared to send an e-mail message to the site's owner with no intervention from me. This service is provided by http://www.siteguest.com/, who describe it as "Caller ID for your web site".

Sure enough, in the next few days I started to get a number of e-mails from this realtor promising the best deals on houses. I'd prefer to choose who gets my e-mail address, and the behaviour of this particular individual has pretty much guaranteed no business from me.

The risk? The usual JavaScript and security warnings should be on, and that combining web and mail functions in one program is not always a good idea.<

Category 23.2 Javascript

2002-03-10 **JavaScript vulnerabilities ICAT CVE CGI**

ICAT Metabase

The ICAT Metabase < http://icat.nist.gov/icat.cfm > for the Common Vulnerabilities and Exposures (CVE) database reported the following vulnerabilities involving JavaScript for the period from 1 Jan 2001 to 10 Mar 2002:

CAN-2001-0365: Eudora before 5.1 allows a remote attacker to execute arbitrary code, when the 'Use Microsoft Viewer' and 'allow executables in HTML content' options are enabled, via an HTML email message containing Javascript, with ActiveX controls and malicious code within IMG tags. Published Before: 6/27/2001 Severity: High

CAN-2001-0596: Netscape Communicator prior to 4.77 allows a remote attacker to execute arbitrary javascript via specially crafted GIF images. The javascript is embedded in the GIF file as a comment. Published Before: 8/2/2001 Severity: High

CAN-2001-0722: Internet Explorer 5.5 and 6.0 allows remote attackers to read and modify user cookies via Javascript in an about: URL. Published Before: 12/6/2001 Severity: Medium

CAN-2001-0723: Internet Explorer 5.5 and 6.0 allows remote attackers to read and modify user cookies via Javascript, aka the "Second Cookie Handling Vulnerability." Published Before: 11/14/2001 Severity: Medium

CAN-2001-0743: Paging function in O'Reilly WebBoard Pager 4.10 allows remote attackers to cause a denial of service via a message with an escaped ' character followed by JavaScript commands. Published Before: 10/18/2001 Severity: Medium

CAN-2001-0745: Netscape 4.7x allows remote attackers to obtain sensitive information such as the user's login, mailbox location and installation path via Javascript that accesses the mailbox: URL in the document.referrer property. Published Before: 10/18/2001 Severity: Medium

CAN-2001-0824: Cross-site scripting vulnerability in IBM WebSphere 3.02 and 3.5 FP2 allows remote attackers to execute Javascript by inserting the Javascript into (1) a request for a .JSP file, or (2) a request to the webapp/examples/ directory, which inserts the Javascript into an error page. Published Before: 12/6/2001 Severity: High

CAN-2001-0828: A cross-site scripting vulnerability in Caucho Technology Resin before 1.2.4 allows a malicious webmaster to embed Javascript in a hyperlink that ends in a .jsp extension, which causes an error message that does not properly quote the Javascript. Published Before: 12/6/2001 Severity: High

CAN-2001-0829: A cross-site scripting vulnerability in Apache Tomcat 3.2.1 allows a malicious webmaster to embed Javascript in a request for a .JSP file, which causes the Javascript to be inserted into an error message. Published Before: 12/6/2001 Severity: High

CAN-2001-0898: Opera 6.0 and earlier allows remote attackers to access sensitive information such as cookies and links for other domains via Javascript. Published Before: 11/15/2001 Severity: Medium

CAN-2001-0919: Internet Explorer 5.50.4134.0100 on Windows ME with "Prompt to allow cookies to be stored on your machine" enabled does not warn a user when a cookie is set using Javascript, Published Before: 11/26/2001 Severity: High

CAN-2001-0987: Cross-site scripting vulnerability in CGIWrap before 3.7 allows remote attackers to execute arbitrary Javascript on other web clients by causing the Javascript to be inserted into error messages that are generated by CGIWrap. Published Before: 7/22/2001 Severity: High

CVE-2001-0148: The WMP ActiveX Control in Windows Media Player 7 allows remote attackers to execute commands in Internet Explorer via javascript URLs, a variant of the "Frame Domain Verification" vulnerability. Published Before: 6/2/2001 Severity: High

CVE-2001-0149: Windows Scripting Host in Internet Explorer 5.5 and earlier allows remote attackers to read arbitrary files via the GetObject Javascript function and the htmlfile ActiveX object. Published Before: 6/2/2001 Severity: High

Category 23.2 Javascript

2004-08-03 **Mozilla Netscape browser critical flaw vulnerability Javascript Webpages**

DHS IAIP Daily; http://www.internetnews.com/security/article.php/3389941

August 03, internetnews.com — PC takeover flaw in Mozilla, Netscape.

Security researchers have discovered a "highly critical" security hole in the Netscape and Mozilla browsers that puts users at risk of computer takeover. According to an advisory from iDefense, the vulnerability is caused by an integer overflow within the SOAPParameter object's constructor. SOAPParameter objects handle support for SOAP , the XML-based messaging protocol that defines rules for structuring messages. "Successful exploitation allows the remote attacker to execute arbitrary code in the context of the user running the browser," iDefense warned. The flaw can be exploited via specially created Web pages containing malicious Javascript. Browser products affected include Mozilla 1.6; and Netscape versions 7.0 and 7.1. The research firm recommends that Netscape users disable Javascript in the browser as a workaround. The open-source Mozilla Foundation has released an update to fix the flaw: http://www.mozilla.org/products/mozilla1.x/

Category 23.2 Javascript

2004-12-08 **multiple browser injection vulnerability JavaScript exploit no update issued**

DHS IAIP Daily; http://www.securitytracker.com/archives/summary/9000.html

December 08, SecurityTracker — Multiple browsers window injection vulnerability.

A remote user can inject arbitrary content into an open window in certain cases to spoof Website contents. It is reported that if the target name of an open window is known, a remote user can create Javascript that, when loaded by the target user, will display arbitrary content in the opened window. A remote user can exploit this to spoof the content of potentially trusted Websites. Specific browsers affected are Apple Safari, KDE Konqueror, Microsoft Internet Explorer, Mozilla Firefox, Netscape, and Opera. There is no solution at this time.

Category 23.2 Javascript

2005-09-16 **java exploit audio file automatic execution e-mail GMAIL spam script**

RISKS 24 04

GMAIL SECURITY FLAW: ACTS ON JAVASCRIPT IN UNOPENED E-MAIL

Suw Charman reported on a new vulnerability and exploit:

* * *

I received a spam this morning that opened audio files without me even opening the e-mail. The spam was from 'news@capitalex.com' and had the subject 'news'.

A closer looks reveals this code:

<Script Language='Javascript'>

<!--

document.write(unescape('%3C%49%46%52%41%4D%45%20%77%69%64%74%68%3D%22%31%22%20%68%65%69%67%68%74%3D%22%31%22%20%53%52%43%3D%22%68%74%74%70%3A%2F%2F%77%77%77%2E%70%72%6F%66%6F%72%65%78%74%72%61%64%65%2E%63%6F%6D%2F%69%6D%61%67%65%73%2F%6E%65%77%65%78%2E%68%74%6D%6C%22%20%66%72%61%6D%65%42%6F%72%64%65%72%3D%22%31%22%20%0D%0A%0D%0A%73%63%72%6F%6C%6C%69%6E%67%3D%22%6E%6F%22%3E%3C%2F%49%46%52%41%4D%45%3E'));

//-->

</Script>

This decodes to

<IFRAME width="1" height="1" SRC="
http://www.proforextrade.com/images/newex.html" frameBorder="1" scrolling="no"></IFRAME>

That page loads automatically, *without me having opened the e-mail*, then runs a shed load of rubbish including two audio files.

Category 23.2 *Javascript*

2005-10-20 **Hackers scammers javascript Websites Internet JS Wonka Unicode JavaScript Internet Explorer Firefox Websense**

DHS IAIP Daily; http://informationweek.com/story/showArticle.jhtml?articleID =172302840

HACKERS, SCAMMERS HID MALICIOUS JAVASCRIPT ON WEBSITES

Internet thieves are using a new, fast spreading technique called "JS/Wonka" to conceal their code. The JS/Wonka technique converts characters to and from their respective Unicode values. JavaScript completes those conversions automatically, so it doesn't require much expertise on the part of the code writer. Dan Hubbard, senior director of security and research at Websense, said, "For whatever reason, the number has just skyrocketed since the last of September…There are 10,000 unique sites using this exact same method. The strange thing is, they're completely different types of sites." Internet Explorer and Firefox, among other browsers, are vulnerable. According to Websense, three out of four of the sites found using JS/Wonka are hosted in the U.S. which is another indication that either a group of scammers is working together, or that a obfuscation toolkit has just been made available, and hasn't had time to spread overseas. Websense's JS/Wonka Alert: http://www.websensesecuritylabs.com/resource/pdf/wslabs_wonk a_analysis_oct05.pdf

23.3 ActiveX

Category 23.3 ActiveX

2000-05-24 **mobile code ActiveX vulnerability certificate**

CERT-CC Advisory http://www.cert.org/advisories/CA-2000-07.html 2000 07

CERT-CC reported, "The Microsoft Office 2000 UA ActiveX control is incorrectly marked as "safe for scripting". This vulnerability may allow an intruder to disable macro warnings in Office products and, subsequently, execute arbitrary code. This vulnerability may be exploited by viewing an HTML document via a web page, newsgroup posting, or e-mail message." The vulnerability applied to all systems with Internet Explorer and any Microsoft Office 2000 products. One interesting aspect of the case is that the vulnerability was first reported to CERT-CC by L0pht Research Labs and @Stake, supporting the view that the pseudonym-using staff of those organizations are genuinely committed to professionalism. More important, however, is that the vulnerability exposes the fundamental weakness of the entire security model for ActiveX: knowing where a control originates in no way guarantees the safety of that code.

Category 23.3 ActiveX

2000-12-22 **activeX security workshop paper publication report**

RISKS, CERT-CC http://www.cert.org/reports/activeX_report.pdf 21 17

Richard M. Smith wrote, "This past summer, CERT sponsored a two-day workshop on security issues with ActiveX controls. The final report was just released today and is available as a PDF file at the CERT Web site: < http://www.cert.org/reports/activeX_report.pdf >. There is a lot of good information in the report about how individuals and organizations can reduce security risks in Internet Explorer when using ActiveX controls. In addition, there is a section aimed at software developers on how to create safer controls.

A good bit of the technical information in the report has not been made public before."

Category 23.3 *ActiveX*

2002-03-10 **ActiveX vulnerabilities ICAT CVE**

ICAT Metabase

The ICAT Metabase < http://icat.nist.gov/icat.cfm > for the Common Vulnerabilities and Exposures (CVE) database reported the following vulnerabilities involving ActiveX for the period from 1 Jan 2001 to 10 Mar 2002:

CAN-2000-1105: The ixsso.query ActiveX Object is marked as safe for scripting, which allows malicious web site operators to embed a script that remotely determines the existence of files on visiting Windows 2000 systems that have Indexing Services enabled. Published Before: 1/9/2001 Severity: Medium

CAN-2001-0365: Eudora before 5.1 allows a remote attacker to execute arbitrary code, when the 'Use Microsoft Viewer' and 'allow executables in HTML content' options are enabled, via an HTML email message containing Javascript, with ActiveX controls and malicious code within IMG tags. Published Before: 6/27/2001 Severity: High

CAN-2001-0538: Microsoft Outlook View ActiveX Control in Microsoft Outlook 2002 and earlier allows remote attackers to execute arbitrary commands via a malicious HTML e-mail message or web page. Published Before: 8/14/2001 Severity: High

CAN-2002-0022: Buffer overflow in the implementation of an HTML directive in mshtml.dll in Internet Explorer 5.5 and 6.0 allows remote attackers to execute arbitrary code via a web page that specifies embedded ActiveX controls in a way that causes 2 Unicode strings to be concatenated. Published Before: 3/8/2002 Severity: High

CVE-2001-0090: The Print Templates feature in Internet Explorer 5.5 executes arbitrary custom print templates without prompting the user, which could allow an attacker to execute arbitrary ActiveX controls, aka the "Browser Print Template" vulnerability. Published Before: 2/16/2001 Severity: High

CVE-2001-0091: The ActiveX control for invoking a scriptlet in Internet Explorer 5.0 through 5.5 renders arbitrary file types instead of HTML, which allows an attacker to read arbitrary files, aka a variant of the "Scriptlet Rendering" vulnerability. Published Before: 2/16/2001 Severity: Medium

CVE-2001-0148: The WMP ActiveX Control in Windows Media Player 7 allows remote attackers to execute commands in Internet Explorer via javascript URLs, a variant of the "Frame Domain Verification" vulnerability. Published Before: 6/2/2001 Severity: High

CVE-2001-0149: Windows Scripting Host in Internet Explorer 5.5 and earlier allows remote attackers to read arbitrary files via the GetObject Javascript function and the htmlfile ActiveX object. Published Before: 6/2/2001 Severity: High

CVE-2001-0434: The LogDataListToFile ActiveX function used in (1) Knowledge Center and (2) Back web components of Compaq Presario computers allows remote attackers to modify arbitrary files and cause a denial of service. Published Before: 7/2/2001 Severity: High

Category 23.3 *ActiveX*

2005-11-10 **Web application active content disable security incompatibility non-standard operating system restrictions design**

RISKS 24 10

LAW SCHOOL FORCES APPLICANTS TO DISABLE SECURITY MEASURES

Tony Lima reports on an annoying case of bad Web design he discovered when a Macintosh-using young friend of his tried to apply to a law school. It took over an hour to disable security sufficiently to allow a required ActiveX control to run on a Windows machine:

>I finally got the control to install after doing the following:

- Disabling my anti-spyware software (ewido security suite). I then tried to install the control with no luck.

- Setting the privacy permission for lsac.org to "allow." Again no luck installing the control.

- Eliminating all security by making the security settings (Tools/Internet Options/Security/Custom Level) completely open. I enabled each and every ActiveX and other control including unsigned controls and controls marked as not safe. The control then installed successfully.

Now perhaps I didn't have to go quite that far but a deadline was approaching and I really didn't want to take the time to perform the trial and error that would apparently be required to determine exactly how much security to give up.<

Prof Lima adds humorously:

"It occurs to me that this is truly THE law school admission test. If you're dumb enough to let this control install you're probably good law school material. OTOH if you don't let the control through then you're too smart to be a lawyer. (That's about all the humor I can manage after 1.5 hours fighting with this stuff. I've disconnected from the net and am running my usual four scanning programs right now.)"

Category 23.3 *ActiveX*

2006-05-10 **VeriSign i-Nav ActiveX control remote buffer overflow vulnerability execute arbitrary code solution update**

DHS IAIP Daily; http://www.securityfocus.com/bid/17939/discuss 23

VERISIGN I-NAV ACTIVEX CONTROL REMOTE BUFFER OVERFLOW VULNERABILITY.

Verisign i-Nav ActiveX control is prone to a buffer overflow vulnerability. The software fails to perform sufficient bounds checking of user supplied input before copying it to an insufficiently sized memory buffer. Analysis: This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of the Verisign i-Nav ActiveX control. User interaction is required to exploit this vulnerability in that the target must visit a malicious Webpage. The specific flaw exists within the "VUpdater.Install" ActiveX control which is used to provide native support for Internationalized Domain Names in Microsoft Internet Explorer, Microsoft Outlook and Microsoft Outlook Express. Solution: Reportedly, the vendor has released updated versions of the affected software to address this issue. Users of affected packages should contact the vendor for further information. For more information: http://www.securityfocus.com/bid/17939/references

---

23.4 HTML, XML, browsers

Category 23.4 *HTML, XML, browsers*

1997-01-09 **web spoofing diddling**

EDUPAGE

Ed Felten's Java-security team at Princeton University published an analysis of many ways that attackers can hijack information being sent to legitimate Web sites by users; one example is to insert unauthorized hot links in a poorly-secured Web site. EDUPAGE reported, "The researchers suggest that Web surfers take the following precautions: disabling JavaScript in their Web browsing software; keeping an eye on the software's location line, to ensure they know where they are; and paying close attention to the addresses they visit. (Chronicle of Higher Education 10 Jan 97 A25) < http://www.cs.princeton.edu/sip/pub/spoofing.html >"

Category 23.4 *HTML, XML, browsers*

1998-11-11 **virus HTML hypertext markup language**

Wired http://www.wired.com/news/print_version/technology/story/16206.html

There was a brief burst of alarm in November 1998 when the "Virus Information Center" posted a demonstration of how HTML could be used to write a virus. Skeptics noted that the "html.internal" virus would not, in fact, infect HTML documents unless the infected site had access to MS-Visual Basic. For VB users, however, such a virus could replicate extensively in any HTML documents on disk. For the time being, however, the virus class posed a theoretical, not a practical, threat.

Category 23.4 *HTML, XML, browsers*

2000-02-03 **alert CERT-CC FBI DOD Web cross-site scripting vulnerability**

NewsScanhttp://www.msnbc.com/news/365542.asp

Carnegie Mellon U.'s CERT Coordination Center, together with the FBI and the Defense Department, has issued a warning citing a security flaw in most complex Web sites that could allow hackers to launch malicious programs on a person's computer or capture information disclosed by a Web site user, such as credit card numbers. The flaw involves "cross-site scripting," which enables dangerous computer code to be embedded in innocuous-looking links to popular Web sites. The vulnerability is not limited to any particular kind of software, and occurs when complex Web sites fail to verify that hidden software code sent from a consumer's browser is safe. "Any information that I type into a form, what pages I visit on that site, anything that happens in that session can be sent to a third party, and it can be done transparently," says top Microsoft security manager Scott Culp. CERT says only a massive effort by Web site designers can remedy the problem, but in the interim, users should avoid clicking on Web links from untrusted sources, such as unsolicited e-mail messages or discussion forum messages. (AP/MSNBC 2 Feb 2000)

Peter Neumann, moderator of the RISKS Forum, added that the alert would be available at < http://www.cert.org/advisories/CA-2000-02.html > and that readers might also want to read the FAQ at < http://www.cert.org/tech_tips/malicious_code_FAQ.html >.

Category 23.4 *HTML, XML, browsers*

2000-03-29 **privacy covert channel monitoring identifier continuity Web browser behavior HTTP programming spyware**

RISKS 20 86

Martin Pool explained a newly-discovered exploit for surreptitiously monitoring the behavior of Web-site visitors. Much like cookies, the headers of cached objects are returned to a Web server when the browser checks to see if there have been any changes to specific objects (if there are, the browser downloads a new copy; if not, the browser uses the cached copy of the object). If an unscrupulous Web-site programmer stores unique information in the Last-Modified field of stored objects, the behavior of tagged users (or at least, of users of a specific browser on a particular computer) can be monitored. Because the Last-Modified field is returned only if the browser client requests exactly the same URL (and all associated parameters), the snooping HTML programmer has to provide an object that will not change and that is common to all pages on the site; an example would be a (near-invisible) single pixel. Using the full extent of the Last-Modified field, snoopers would be able to generate approximately 1B unique identifiers per object — and each new object would offer the opportunity for another billion identifiers.

Category 23.4 *HTML, XML, browsers*

2000-07-31 **QA quality assurance Web site source testing tool editor concealment distortion trickery compensation bad design standards interoperability**

RISKS 20

Lloyd Wood reported on a dangerous feature of Internet Explorer 5.5: it alters the appearance of HTML source code by suppressing the visibility of embedded backslashes. He discovered this extraordinary deception when he tried to figure out why the non-standard (invalid) HTML code one of his colleagues generated using MS-Word was failing with other browsers but working in IE. As he wrote in RISKS, "If you view source, you expect to see the actual source, and not a prefiltered version. This filtering is clearly a risk in that it allows behaviour that would previously have been clearly exposed as bugs in the composing products to stay, unnoticed and uncorrected, because it means you can't trust the tool you're using, and because it screws up interoperability testing. (Which, because IE comes from Microsoft, is hardly a surprise.)"

Category 23.4 *HTML, XML, browsers*

2000-09-20 **denial of service filtering censorship HTML-enabled e-mail attack vulnerability**

RISKS 21 05

Dan Birchall noted in RISKS that HTML-enabled e-mail could be used to cause trouble for anyone behind a proxy server equipped with anti-porn (or other) censorware. By embedding invisible pixels addressing banned sites in such e-mail, an attacker could generate an arbitrary number of entries in the censorware log files, thus initiating investigations of specific victims. The poor souls under investigation would have no idea that the e-mail they had received was surreptitiously harming their reputations.

Category 23.4 *HTML, XML, browsers*

2000-11-22 **e-mail monitoring spyware covert channel privacy hostile code HTML Web bugs**

NewsScan, New York Times
http://partners.nytimes.com/2000/11/22/technology/22NET.html

Privacy advocates are concerned about the fact that the new e-mail software system called HTML mail makes it possible for people sending you messages to monitor when and what time of day you open them, how often you reopen them, and whether you forward them to other people. The marketing companies that use HTML mail say it helps them develop more personalized promotions; individuals who use it claim they have a right to monitor their own correspondence. Richard M. Smith, the chief technology officer for the Privacy Foundations, argues: "You can buy 50,000 addresses of people who subscribe to The New Yorker. But you don't know what articles they're reading in it, or what books they've bought or what medical problems they've been researching lately. That's very much a possibility within this technology." (New York Times 22 Nov 2000)

Category 23.4 *HTML, XML, browsers*

2001-01-23 **cross-site scripting vulnerability Web**

RISKS 21 22

Michael Sims reported cross-site scripting vulnerabilities on the News.com (CNET) Web site. Users were able to insert arbitrary headlines on the Web site; e.g., Sims wrote, "http://news.cnet.com/news/topic/0-1003-249-0.html?title=CNET%20Editors%20Agree:%20Slashdot%20is%20a%20better%20news%20site%20than%20News.com&topic=slashdot"

Sims wrote, "CNET was notified six hours before this e-mail was sent to RISKS; they have not replied at this time or taken any corrective action."

Category 23.4 *HTML, XML, browsers*

2001-10-02 **html malicious code programming Web site hijacking misspellings cybersquatting fraud court case injunction diversion advertising pornography**

NewsScan

COURT SHUTS DOWN THOUSANDS OF WEB SITES
A U.S. court shut down more than 5,500 Web sites operated by John Zuccarini of Andalusia, Penn., after it determined that the sites illegally diverted Web surfers from their intended destinations and forced them to download pop-up ads for pornography and gambling. Zuccarini had registered many misspellings of popular sites, including 41 variations on "Britney Spears," in a strategy to corral sloppy typists and bombard them with the unwanted ads. Visitors to Zuccarini's sites often could not leave without shutting down their systems, because the "back" button on their Web browsers was rigged to trigger more ads. (Reuters/Los Angeles Times 2 Oct 2001)
http://www.latimes.com/technology/la-000078749oct02.story?coll=la%2Dheadline s%2Dtechnology

---

Category 23.4 *HTML, XML, browsers*

2001-12-11 **html malicious code programming Web site hijacking flaw vulnerability browser patch**

NewsScan

MICROSOFT FIXING SECURITY FLAW IN INTERNET EXPLORER [11 Dec 2001]
Finnish security researcher Jouko Pynnonen of Oy Online Solutions says that Microsoft is working on a software patch to fix a security vulnerability in Internet Explorer versions 5, 5.5, and 6, which would make it possible for a malicious intruder to exploit ordinary Web page code to bypass the browser's system for securely handling downloaded files. A Microsoft spokesperson declined to discuss the status of the browser patch at this time. (Newsbytes 11 Dec 2001)
http://www.newsbytes.com/news/01/172878.html

Category 23.4 *HTML, XML, browsers*

2002-01-10 **SSL https padlock icon misleading interpretation programming**

RISKS 21 86ff

A discussion in RISKS led to some interesting analysis of the disconnect between the state of the padlock icon on Web browsers and the use of SSL. The problem began with a visit to the Kaiser Permanent Web site for members at < http://www.kponline.org/ >. All attempts to initiate https connections appeared to fail. However, in a followup, Geoff Kuenning summarized the situation neatly as follows:

>. . . [I]n viewing the source of the referenced Web page, it appears that the "sign on" button makes an https (SSL) connection. Thus, although the "padlock" icon in the browser is unlocked, anything sent from that page is in fact sent using SSL.

I have recommended that Kaiser change their main page so that it forwards the browser to an SSL equivalent, solely so that the padlock icon will appear locked.

I think that the true RISK is not in Kaiser's Web page, but rather in the browser. The "padlock" icon reflects not whether the page SENDS information securely, but rather the fact that the page was FETCHED securely. This disconnect between what is shown and what is expected has been raised recently by Jeff Mogul in the converse direction: a page that had the padlock proceeded to send information insecurely.

The first problem (apparently insecure page is actually secure) can be patched around with the forwarding kludge I mentioned above. The second can be handled by the user to some extent (certain browser settings can warn you when you transition from a secure page to an insecure one). However, the true problem is in browser design. The "padlock" icon should be associated with a LINK, not a page. Regardless of how it was fetched, if a page contains both secure and insecure links, the lock should be shown as unlocked and should lock only when you mouse over a secure link. Only if all outgoing links from a page are secure should the padlock be permanently displayed in its locked form.
<

MORAL: It is not enough to be secure; you must be SEEN to be secure.

Category 23.4 *HTML, XML, browsers*

2002-01-28 **Web page hijacking URL user ID misleading trickery dissimulation spoofing browser**

RISKS 21 89

Rob Graham spotted a dangerous application of syntax in a URL that looked like this:

< http://www.microsoft.com&item=3Dq209354@hardware.no/nyheter/feb01/Q209354 %20%20HOWTO.htm >

The naïve users would assume that the URL is part of the microsoft.com domain; in fact, this syntax means that a user ID and password (the part in front of the @ sign) is being passed to the URL _following_ the @ sign.

[MK notes: In testing this in March 2002 using MS IE6, I was taken directly to the "hardware.no" site, where a message read "This page has been removed after request from Microsoft. . . ." In contrast, using my preferred browser, Opera 6.01, I received a pop-up warning from the browser alerting me to the fact that the string "www.microsoft.com&item=3Dq209354" was in fact a user ID and password and asking if it was OK to proceed. Bravo Opera!]

Category 23.4 HTML, XML, browsers

2002-03-10 **HTML vulnerabilities ICAT CVE CGI**

ICAT Metabase

The ICAT Metabase < http://icat.nist.gov/icat.cfm > for the Common Vulnerabilities and Exposures (CVE) database reported the following vulnerabilities involving ActiveX for the period from 1 Jan 2001 to 10 Mar 2002:

CAN-2000-0898: Small HTTP Server 2.01 does not properly process Server Side Includes (SSI) tags that contain null values, which allows local users, and possibly remote attackers, to cause the server to crash by inserting the SSI into an HTML file. Published Before: 1/9/2001 Severity: Medium

CAN-2000-1172: Buffer overflow in Gaim 0.10.3 and earlier using the OSCAR protocol allows remote attackers to conduct a denial of service and possibly execute arbitrary commands via a long HTML tag. Published Before: 1/9/2001 Severity: High

CAN-2001-0322: MSHTML.DLL HTML parser in Internet Explorer 4.0, and other versions, allows remote attackers to cause a denial of service (application crash) via a script that creates and deletes an object that is associated with the browser window object. Published Before: 6/2/2001 Severity: Medium

CAN-2001-0365: Eudora before 5.1 allows a remote attacker to execute arbitrary code, when the 'Use Microsoft Viewer' and 'allow executables in HTML content' options are enabled, via an HTML email message containing Javascript, with ActiveX controls and malicious code within IMG tags. Published Before: 6/27/2001 Severity: High

CAN-2001-0389: IBM Websphere/NetCommerce3 3.1.2 allows remote attackers to determine the real path of the server by directly calling the macro.d2w macro with a NOEXISTINGHTMLBLOCK argument. Published Before: 7/2/2001 Severity: Medium

CAN-2001-0484: Tektronix PhaserLink 850 does not require authentication for access to configuration pages such as _ncl_subjects.shtml and _ncl_items.shtml, which allows remote attackers to modify configuration information and cause a denial of service by accessing the pages. Published Before: 6/27/2001 Severity: Medium

CAN-2001-0519: Aladdin eSafe Gateway versions 2.x allows a remote attacker to circumvent HTML SCRIPT filtering via a special arrangement of HTML tags which includes SCRIPT tags embedded within other SCRIPT tags. Published Before: 8/14/2001 Severity: Medium

CAN-2001-0520: Aladdin eSafe Gateway versions 3.0 and earlier allows a remote attacker to circumvent filtering of SCRIPT tags by embedding the scripts within certain HTML tags including (1) onload in the BODY tag, (2) href in the A tag, (3) the BUTTON tag, (4) the INPUT tag, or (5) any other tag in which scripts can be defined. Published Before: 8/14/2001 Severity: Medium

CAN-2001-0521: Aladdin eSafe Gateway versions 3.0 and earlier allows a remote attacker to circumvent HTML SCRIPT filtering via the UNICODE encoding of SCRIPT tags within the HTML document. Published Before: 8/14/2001 Severity: Medium

CAN-2001-0523: eEye SecureIIS versions 1.0.3 and earlier allows a remote attacker to bypass filtering of requests made to SecureIIS via the escaping of HTML characters within the request, which could allow a remote attacker to use restricted variables and perform directory traversal attacks on vulnerable programs that would otherwise be protected by SecureIIS. Published Before: 8/14/2001 Severity: Medium

CAN-2001-0538: Microsoft Outlook View ActiveX Control in Microsoft Outlook 2002 and earlier allows remote attackers to execute arbitrary commands via a malicious HTML e-mail message or web page. Published Before: 8/14/2001 Severity: High

CAN-2001-0726: Outlook Web Access (OWA) in Microsoft Exchange 5.5 Server, when used with Internet Explorer, does not properly detect certain inline script, which can allow remote attackers to perform arbitrary actions on a user's Exchange mailbox via an HTML e-mail message. Published Before: 12/6/2001 Severity: High

CAN-2001-0835: Cross-site scripting vulnerability in Webalizer 2.01-06, and possibly other versions, allows remote attackers to inject arbitrary HTML tags by specifying them in (1) search keywords embedded in HTTP referrer information, or (2) host names that are retrieved via a reverse DNS lookup. Published Before: 12/6/2001 Severity: High

CAN-2001-0837: DeltaThree Pc-To-Phone 3.0.3 places sensitive data in world-readable locations in the installation directory, which allows local users to read the information in (1) temp.html, (2) the log folder, and (3) the PhoneBook folder. Published Before: 12/6/2001 Severity: Medium

CAN-2001-0874: Internet Explorer 5.5 and 6.0 allow remote attackers to read certain files via HTML that passes information from a frame in the client's domain to a frame in the web site's domain, a variant of the "Frame Domain Verification"

vulnerability. Published Before: 12/13/2001 Severity: Medium

CAN-2001-0901: Hypermail allows remote attackers to execute arbitrary commands on a server supporting SSI via an attachment with a .shtml extension, which is archived on the server and can then be executed by requesting the URL for the attachment. Published Before: 11/19/2001 Severity: High

CAN-2001-0925: The default installation of Apache before 1.3.19 allows remote attackers to list directories instead of the multiview index.html file via an HTTP request for a path that contains many / (slash) characters, which causes the path to be mishandled by (1) mod_negotiation, (2) mod_dir, or (3) mod_autoindex. Published Before: 3/12/2001 Severity: Medium

CAN-2001-0948: Cross-site scripting (CSS) vulnerability in ValiCert Enterprise Validation Authority (EVA) 3.3 through 4.2.1 allows remote attackers to execute arbitrary code or display false information by including HTML or script in the certificate's description, which is executed when the certificate is viewed. Published Before: 12/4/2001 Severity: High

CAN-2001-1013: Apache on Red Hat Linux with with the UserDir directive enabled generates different error codes when a username exists and there is no public_html directory and when the username does not exist, which could allow remote attackers to determine valid usernames on the server. Published Before: 9/12/2001 Severity: Medium

CAN-2001-1019: Directory traversal vulnerability in view_item CGI program in sglMerchant 1.0 allows remote attackers to read arbitrary files via a .. (dot dot) in the HTML_FILE parameter. Published Before: 9/8/2001 Severity: Medium

CAN-2002-0022: Buffer overflow in the implementation of an HTML directive in mshtml.dll in Internet Explorer 5.5 and 6.0 allows remote attackers to execute arbitrary code via a web page that specifies embedded ActiveX controls in a way that causes 2 Unicode strings to be concatenated. Published Before: 3/8/2002 Severity: High

CAN-2002-0024: File Download box in Internet Explorer 5.01, 5.5 and 6.0 allows an attacker to use the Content-Disposition and Content-Type HTML header fields to modify how the name of the file is displayed, which could trick a user into believing that a file is safe to download. Published Before: 3/8/2002 Severity: High

CAN-2002-0025: Internet Explorer 5.01, 5.5 and 6.0 does not properly handle the Content- Type HTML header field, which allows remote attackers to modify which application is used to process a document. Published Before: 3/8/2002 Severity: Medium

CVE-2000-0897: Small HTTP Server 2.01 allows remote attackers to cause a denial of service by repeatedly requesting a URL that references a directory that does not contain an index.html file, which consumes memory that is not released after the request is completed. Published Before: 1/9/2001 Severity: Medium

CVE-2000-1187: Buffer overflow in the HTML parser for Netscape 4.75 and earlier allows remote attackers to execute arbitrary commands via a long password value in a form field. Published Before: 1/9/2001 Severity: High

CVE-2001-0002: Internet Explorer 5.5 and earlier allows remote attackers to obtain the physical location of cached content and open the content in the Local Computer Zone, then use compiled HTML help (.chm) files to execute arbitrary programs. Published Before: 7/21/2001 Severity: High

CVE-2001-0028: Buffer overflow in the HTML parsing code in oops WWW proxy server 1.5.2 and earlier allows remote attackers to execute arbitrary commands via a large number of " (quotation) characters. Published Before: 2/12/2001 Severity: High

CVE-2001-0089: Internet Explorer 5.0 through 5.5 allows remote attackers to read arbitrary files from the client via the INPUT TYPE element in an HTML form, aka the "File Upload via Form" vulnerability. Published Before: 2/16/2001 Severity: Medium

CVE-2001-0091: The ActiveX control for invoking a scriptlet in Internet Explorer 5.0 through 5.5 renders arbitrary file types instead of HTML, which allows an attacker to read arbitrary files, aka a variant of the "Scriptlet Rendering" vulnerability. Published Before: 2/16/2001 Severity: Medium

CVE-2001-0130: Buffer overflow in HTML parser of the Lotus R5 Domino Server before 5.06, and Domino Client before 5.05, allows remote attackers to cause a denial of service and possibly execute arbitrary commands via a malformed font size specifier. Published Before: 3/12/2001 Severity: High

CVE-2001-0149: Windows Scripting Host in Internet Explorer 5.5 and earlier allows remote attackers to read arbitrary files via the GetObject Javascript function and the htmlfile ActiveX object. Published Before: 6/2/2001 Severity: High

CVE-2001-0154: HTML e-mail feature in Internet Explorer 5.5 and earlier allows attackers to execute attachments by setting an unusual MIME type for the attachment, which Internet Explorer does not process correctly. Published Before: 5/3/2001 Severity: Medium

CVE-2001-0243: Windows Media Player 7 and earlier stores Internet shortcuts in a user's Temporary Files folder with a fixed filename instead of in the Internet Explorer cache, which causes the HTML in those shortcuts to run in the Local Computer Zone instead of the Internet Zone, which allows remote attackers to read certain files. Published Before: 6/27/2001 Severity: Medium

CVE-2001-0340: An interaction between the Outlook Web Access (OWA) service in Microsoft Exchange 2000 Server and Internet Explorer allows attackers to execute malicious script code against a user's mailbox via a message attachment that contains HTML code, which is executed automatically. Published Before: 7/21/2001 Severity: High

CVE-2001-0457: man2html before 1.5-22 allows remote attackers to cause a denial of service (memory exhaustion). Published Before: 6/27/2001 Severity: Medium

---

Category 23.4 *HTML, XML, browsers*

2002-04-22 **HTLM vulnerability arbitrary code denial-of-service attack DoS kernel panic crash Macintosh**

RISKS, http://news.com.com/2100-1001-884364.html 22 04

Robert Lemos wrote in CNET News:

Microsoft acknowledged on Tuesday that its popular Office applications for the Macintosh have a critical security flaw that leaves users' systems open to attack by worms and online vandals. The software slip-up happens because the Microsoft applications incorrectly handle the input to a certain HTML (Hypertext Markup Language) feature. By formatting a link in a particular manner, an attacker can cause a program to crash a Macintosh or run arbitrary commands. The link could appear on a Web page or in an HTML-enabled e-mail. [...]
http://news.com.com/2100-1001-884364.html

Category 23.4 *HTML, XML, browsers*

2002-06-10 **Excel spreadsheet vulnerability arbitrary code XML**

RISKS 22 12

Patrick O'Beirne contributed this item to RISKS:
>A security hole in Excel XP spreadsheets which could lead to a hack attack has been exposed. The discovery was made by independent security expert Georgi Guninski, who said on his Web site: "Excel XP tries to play with new technologies like XML and XSLT. Unfortunately the Excel seem so flawed that if the user opens a .xls file and chooses to view it with xml stylesheet arbitrary code may be executed. As script kiddies know this may lead to taking full control over a user's computer." Guninski, who has posted a sample of the code in his site, said users should not use XML stylesheets.<

Category 23.4 *HTML, XML, browsers*

2002-07-16 **content filter substitution replacement Web site corruption criminal hackers cross-site scripting HTML**

NewsScan

THE NEW LANGUAGE OF THE WEB
An e-mail security filter used by Yahoo has spawned a bizarre revision of the text in hundreds of Web sites by deleting letter combinations that could be used by hackers and replacing them with innocuous words. For example, "eval" has been converted to "review", so that the word "medieval" now appears as "medireview" on many sites. A recent search conducted by British Internet site NTK found that 640 different Web sites now contain the word "medireview" in place of "medieval." The offending words, which also include "mocha" (changed to "espresso") and "expression" (replaced by "statement"), are blacklisted because they could be used for cross-site scripting -- embedding potentially dangerous code into a Web page or an e-mail message written in HTML. (New Scientist 15 Jul 2002)
http://www.newscientist.com/news/news.jsp?id=ns99992546

Category 23.4 *HTML, XML, browsers*

2003-07-09 **MS03-023 Buffer Overrun HTML converter allow code execution vulnearbility microsoft security bulletin Internet Explorer Enhanced Security Configuration**

NIPC/DHS

July 09, Microsoft — Microsoft Security Bulletin MS03-023: Buffer Overrun In HTML Converter Could Allow Code Execution.

There is a flaw in the way the HTML converter for Microsoft Windows handles a conversion request during a cut-and-paste operation which results in a vulnerability. A specially crafted request to the HTML converter could cause the converter to fail in such a way that it could execute code. An attacker could craft a specially formed Web page or HTML e-mail that would cause the HTML converter to run arbitrary code on a user's system. If Internet Explorer Enhanced Security Configuration has been disabled, the protections put in place that prevent this vulnerability from being automatically exploited would be removed. Exploiting the vulnerability would allow the attacker only the same privileges as the user. Microsoft has assigned a risk rating of "Critical" to this issue and recommends that system administrators install the patch immediately.

Category 23.4 *HTML, XML, browsers*

2003-12-16 **denial-of-service SOAD document type definition DTD parameter vulnerability XML parser error**

NIPC/DHS

December 15, eSecurity Planet — DoS Flaw in SOAP DTD Parameter. IBM and Microsoft have released fixes for a potentially serious vulnerability that could be exploited to trigger denial-of-service attacks. The companies said the vulnerability was caused by an error in the XML parser when parsing the DTD (Document Type Definition) part of XML documents. Affected software include the IBM WebSphere 5.0.0 and Microsoft ASP.NET Web Services (.NET framework 1.0, .NET framework 1.1). According to IBM, the security patch fixes a flaw that could be exploited by sending a specially crafted SOAP request. "This can cause the WebSphere XML Parser to consume an excessive amount of CPU resources," the company warned. IBM's security patch is available here:
http://www-1.ibm.com/support/docview.wss?rs=180&context=SSEQ TP&q=PQ709%2021&uid=swg24005582. Microsoft confirmed the DTD error parsing vulnerability. In some cases, Microsoft recommended the rejection of XML messages that contain DTS, because of its limitations. The company said the SOAP 1.1 specification states that a SOAP message must not contain a DTD. Microsoft's security patch is available here:
http://support.microsoft.com/default.aspx?kbid=826231.

Category 23.4 *HTML, XML, browsers*

2004-02-18 **W3C Web DARPA standards adoption Defense Research Projects Agency**

DHS IAIP Daily; http://fcw.com/fcw/articles/2004/0216/web−daml−02−19−04.asp

February 18, Federal Computer Week — W3C adopts DARPA language.

The Defense Advanced Research Projects Agency (DARPA) this month announced that the World Wide Web Consortium (W3C) approved a computer language based on DARPA Agent Markup Language (DAML) as an international standard. Web Ontology Language, known as OWL, was designated an official Web standard, joining such better-known languages as HTML and Extensible Markup Language (XML). The DARPA markup language project last year evolved into OWL and is continuing development under W3C's watch. OWL builds on XML and is designed to allow a higher level of interoperability among devices, Web sites and databases. It uses XML as to transport data, but OWL is designed to link disparate data from different sources and determine relationships between them. OWL's proponents say it can refine searches and Web services, giving users more accurate and precise information based on queries. And the language could potentially let computers recognize how disparate forms of information are linked and draw conclusions based on those links.

Category 23.4 *HTML, XML, browsers*

2004-03-20 **XML Extensible Markup Language security concern**

NIPC/DHS

March 29, CNET News.com — Extra headaches of securing XML.

Extensible Markup Language and XML-based protocols are rapidly becoming a common way for businesses to format and exchange corporate information. Businesses typically have used Web services to connect internal applications and share information with a well-known network of business partners. However, once companies start using Web services and XML more extensively, they need to reconsider how they are exposing their data--and to what, Gartner analyst Benoit Lheureux said. Infiltrating a corporate network by tapping into Web services interfaces is potentially more damaging than simply knocking out a Website, because business-to-business applications expose valuable corporate information, he noted. Typical security products are designed to keep unwanted intruders from entering corporate networks or to prevent attacks that can disable a machine. Applications that send information via XML documents use the same Internet network protocols that traditional security products monitor. But because XML messages are wrapped in the IP "envelope" that most firewalls are designed to track, corporate networks inspect the envelope but not the contents. Fraudulent XML messages could therefore enter corporate networks undetected.

Category 23.4 *HTML, XML, browsers*

2004-07-30 **Microsoft security bulletin patch update privilege US-CERT**

DHS IAIP Daily; http://www.microsoft.com/technet/security/bulletin/ms04−
025. mspx

July 30, Microsoft — Microsoft Security Bulletin MS04-025: Cumulative Security Update for Internet Explorer.

This update resolves several newly discovered public vulnerabilities. If a user is logged on with administrative privileges, an attacker who successfully exploited the most severe of these vulnerabilities could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges. Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges. Microsoft has assigned a risk rating of "Critical" to this issue and recommends that users install the patch immediately. US-CERT released Technical Cyber Security Alert TA04-212A: Critical Vulnerabilities in Microsoft Windows for this issue: http://www.us-cert.gov/cas/techalerts/TA04-212A.html

---

Category 23.4 *HTML, XML, browsers*

2004-10-04 **XML RSS Really Simple Syndication broadcasting**

NewsScan; http://online.wsj.com/article/0

RSS GIVES XML A NEW LEASE ON LIFE

A year ago, blogs were widely regarded as the private diaries of tech-savvy eccentrics, and pundits were still waiting for the highly touted XML (extensible markup language) to make its mark on the Net, says Wall Street Journal columnist Lee Gomes. "Fast forward now to something called RSS, or Really Simple Syndication, which is a technology that bloggers use to, in a manner of speaking, broadcast their writing throughout the Internet. RSS, it turns out, is actually a kind of XML… In other words, thanks to blogs, XML -- in the form of RSS -- has finally arrived. This real XML revolution, though, is nothing like the stolid, corporate, rather dull affair that was first predicted. (If you liked database algorithms, you'd have loved XML.) Instead, it has a grassroots, quirky, somewhat antiauthoritarian cast to it." Gomes warns that while some major Internet giants, such as Yahoo and Microsoft, have signed on to support RSS feeds, blogs may ultimately change the traditional Web economics, because readers can skip frequent visits to their sites to check for new content. And while most RSS boosters describe the technology as an antidote for information overload, it could make things worse: "As e-mail proves, if it's easy for people to use computers to say something, they will. Do they have something to say? Who cares!" says Gomes.

Category 23.4 *HTML, XML, browsers*

2005-01-18 **Google links search engine blogs no follow tag priority cheat fraud fake false**

NewsScan;
http://news.com.com/Google+aims+to+outsmart+search+tricksters/2100-1024_3-5540740.html

GOOGLE MOVES TO OUTSMART SEARCH MANIPULATORS

Google is implementing a new tactic for blocking "link spammers" -- people who use the comment form on Web forums or blogs to place a link pointing back to their own Web site. The strategy is used to trick Google's PageRank technology into boosting a Web site's ranking in its results. The problem has become particularly rampant in the age of blogging, when publishers have little recourse to stop outsiders from littering their comment forms with bogus links. Google's answer, says search expert Danny Sullivan, is to give publishers a "no follow" tag that they can insert on a Web page to indicate that comments or links are not their own and signal Google as it indexes the Web that the pages are to be overlooked. "The tag provides you a way to flag links that are basically not yours," says Sullivan. "The reason why that's helpful is because they won't count those links. It makes the idea of spamming less attractive." Blog publisher Six Apart says it will adopt the tagging standard for its roughly 6.5 million blogs. "We're interested in deploying this tool so that all the search engines, whether it's Google, Yahoo or MSN, can properly distinguish content published by the author from content from commentors," says Six Apart VP Anil Dash. (CNet News.com 18 Jan 2005)

Category 23.4 *HTML, XML, browsers*

2005-02-01 **Mozilla Firefox Thunderbird multiple vulnerabilities information disclosure attack Internet Web browser e-mail client update issued**

DHS IAIP Daily; http://secunia.com/advisories/14017/

FIREFOX / MOZILLA / THUNDERBIRD MULTIPLE VULNERABILITIES

Details have been released about several vulnerabilities in Firefox, Mozilla and Thunderbird. These can be exploited by malicious people to bypass certain security restrictions, conduct spoofing and script insertion attacks and disclose sensitive and system information. Update to Mozilla 1.7.5, Firefox 1.0, and Thunderbird 1.0: http://www.mozilla.org/products/

Category 23.4 *HTML, XML, browsers*

2005-02-07 **Mozilla Firefox Camino Internet Web browser International Domain Names IDN spoofing security vulnerability no update issued**

DHS IAIP Daily; http://secunia.com/advisories/14163/

MOZILLA / FIREFOX / CAMINO WEB BROWSERS IDN SPOOFING SECURITY ISSUE

A security issue has been reported which can be exploited by a malicious Website to spoof the URL displayed in the address bar, SSL certificate, and status bar. The problem is caused due to an unintended result of the IDN (International Domain Name) implementation, which allows using international characters in domain names. This can be exploited by registering domain names with certain international characters that resemble other commonly used characters, thereby causing the user to believe they are on a trusted site. No solution is currently available.

Category 23.4 *HTML, XML, browsers*

2005-02-08 **Mozilla Firefox Internet Web browser multiple vulnerabilities command execution attack JavaScript hybrid image**

DHS IAIP Daily; http://securitytracker.com/alerts/2005/Feb/1013108.html

MOZILLA FIREFOX MULTIPLE VULNERABILITIES

There are several vulnerabilities in Mozilla Firefox. A remote user may be able to cause a target user to execute arbitrary operating system commands in certain situations or access access content from other windows, including the 'about:config' settings. This is due to a hybrid image vulnerability that allows batch statements to be dragged to the desktop and because tabbed javascript vulnerabilities let remote users access other windows. These vulnerabilities have been fixed in the CVS repository.

Category 23.4 HTML, XML, browsers

2005-02-08 **e-mail browser client vulnerabilities arbitrary code execution patch**

RISKS; http://www.ngssoftware.com/advisories/eudora-01.txt 23 72

HIGH RISK VULNERABILITIES IN EUDORA FOR WINDOWS

The Windows e-mail client Eudora v6.2.0 and earlier versions were reported by John Heasman of NGSSoftware to have serious vulnerabilities. Monty Solomon summarized them in RISKS:

The flaws permit execution of arbitrary code via:

1) previewing or opening a specially crafted e-mail 2) opening specially crafted stationary or mailbox files

These issues have been resolved in Eudora 6.2.1 as detailed at
http://www.eudora.com/security.html

It can be downloaded from:
http://www.eudora.com/products/

NGSSoftware are going to withhold details of this flaw for three months. Full details will be published on the 2nd of May 2005. This three month window will allow users of Eudora the time needed to apply the patch before the details are released to the general public. This reflects NGSSoftware's approach to responsible disclosure.

NGSSoftware Insight Security Research
http://www.databasesecurity.com/
http://www.nextgenss.com/ +44(0)208 401 0070

Category 23.4 HTML, XML, browsers

2005-02-12 **Firefox remote SMB document local file disclosure vulnerability HTML code share flash content no update issued**

DHS IAIP Daily; http://www.securityfocus.com/bid/12533/discussion/

FIREFOX REMOTE SMB DOCUMENT LOCAL FILE DISCLOSURE VULNERABILITY

A vulnerability has been published that may allow attackers to read the contents of attacker-specified files on the client users filesystem. To exploit this vulnerability, the attacker must place a HTML document containing code to read the target file on a remote SMB share. The attacker must then create flash content that will load the remote document via file:// URI. There is no solution at this time.

Category 23.4 HTML, XML, browsers

2005-02-23 **phpBB2 PHP bulletin board vulnerabilities file unlink information disclosure vulnerabilities directory traversal update issued**

DHS IAIP Daily; http://www.k−otik.com/english/advisories/2005/0194

PHPBB2 ARBITRARY FILE UNLINK AND DISCLOSURE VULNERABILITIES

Two vulnerabilities were identified in phpBB, and may be exploited by remote attackers to read or deleted arbitrary system files. The first flaw is due to an input validation error when handling specially crafted requests to upload avatars, which may be exploited by attackers to read arbitrary system files. The second vulnerability is due to a directory traversal error when handling the "avatarselect" return value, which may be exploited by attackers to unlink arbitrary system files. Updates to phpBB version 2.0.12: http://www.phpbb.com/downloads.php

---

Category 23.4 HTML, XML, browsers

2005-02-23 **PHP code injection vulnerability vBulletin code execution attack update issued**

DHS IAIP Daily; http://www.k−otik.com/english/advisories/2005/0192

VBULLETIN "MISC.PHP" REMOTE PHP CODE INJECTION VULNERABILITY

A new vulnerability was identified in vBulletin, and may be exploited by remote attackers to execute arbitrary PHP commands. The flaw resides in the "Add Template Name in HTML Comments" option when handling the "template" (misc.php) parameter, which may be exploited to execute arbitrary php commands with the web server privileges. Update to version 3.0.7: http://www.vbulletin.com

---

Category 23.4 *HTML, XML, browsers*

2005-02-24 **Mozilla Firefox flaws Web browser spoofing Windows Mac OS X Linux IDN Punycode address**

EDUPAGE; http://news.zdnet.com/2100-1009_22-5589693.html

MOZILLA FIXES FIREFOX FLAWS

The Firefox 1.0.1 update released by the Mozilla Foundation fixes several flaws in the Web browser, including one that permitted domain spoofing. The update is available for Windows, Mac OS X, and Linux. The updated browser displays the IDN Punycode (encoding of Unicode strings into the limited character set) in the address bar to prevent spoofing.

Category 23.4 *HTML, XML, browsers*

2005-02-28 **Mozilla Firefox Internet Web browser out of memory head corruption design flaw crash no update issued**

DHS IAIP Daily;
http://www.idefense.com/application/poi/display?id=200&type=
vulnerabilities&flashstatus=false

MOZILLA FIREFOX AND MOZILLA BROWSER OUT OF MEMORY HEAP CORRUPTION DESIGN ERROR

Remote exploitation of a design error in Mozilla 1.7.3 and Firefox 1.0 may allow a remote attacker to cause heap corruption, resulting in execution of arbitrary code. The vulnerability specifically exists in string handling functions, such as nsCSubstring::Append. Certain functions, such as nsTSubstring_CharT::Replace() fail to check the return value of functions which resize the string. A failed exploitation attempt may result in the browser crashing. There is no solution at this time.

Category 23.4 *HTML, XML, browsers*

2005-02-28 **phpWebSite PHP scripting vulnerability image upload no update issued**

DHS IAIP Daily; http://secunia.com/advisories/14399/

PHPWEBSITE ANNOUNCEMENT IMAGE UPLOAD VULNERABILITY

A vulnerability exists in phpWebSite 0.10.0 and prior, which potentially can be exploited by malicious people to compromise a vulnerable system. The vulnerability is caused due to an error in the uploading of images when submitting an announcement. This can be exploited to upload arbitrary PHP scripts to a directory inside the web root. There is no vendor solution at this time.

Category 23.4 *HTML, XML, browsers*

2005-04-26 **HP-UX operating system Mozilla browser vulnerabilities command execution attack system compromise update issued**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/0394

HP-UX MOZILLA MULTIPLE VULNERABILITIES

Multiple vulnerabilities were identified in HP-UX Mozilla, which may be exploited by malicious Websites to execute arbitrary commands. HP has acknowledged multiple vulnerabilities in Mozilla for HP-UX, which can be exploited by malicious people to cause a DoS (Denial of Service), gain knowledge of potentially sensitive information, bypass certain security restrictions, and compromise a user's system. Upgrade to Mozilla HP-UX version 1.7.3.02: http://www.hp.com/go/mozilla

---

Category 23.4 *HTML, XML, browsers*

2005-04-29 **Red Hat Linux Mozilla Internet Web browser vulnerabilities patch issued code execution**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/0428

REDHAT SECURITY UPDATE FIXES MULTIPLE MOZILLA VULNERABILITIES

Redhat has released a security patch to correct various vulnerabilities in Mozilla. The vulnerabilities can be exploited by malicious people to gain knowledge of potentially sensitive information. This could allow cross-site scripting attacks, bypass certain security restrictions, and compromise a user's system. The flaws could be exploited by malicious websites to execute arbitrary commands and cause a denial of service. Use Red Hat Network to download and update your packages: http://rhn.redhat.com/

Category 23.4 *HTML, XML, browsers*

2005-05-09 **Mozilla Firefox Internet Web browser JavaScript URL vulnerability**

DHS IAIP Daily; http://secunia.com/advisories/15292/

TWO VULNERABILITIES IN MOZILLA FIREFOX

Two vulnerabilities have been discovered in Firefox, which can be exploited by malicious people to conduct cross-site scripting attacks and compromise a user's system. "IFRAME" JavaScript URLs are not properly protected from being executed in context of another URL in the history list. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an arbitrary site. Input passed to the "IconURL" parameter in "InstallTrigger.install()" is not properly verified before being used. This can be exploited to execute arbitrary JavaScript code with escalated privileges via a specially crafted JavaScript URL. A temporary solution has been added to the sites "update.mozilla.org" and "addons.mozilla.org" where requests are redirected to "do-not-add.mozilla.org". This will stop the publicly available exploit code using the two vulnerabilities to execute arbitrary code in the default settings of Firefox.

Category 23.4 *HTML, XML, browsers*

2005-05-10 **Mozilla Firefox Internet Web browser authentication dialog vulnerability HTTP**

DHS IAIP Daily; http://www.securityfocus.com/bid/12728/solution/

MOZILLA SUITE/FIREFOX HTTP AUTHENTICATION DIALOGS TAB FOCUS VULNERABILITY

Mozilla Suite prior to 1.7.6 and Mozilla Firefox prior to 1.0.1 are reported prone to a vulnerability that may result in the loss of authentication credentials. It is reported that HTTP authentication dialogs do not remain focused for the tab that invoked the dialog, rather the dialog focuses over the active tab. A remote attacker may potentially exploit this condition to aid in phishing attacks. Netscape 7.2 is reportedly vulnerable to this issue as well. It is also 8 possible that other versions of Netscape are affected. The vendor has released upgrades for Firefox dealing with this issue. Mozilla has reported that a pending release of Mozilla Suite 1.7.6 will be released dealing with this issue in the near future.

Category 23.4 *HTML, XML, browsers*

2005-05-11 **operating system Macintosh Apple Tiger OS X vulnerability data loss mobile code malware widgets proof-of-concept exploits browser Safari**

http://www.vnunet.com/news/1162958

APPLE OS X & SAFARI EXPLOITS APPEAR QUICKLY

Apple's OS X v10.4 and Safari browser v2.0 turned out to have vulnerabilities that were quickly exploited by proof-of-concept tools available on the Web. Safari automatically downloads mobile code (widgets) written in Java. Unfortunately, malicious widgets would be difficult to remove, requiring manual deletion of files.

Category 23.4 *HTML, XML, browsers*

2005-05-11 **Gecko browser HTTP authentication prompt vulnerability no update issued**

DHS IAIP Daily; http://www.securiteam.com/securitynews/5RP0C0AFPA.html

GECKO BASED BROWSERS HTTP AUTHENTICATION PROMPT VULNERABILITY

The HTTP authentication prompt appears above the currently open tab regardless of which tab triggered it. A spoofer who could get a user to open a high value target in another tab might be able to capture the user's ID and password. There is no solution at this time.

Category 23.4 *HTML, XML, browsers*

2005-05-12 **Mozilla Suite Firefox Internet Web browser vulnerability code execution attack**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/0530

MOZILLA SUITE AND FIREFOX MULTIPLE CODE EXECUTION VULNERABILITIES

Mozilla has released new versions of Mozilla Suite and Firefox, to correct vulnerabilities that could be exploited by attackers to compromise a vulnerable system or perform Cross Site Scripting. The first flaw is due to an input validation error when handling a "javascript:" url in the "view-source:" or "jar:" pseudo-protocols, which may be exploited via a malicious Website to perform Cross Site Scripting and execute arbitrary code. This issue is a variant of the "favicon" vulnerability. The second vulnerability occurs when executing Javascript eval and Script objects without dropping the privileges of the context calling them, which may be exploited by remote attackers to compromise a vulnerable system. This flaw is a variant of the "DOM" issue. Upgrade to Firefox 1.0.4 or Mozilla Suite 1.7.8: http://www.mozilla.org/download.html

Category 23.4 *HTML, XML, browsers*

2005-05-16 **Mozilla Suite Firefox Internet Web browser script manager cross site scripting vulnerability**

DHS IAIP Daily; http://www.securityfocus.com/bid/13641/discussion/

MOZILLA SUITE AND FIREFOX MULTIPLE SCRIPT MANAGER SECURITY BYPASS VULNERABILITIES

Multiple issues exist in Mozilla Suite and Firefox. These issues allow attackers to bypass security checks in the script security manager. These vulnerabilities allow remote attackers to execute script code with elevated privileges, leading to the installation and execution of malicious applications on an affected computer. Cross-site scripting, and other attacks are also likely possible. Original advisory and updates: http://www.mozilla.org/projects/security/known-vulnerabilities.html

---

Category 23.4 *HTML, XML, browsers*

2005-05-17 **Microsoft HTML Help Workshop memory corruption vulnerability no update issued**

DHS IAIP Daily; http://www.securityfocus.com/bid/13668/discussion/

MICROSOFT HTML HELP WORKSHOP MEMORY CORRUPTION VULNERABILITY

The Microsoft HTML Help Workshop compiler tool, 'hhc.exe', is prone to a memory corruption vulnerability. Immediate consequences of exploitation of this issue result in an application crash; this would not be considered a vulnerability. However, it may be possible to subtly manipulate the contents of the affected registers so that an exploitable code path is reached. There is no solution at this time.

Category 23.4 *HTML, XML, browsers*

2005-06-14 **survey study security hackers Web Internet browser attacks phishing personal information theft viruses worms**

EDUPAGE; http://news.com.com/2100-7349_3-5747050.html

SURVEY SHOWS MORE BAD GUYS TURNING TO BROWSER ATTACKS

According to a new survey by the Computing Technology Industry Association (CompTIA), the incidence of browser-based attacks rose sharply last year, while that of viruses and worms fell slightly. Browser-based attacks exploit the naivety of computer users, as in the case of phishing attacks, or technical vulnerabilities in browser or operating system software. Phishing scams work by fooling users into disclosing private information; other attacks attempt to download malicious code to the computers of visitors to a Web site to steal information or take control of the computer. According to CompTIA's survey of nearly 500 organizations, 56.6 percent have been targets of browser-based attacks, up from 36.8 percent one year ago. Viruses and worms continue to head the list of computer security threats, at 66 percent, which is just down from last year's number of 68.6 percent. CNET, 14 June 2005

Category 23.4 *HTML, XML, browsers*

2005-06-16 **vulnerability cross-site scripting security bypass Opera Web browser**

DHS IAIP Daily; http://www.securityfocus.com/bid/6962/solution

OPERA CROSS SITE SCRIPTING AND SECURITY BYPASS VULNERABILITIES

Multiple vulnerabilities were identified in Opera, which may be exploited by malicious Websites to conduct cross-site scripting attacks. The first flaw is due to insufficient validation of server side redirects when handling "XMLHttpRequest" objects, which could be exploited to access resources from outside the domain of which the object was opened. The second vulnerability is caused due to Opera not properly restricting the privileges of "javascript:" URLs when opened in e.g. new windows or frames which could be exploited to conduct cross site scripting attacks and to read local files. The third issue exists in the way the Opera browser generates a temporary page for displaying a redirection when "Automatic redirection" is disabled (not default setting), which could be exploited to conduct cross site scripting attacks. Update to Opera 8.01: http://www.opera.com

---

Category 23.4 *HTML, XML, browsers*

2005-06-23 **vulnerability multiple Cacti cross-site scripting SQL injection attacks compromise browser session update issued**

DHS IAIP Daily; http://secunia.com/advisories/15490/

CACTI MULTIPLE UNSPECIFIED VULNERABILITIES

Some vulnerabilities have been reported in Cacti, which can be exploited by malicious people to conduct cross site scripting and SQL injection attacks or compromise a vulnerable system. Unspecified input is not properly sanitized before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code. Unspecified input is not properly sanitized before being used to include files. This can be exploited to include arbitrary files from external or local resources or execute arbitrary HTML and script code in a user's browser session in context of a vulnerable site. Update to version 0.8.6e: http://www.cacti.net/download_cacti.php

---

Category 23.4 *HTML, XML, browsers*

2005-06-24 **Web Internet browser vulnerability flaw Secunia Dialog Origin Spoofing**

DHS IAIP Daily; http://www.vnunet.com/vnunet/news/2138716/spoofing−flaw−swee ps−browsers

SPOOFING FLAW HITS MAJOR BROWSERS

Security company Secunia has warned of a flaw in a number of browsers that could expose users to phishing attacks. The company claims that most major browsers, including Internet Explorer, Firefox and Safari, suffer from a so-called Dialog Origin Spoofing Vulnerability. Opera 8.01 is not affected by the flaw. A hacker could use a JavaScript dialog box to request a web visitor to enter confidential information. The flaw centers around the fact that users have no way of verifying the origin of the dialog box. Hackers could exploit the flaw by offering a link to a trusted Website that simultaneously provides a malicious pop up that asks for confidential information. Microsoft has acknowledged the threat, but said that it will not release a patch because it uses a "current standard web browser functionality." Instead the software vendor urged users to use common sense before entering confidential information through a Web browser. "If a particular window or dialog box does not have an address bar and does not have a lock icon that can be used to verify the site's certificate, the user is not provided with enough information on which to base a valid trust decision about the window or dialog box," said Microsoft.

Category 23.4 *HTML, XML, browsers*

2005-07-14 **Thread CFM Cross Scripting Vulnerability Message input browser cookie credentials patches**

DHS IAIP Daily; http://www.securityfocus.com/bid/14268/discuss

SIMPLE MESSAGE BOARD THREAD.CFM CROSS-SITE SCRIPTING VULNERABILITY

A cross-site scripting vulnerability affects Simple Message Board. This issue is due to a failure of the application to properly sanitize user-supplied input. An attacker may leverage this issue to have arbitrary script code executed in the browser of an unsuspecting user. This may facilitate the theft of cookie-based authentication credentials as well as other attacks. Currently Security Focus is not aware of any vendor-supplied patches for this issue.

Category 23.4 *HTML, XML, browsers*

2005-07-25 **Netscape Browser fixes vulnerabilities malicious Websites validation error java cloning objects scripts prototype**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1214

NETSCAPE BROWSER SECURITY UPDATE FIXES MULTIPLE VULNERABILITIES

Two vulnerabilities were identified in Netscape Browser, which could be exploited by malicious Websites to execute arbitrary commands. The first issue is due to an input validation error in the processing of java script URLs opened by media players, which could be exploited by attackers to execute arbitrary code. The second vulnerability is due to an improper cloning of base objects, which could allow web content scripts to walk up the prototype chain to get to a privileged object and execute arbitrary code. Netscape Browser version 8.0.2 and prior are affected. Users should upgrade to Netscape Browser version 8.0.3.1: http://browser.netscape.com/ns8/download/default.jsp

---

Category 23.4 *HTML, XML, browsers*

2005-07-29 **vulnerability hole Opera Web browser download dialog spoofing malicious file execution update issued**

DHS IAIP Daily; http://www.securityfocus.com/bid/14402/info

OPERA WEB BROWSER CONTENT-DISPOSITION HEADER DOWNLOAD DIALOG FILE EXTENSION SPOOFING VULNERABILITY

Opera Web Browser is prone to a vulnerability that can allow remote attackers to spoof file extensions through the download dialog. An attacker may exploit this issue by crafting a malformed HTTP 'Content-Disposition' header that spoofs file extensions to trick vulnerable users into opening and executing a malicious file. Opera Web Browser versions prior to 8.02 are affected by this issue. The vendor has released Opera Web Browser 8.02 to address this issue: http://www.opera.com/download/

Category 23.4 *HTML, XML, browsers*

2005-09-13 **vulnerability flaw hole Firefox Internet Web browser hacker exploit**

DHS IAIP Daily; http://www.snpx.com/cgi−bin/news55.cgi?target=109361173?−2622

HACKERS WORK TO EXPLOIT LATEST FIREFOX FLAW

There has been a exploit found working on a Firefox flaw and the latest Netscape Web browser. According to the article, at least two security researchers have posted messages to popular security mailing lists claiming they have found ways attackers could take advantage of the vulnerability. The security vulnerability in question is a buffer overflow flaw. An attacker could host a Web site containing malicious code to exploit the vulnerability.

Category 23.4 *HTML, XML, browsers*

2005-10-05 **TellMe scripting vulnerabilities sanitization input code browser affected cookie credentials**

DHS IAIP Daily; TellMe Multiple Cross−Site Scripting Vulnerabilities

TELLME MULTIPLE CROSS-SITE SCRIPTING VULNERABILITIES

There has been a multiple cross-site scripting vulnerability identified in TellMe. This is due to a lack of proper sanitization of user-supplied input. An attacker may leverage this to have arbitrary script code executed in the browser of an unsuspecting user in the context of the affected site. This attack may facilitate the theft of cookie-based authentication credentials.

Category 23.4 *HTML, XML, browsers*

2005-10-10 **Utopia News Pro SQL injection vulnerabilities Two input validation parameter code browser**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/2012

UTOPIA NEWS PRO SQL INJECTION AND CROSS-SITE SCRIPTING VULNERABILITIES

Two vulnerabilities were identified in Utopia News Pro, which could be exploited by malicious users to perform SQL injection or cross site scripting attacks. The first issue is due to an input validation in the "header.php" and "footer.php" scripts when processing a specially crafted "sitetitle" or "version" parameter, which may be exploited by attackers to cause arbitrary scripting code to be executed by the user's browser. The second vulnerability is due to an input validation error in "news.php" when processing a specially crafted "newsid" parameter, which may be exploited by remote users to conduct SQL injection attacks. Utopia News Pro version 1.1.4 and prior are affected. The FrSIRT is not aware of any official supplied patch for this issue.

Category 23.4 *HTML, XML, browsers*

2005-10-19 **Browser Firefox crom restriction bypass Mozilla arbitrary**

DHS IAIP Daily; http://www.securityfocus.com/bid/14920/info

BROWSER/FIREFOX CROME PAGE LOADING RESTRICTION BYPASS

Mozilla Browser/Firefox are prone to a potential arbitrary code execution weakness. This may be used by an attacker to load privileged 'chrome' pages from an unprivileged 'about:' page. This issue does not pose a threat unless it is combined with a same-origin violation issue. This issue also may allow a remote attacker to execute arbitrary code and gain unauthorized remote access to a computer. This would occur in the context of the user running the browser.

Category 23.4 *HTML, XML, browsers*

2005-10-19 **Netscapre browser vulnerabilities arbitrary spoofing servers HTTP smuggling IP address**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/2147

NETSCAPE BROWSER SECURITY UPDATE FIXES MULTIPLE VULNERABILITIES

Multiple vulnerabilities have been identified in Netscape. These could be exploited by malicious Websites to execute arbitrary commands or conduct spoofing attacks. The severity of this vulnerability depends on the value of servers which might be vulnerable to HTTP request smuggling and similar attacks, or which share an IP address (virtual hosting) with the attacker's page. For users connecting to the Web through a proxy this flaw could be used to bypass the same origin restriction on XMLHttpRequests by tricking the proxy into handling a single request as multiple pipe lined requests directed at arbitrary hosts.

Category 23.4 *HTML, XML, browsers*

2005-12-09 **Web Internet browser Firefox exploit proof-of-concept code published threat**

DHS IAIP Daily; http://www.vnunet.com/vnunet/news/2147377/firefox−expoit−made−public

FIRST FIREFOX 1.5 EXPLOIT MADE PUBLIC

Security experts at Packet Storm have published proof-of-concept code that exploits an unpatched flaw in the Firefox 1.5 browser, making the application vulnerable to a denial of service attack. The code marks the first publicly disclosed security vulnerability in Firefox 1.5 since the version became available in late November. The published code will add a large entry to the 'history.dat' file of the browser, causing the application to freeze or crash the next time it is launched. Users can fix the problem by manually erasing the file. Another option is to change the browser setting to disable the saving of history data by setting the days of saved history to zero or increasing the privacy control. While the proof-of-concept code is relatively harmless, the flaw could be exploited to install malware, according to John Bambenek, a researcher with the University of Illinois at Urbana-Champaign and a volunteer at the SANS Internet Storm Center. "Presumably, if the topic was more tightly crafted than in the proof-of-concept code, a more malicious attack could be crafted that would install malware on the machine with the extra step of being reinstalled after each restart of Firefox," Bambenek wrote.

Category 23.4 *HTML, XML, browsers*

2005-12-22 **Apple Mac OS X KHTMLParser denial of service vulnerability application crash Safari Web browser TextEdit processor**

DHS IAIP Daily; http://www.securityfocus.com/bid/16045/references

Apple Mac OS X KHTMLParser remote denial of service vulnerability.

Apple Mac OS X KHTMLParser is affected by a remote denial of service vulnerability. Successful exploitation may cause an application employing KHTMLParser to crash. KHTMLParser is used by Apple Safari Web browser and Apple TextEdit word processor.

Category 23.4 *HTML, XML, browsers*

2005-12-31 **denial of service DoS vulnerability browser Blackberry Handheld JAD update software**

DHS IAIP Daily; http://www.securityfocus.com/bid/16099/solution 23

BLACKBERRY HANDHELD JAD FILE BROWSER DENIAL OF SERVICE VULNERABILITY

Blackberry Handheld devices are prone to a denial of service attack. The embedded Web browser will stop responding due to a dialog box that has not been properly dismissed when handling a malformed JAD (Java Application Description) file. Security Focus reports that the vendor has addressed this issue in version 4.0.2 of the Blackberry Device Software. The vendor encourages affected users to contact their service providers to obtain updated software.

Category 23.4 *HTML, XML, browsers*

2006-01-26 **Microsoft Internet Explorer IE ActiveX arbitrary code execution quality assurance failure**

DHS IAIP Daily; http://www.hackerscenter.com/archive/view.asp?id=22251 23

MICROSOFT INTERNET EXPLORER DOES NOT HONOR ACTIVEX.

Internet Explorer (IE) fails to properly check the kill bit for ActiveX controls, which may allow a remote attacker to execute arbitrary code on a vulnerable system. By convincing a user to view a specially crafted HTML document an attacker could execute arbitrary code with the privileges of the user. Depending on the ActiveX control being used, an attacker may be able to take other actions. There are a number of significant vulnerabilities in technologies involving the IE domain/zone security model, local file system (Local Machine Zone) trust, the Dynamic HTML (DHTML) document object model in particular, proprietary DHTML features; the HTML Help system, MIME type determination, the graphical user interface (GUI), and ActiveX. These technologies are implemented in operating system libraries that are used by IE and many other programs to provide Web browser functionality. IE is integrated into Windows to such an extent that vulnerabilities in IE frequently provide an attacker significant access to the operating system.

Category 23.4 *HTML, XML, browsers*

2006-01-30 **Mozilla Firefox Internet browser cross domain scripting vulnerability attack execute arbitrary script code**

DHS IAIP Daily; http://www.securityfocus.com/bid/16427/references 23

MOZILLA FIREFOX XBL -MOZ-BINDING PROPERTY CROSS DOMAIN SCRIPTING VULNERABILITY.

The Mozilla and Mozilla Firefox browsers are vulnerable to a cross domain scripting attack by which a malicious Webpage could access trusted sites' properties and execute arbitrary script code in the context of an arbitrary domain. The issue affects the "-moz-binding" property supported by the Mozilla Extensible Binding Language. XBL is a markup language for describing bindings that can be attached to elements in other documents. Bindings can be attached to elements using either cascading stylesheets [CSS] or the document object model [DOM]. A malicious site could access the properties of a trusted site and facilitate various attacks including disclosure of sensitive information.

Category 23.4 *HTML, XML, browsers*

2006-01-31 **new Internet browser cross site cooking threat Michael Zalewski Mozilla**

DHS IAIP Daily; 23
http://www.techworld.com/security/news/index.cfm?NewsID=5276
&Page=1&pagePos=6&inkc=0

BROWSERS FACE TRIPLE THREAT.

Polish security researcher Michael Zalewski has highlighted three bugs in the handling of cookies that he says could be used to carry out attacks on commercial Websites. The bugs, for which Zalewski has coined the term "cross site cooking," are fundamental to the design and implementation of cookies. The first problem involves the way browsers handle the domain specified in a cookie. Browsers should theoretically reject cookies where the domain is specified too broadly, but the mechanism doesn't work in Mozilla-based browsers, though Internet Explorer doesn't seem to be affected, Zalewski said. A variant on this bug is that browsers don't check to see if anything is between the periods in a domain name specified by a cookie. The third problem Zalewski outlined is a trick that he said could be easily used to force random visitors to a site to accept and relay malicious cookies to third-party sites. "Using this trick, a brand new identity may be temporarily bestowed upon the user, and used to perform certain undesirable or malicious tasks on the target site," he said.

Category 23.4 *HTML, XML, browsers*

2006-02-01 **Symantec Sygate Management server SMS authentication servlet SQL injection vulnerability quality assurance solution update**

DHS IAIP Daily; http://www.securityfocus.com/bid/16452/references 23

SYMANTEC SYGATE MANAGEMENT SERVER SMS AUTHENTICATION SERVLET SQL INJECTION VULNERABILITY.

Symantec Sygate Management Server is prone to an SQL injection vulnerability. The vulnerability specifically affects the SMS Authentication Servlet component of the server. A remote attacker can pass malicious input to database queries through HTTP GET requests, resulting in modification of query logic or other attacks. This allows attackers to overwrite the password of any account on the server. This can facilitate a complete compromise if the attacker can overwrite the administrator password. Solution: Symantec has released SYM06-002 to address this issue.

Category 23.4 *HTML, XML, browsers*

2006-02-02 **Netscape property validation vulnerability flaw cross-domain scripting attack**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2006/Feb/1015563.html 23

NETSCAPE '-MOZ-BINDING' PROPERTY VALIDATION FLAW LETS REMOTE USERS CONDUCT CROSS-DOMAIN SCRIPTING ATTACKS.

A vulnerability was reported in Netscape. A remote user can conduct cross-domain scripting attacks. The Netscape browser '-moz-binding' CSS property does not properly restrict HTML code from other domains before displaying the input. A remote user can create specially crafted HTML that, when loaded by a target user, will cause arbitrary scripting code to be executed by the target user's browser. The code can originate from an arbitrary domain but will run in the security context of the domain serving the HTML. As a result, the code will be able to access the target user's cookies (including authentication cookies), if any, associated with the domain, access data recently submitted by the target user via Web form to the domain, or take actions on the domain acting as the target user. Solution: No solution was available at the time of this entry.

Category 23.4 *HTML, XML, browsers*

2006-02-02 **Mozilla Internet browser Firefox Thunderbird multiple vulnerabilities remote attacker bypass security memory corruption**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2006/0413 23

MOZILLA PRODUCTS HAVE MULTIPLE MEMORY CORRUPTION AND SECURITY BYPASS ISSUES.

Multiple vulnerabilities were identified in Mozilla Suite, Mozilla Firefox and Thunderbird, which may be exploited by remote attackers to take complete control of an affected system or bypass security restrictions. The first issue is due to errors in the JavaScript engine that fails to properly protect certain temporary variables during garbage collection. The second flaw is due to a memory corruption error when dynamically changing the style of an element from "position:relative" to "position:static." The third vulnerability is due to an error when handling large history information passed in the "history.dat" file. The fourth issue is due to a memory corruption error when calling the "QueryInterface" method of the built-in Location and Navigator objects. The fifth flaw is due to an error in the "XULDocument.persist()" function that does not properly validate the attribute name. The sixth vulnerability is due to integer overflow errors in the E4X, SVG, and Canvas features. The seventh issue is due to an error in the XML parser. And the eighth flaw is due to an error in the E4X implementation that exposes the internal "AnyName" object to Web content. Solution: Upgrade to Firefox 1.5.0.1 or SeaMonkey 1.0: http://www.mozilla.org/products/ Disable JavaScript in Thunderbird and Mozilla Suite.

Category 23.4 *HTML, XML, browsers*

2006-02-07 **Mozilla software multiple vulnerabilities execute arbitrary code solution upgrade**

DHS IAIP Daily; http://www.uscert.gov/cas/techalerts/TA06−038A.html 23

US-CERT TECHNICAL CYBER SECURITY ALERT TA06-038A:
MULTIPLE VULNERABILITIES IN MOZILLA PRODUCTS.

Several vulnerabilities exist in the Mozilla Web browser and derived products. Systems affected: Mozilla software, including the following, is affected: Mozilla Web browser, e-mail and newsgroup client; Mozilla SeaMonkey; Firefox Web browser; and Thunderbird e-mail client. Impact: The most severe impact of these vulnerabilities could allow a remote attacker to execute arbitrary code with the privileges of the user running the affected application. Other impacts include a denial-of-service or local information disclosure. Solution: Upgrade to Mozilla Firefox 1.5.0.1 or SeaMonkey 1.0. For Mozilla-based products that have no updates available, users are strongly encouraged to disable JavaScript. Mozilla Firefox 1.5.0.1: http://www.mozilla.com/firefox/ SeaMonkey 1.0: http://www.mozilla.org/projects/seamonkey/

Category 23.4 *HTML, XML, browsers*

2006-02-07 **Mozilla Firefox Internet browser vulnerability exploit source code published Metasploit project**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/holes/story/0,10801,108469,00.html?SKC=security−108469 23

ATTACK CODE PUBLISHED FOR FIREFOX FLAW.

A hacker Tuesday, February 7, published code that exploits a vulnerability found in the latest version of Mozilla Corp.'s Firefox browser. The code, which targets the Firefox 1.5 browser, was posted Tuesday on The Metasploit Project site by a hacker known as H D Moore. Metasploit is a widely used hacking tool. Moore said that a hacker by the name of Georgi Guninski reported the flaw to the Mozilla Foundation on December 6, and that he had simply implemented and posted the technique described by Guninski. Mozilla published an advisory about the exploit last Wednesday as it released the Firefox 1.5.0.1 browser, which included a patch for the flaw. According to the advisory, the vulnerability, which had been rated as moderate, causes a corruption in the browser's memory that could be exploitable to run arbitrary code. Hacker Aviv Raff on Tuesday criticized Mozilla in his blog for under-rating the flaw. He has blasted the open-source group in the past for downplaying the seriousness of vulnerabilities that have been found in its software.

Category 23.4 *HTML, XML, browsers*

2006-02-08 **domain hijacking Web domain Internet browsers proxy servers**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1923546,00.asp 23

EFFECTS OF DOMAIN HIJACKING CAN LINGER.

Malicious hackers who are able to hijack an organization's Web domain may be able to steal traffic from the legitimate Website long after the domain has been restored to its owner, according to a recent report. Design flaws in the way Web browsers and proxy servers store data about Websites allow malicious hackers to continue directing Web surfers to malicious Webpages for days or even months after the initial domain hijacking. The persistent attack could lead to information or identity theft, according to Amit Klein, a Web application security researcher with the Web Application Security Consortium. The problem, which Klein termed "domain contamination" exists because of features in Web proxy servers, which store versions of Webpages, and Web "clients," or browsers, including Microsoft's Internet Explorer, the Mozilla Foundation's Firefox and the Opera browser. Proxy servers and browsers both establish trust relationships with Web servers that are identified as the authoritative host for a Webpage in the DNS (domain name system), Klein said. "Once a client believes it is communicating with the legitimate server for some domain, there's an implicit trust that's placed in that server that is not revoked," said Klein. Report: Domain Contamination: http://www.webappsec.org/projects/articles/020606.shtml

---

Category 23.4 *HTML, XML, browsers*

2006-02-14 **Microsoft IE zero-day exploit no patch advisory**

DHS IAIP Daily; http://www.crn.com/sections/breakingnews/dailyarchives.jhtml?articleId=180201596 23

MICROSOFT: IE ZERO-DAY BUG NOT WORTH PATCHING.

A new zero-day vulnerability in Internet Explorer (IE) is such a small deal, Microsoft said Tuesday, February 14, that it will not patch the bug, but instead will wait to fix it until it releases Windows XP SP3 in late 2007. The drag-and-drop flaw in IE 5.01, 5.5, and 6.0 was first reported to Microsoft in August 2005, and is somewhat similar to one addressed in a February 2005 security bulletin. "If an attacker can persuade a user to drag any object within the top-level window that his/her site is contained in, malicious script can redirect these inputs to other top-level windows, potentially resulting in an unintended consequence such as file installation," read an advisory published by SecuriTeam. Microsoft IE Advisory issued by SecuriTeam: http://www.securiteam.com/windowsntfocus/5MP0B0UHPA.html

---

Category 23.4 *HTML, XML, browsers*

2006-02-22 **Mozilla Thunderbird e-mail client validation error remote arbitrary code JavaScript execution**

DHS IAIP Daily; http://securitytracker.com/alerts/2006/Feb/1015665.html 23

MOZILLA THUNDERBIRD VALIDATION ERROR IN IFRAME SRC TAG LETS REMOTE USERS EXECUTE ARBITRARY JAVASCRIPT.

A vulnerability was reported in Mozilla Thunderbird. A remote user can cause arbitrary scripting code to be executed on the target user's system. Analysis: The software does not properly filter javascript from HTML tags. A remote user can send HTML based e-mail with arbitrary javascript in the SRC attribute of the IFRAME tag. When the target user edits the message (when replying to the message, for example), the javascript will be executed, regardless of the javascript settings in the preferences. Affection versions: 1.0.7 and prior versions. Solution: The vendor has issued a fixed version (1.5), available at: http://www.mozilla.com/thunderbird/

Category 23.4 *HTML, XML, browsers*

2006-02-22 **US CERT Alert Apple Mac OS X Safari command execution vulnerability**

DHS IAIP Daily; http://www.uscert.gov/cas/techalerts/TA06−053A.html 23

US-CERT TECHNICAL CYBER SECURITY ALERT TA06-053A:
APPLE MAC OS X SAFARI COMMAND EXECUTION VULNERABILITY.

A file type determination vulnerability in Apple Safari could allow a remote attacker to execute arbitrary commands on a vulnerable system. Apple Safari is a Web browser that comes with Apple Mac OS X. The default configuration of Safari allows it to automatically "Open 'safe' files after downloading." Due to this default configuration and inconsistencies in how Safari and OS X determine which files are "safe," Safari may execute arbitrary shell commands as the result of viewing a specially crafted Webpage. Systems affected: Apple Safari running on Mac OS X. Impact: A remote, unauthenticated attacker could execute arbitrary commands with the privileges of the user running Safari. If the user is logged on with administrative privileges, the attacker could take complete control of an affected system. Solution: Since there is no known patch for this issue at this time, US-CERT is recommending a workaround. Workaround: Disable "Open 'safe' files after downloading". Disable the option to "Open 'safe' files after downloading," as specified in the document "Securing Your Web Browser": http://www.us-cert.gov/reading_room/securing_browser/#sgeneral.

Category 23.4 *HTML, XML, browsers*

2006-02-28 **Internet Explorer Microsoft IE vulnerability flaw folder deletion iframe solution**

DHS IAIP Daily; http://www.hackerscenter.com/archive/view.asp?id=23176 23

INTERNET EXPLORER IFRAME FOLDER DELETION WEAKNESS.

Cyber flash has discovered a weakness in Internet Explorer, which can be exploited by malicious people to trick users into deleting local folders. Affected software: Microsoft Internet Explorer 6.x. Analysis: The problem is that network shares can be included in an iframe where only certain parts of the content is visible to the user. This can be exploited to trick users into deleting local folders via an iframe referencing "\127.0.0.1c$." Successful exploitation requires that the user selects a folder icon, presses the delete key, and accepts a "Folder Delete" dialog. Solution: Do not accept suspicious "Folder Delete" dialogs when visiting untrusted Websites.

Category 23.4 *HTML, XML, browsers*

2006-03-16 **US CERT Cyber Security Alert Adobe Macromedia Flash vulnerabilities flaws**

DHS IAIP Daily; http://www.uscert.gov/cas/techalerts/TA06−075A.html 23

US-CERT TECHNICAL CYBER SECURITY ALERT TA06-075A:
ADOBE MACROMEDIA FLASH PRODUCTS CONTAIN VULNERABILITIES.

There are critical vulnerabilities in Macromedia Flash player and related software. Exploitation of these vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary code or cause a denial-of-service on a vulnerable system. Systems affected: Microsoft Windows, Apple Mac OS X, Linux, Solaris, or other operating systems with any of the following Adobe Macromedia products installed: Flash Player 8.0.22.0 and earlier; Flash Professional 8; Flash Basic; Flash MX 2004; Flash Debug Player 7.0.14.0 and earlier; Flex 1.5; Breeze Meeting Add-In 5.1 and earlier; Adobe Macromedia Shockwave Player 10.1.0.11 and earlier. For more complete information, refer to Adobe Security Bulletin APSB06-03: http://www.macromedia.com/devnet/security/security_zone/apsb 06-03.html Solution: Apply updates: Adobe has provided the updates for these vulnerabilities in APBS06-03: http://www.macromedia.com/devnet/security/security_zone/apsb 06-03.html Disable Flash: Please see Microsoft Security Advisory 916208 for instructions on how to disable Flash on Microsoft Windows. For other operating systems and Web browsers, please contact the appropriate vendor. Microsoft Security Advisory 916208: http://www.microsoft.com/technet/security/advisory/916208.mspx

---

Category 23.4 *HTML, XML, browsers*

2006-03-20 **Microsoft IE Internet Explorer vulnerability denial-of-service DoS weakness**

DHS IAIP Daily; http://www.hackerscenter.com/archive/view.asp?id=23679 23

INTERNET EXPLORER MULTIPLE EVENT HANDLERS DENIAL-OF-SERVICE WEAKNESS.

There is a weakness in Internet Explorer, which can be exploited by malicious people to cause a denial-of-service. Analysis: The vulnerability is caused due to an array boundary error in the handling of HTML tags with multiple event handlers. This can be exploited to crash a vulnerable browser via a HTML tag with 94 or more event handlers. Affected software: Microsoft Internet Explorer 6.x. Solution: Do not visit untrusted Websites.

Category 23.4 *HTML, XML, browsers*

2006-03-23 **Microsoft IE Internet Explorer dangerous zero-day exploit security advisory**

DHS IAIP Daily; http://www.techweb.com/wire/security/183702421 23

MICROSOFT WARNS OF DANGEROUS INTERNET EXPLORER EXPLOIT.

An exploit for a new zero-day bug in Internet Explorer appeared Thursday, March 23, causing security companies to ring alarms and Microsoft to issue a security advisory that promised it would patch the problem. Just a day after anti-virus vendors warned of a new zero-day vulnerability in Internet Explorer -- the second such alert since Friday, March 17 -- companies including Symantec and Secunia boosted security levels as news of a public exploit spread. Although the publicly-posted exploit only launches a copy of the Windows calculator, "replacing the shellcode in this exploit would be trivial even for an unskilled attacker," Symantec continued. Microsoft confirmed the severity of the bug and the success of the exploit in its own advisory, issued late Thursday. Microsoft advisory: http://www.microsoft.com/technet/security/advisory/917077.mspx

---

Category 23.4 *HTML, XML, browsers*

2006-03-27 **Microsoft IE Internet Explorer system compromise vulnerability .HTA application run**

DHS IAIP Daily; http://secunia.com/advisories/19378/ 23

INTERNET EXPLORER UNSPECIFIED AUTOMATIC .HTA APPLICATION EXECUTION.

A vulnerability has been reported in Internet Explorer, which can be exploited to compromise a user's system. Analysis: The vulnerability is caused due to an unspecified error when handling .HTA applications and allows execution of the .HTA application on the user's system without any user interaction when e.g. visiting a malicious Website. Vulnerable software: Microsoft Internet Explorer 6.x. Solution: Do not visit untrusted Websites. Disabling Active Scripting support may prevent exploitation, but has not been proven.

Category 23.4 *HTML, XML, browsers*

2006-03-28 **Microsoft IE Internet Explorer browser zero-day exploit temporary patch release Eeye Digital Security**

DHS IAIP Daily; 23
http://www.securitypipeline.com/news/184400787;jsessionid=PDRAQICTESZRYQSNDBECKICCJUMEKJVN

SECURITY FIRM RELEASES PATCH FOR ZERO-DAY INTERNET EXPLORER FLAW.

Eeye Digital Security has released a temporary patch for a zero-day vulnerability in Internet Explorer (IE) that is being used by malicious Websites to install spyware on users' computers, officials said Tuesday, March 28. The eEye patch is meant as a placeholder until Microsoft Corp. releases a permanent fix, which is expected by Tuesday, April 11, said Marc Maiffret, co-founder and chief hacking officer of eEye. At that time, users of the eEye patch are advised to use the add/remove program in Windows to delete the fix before installing the Microsoft patch. The vulnerability, called the CreateTextRange bug, enables hackers to exploit active scripting in IE to install keystroke loggers and other malicious software.

Category 23.4 *HTML, XML, browsers*

2006-03-30 **hacker BBC News Website IE attack lure social engineering Websense Security**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1944579,00.asp 23

HACKERS USE BBC NEWS AS IE ATTACK LURE.

According to an alert issued by Websense Security Labs, excerpts from actual BBC News stories are being used to lure Internet Explorer users to Websites that launch drive-by downloads of bots, spyware, back doors and other Trojan downloaders. One version of the spammed e-mail contains a portion of a BBC News item published on Monday, March 27, about the Chinese Yuan hitting a 12 post-revaluation high against the U.S. dollar. Websense researchers found that the rigged site exploits the unpatched createTextRange vulnerability. Websense Security Labs Alert: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =452 After the legitimate excerpt, the hackers embedded a "read more" link.

Category 23.4 *HTML, XML, browsers*

2006-03-31 **Microsoft Internet Explorer IE malware malicious software exploit vulnerability class**

DHS IAIP Daily; 23
http://www.infoworld.com/article/06/03/31/77027_HNiemalware_ 1.html

NEW GENERATION OF IE MALWARE NOW CIRCULATING.

Hackers have posted a new version of malicious software that will make it easier for them to exploit an unpatched vulnerability in the Internet Explorer (IE) browser. The software was posted by hackers Friday, March 31, to the Milw0rm.com Website. The code exploits a flaw in the way IE processes Webpages using the createTextRange() method. Hackers have been using malware that takes advantage of this vulnerability to install unauthorized software on victims' computers over the past week, but this new generation is considered to be more dangerous. The new software works more quickly, meaning it will be particularly effective on older machines with limited memory and processing capabilities.

Category 23.4 *HTML, XML, browsers*

2006-04-06 **Microsoft Internet Explorer IE risky vulnerability patch issue**

DHS IAIP Daily; http://news.zdnet.com/2100−1009_22−6058548.html 23

MICROSOFT TO SLAP PATCH ON RISKY IE HOLE.

As part of its monthly patching cycle, Microsoft plans to release five security bulletins (at least one of which is classified “critical”) with fixes for flaws in Windows and Office on Tuesday, April 11. One of Tuesday's bulletins will be for its Internet Explorer (IE) Web browser. It will include a comprehensive update with multiple fixes, including one for the publicly known "CreateTextRange" vulnerability. In addition, Microsoft will be releasing an updated version of the Windows Malicious Software Removal Tool and a patch to change the way IE handles Web programs called ActiveX controls.

Category 23.4 HTML, XML, browsers

2006-04-12 **packet data fuzzing crash Internet browser crash methods HD Moore**

DHS IAIP Daily; http://www.securityfocus.com/news/11387 23

BROWSER CRASHERS WARM TO DATA FUZZING.

Last month, security researcher HD Moore decided to write a simple program that would mangle the code found in Webpages and gauge the effect such data would have on the major browsers. The result: hundreds of crashes and the discovery of several dozen flaws. The technique -- called packet, or data, fuzzing -- is frequently used to find flaws in network applications. Moore and others are now turning the tool on browsers to startling results. In a few weeks, the researcher had found hundreds of ways to crash Internet Explorer and, to a lesser extent, other browsers. In another example, it took less than an hour at the CanSecWest Conference last week for Moore and information-systems student Matthew Murphy to hack together a simple program to test a browser's handling of cascading style sheets, finding another dozen or so ways to crash browsers. "Fuzzing is probably the easiest way to find flaws, because you don't have to figure out how the application is dealing with input," said Moore, a well-known hacker and the co-founder of the Metasploit Project.

Category 23.4 HTML, XML, browsers

2006-04-12 **Microsoft backlash IE patch lawsuit patent lawsuit Eolas ActiveX changes**

DHS IAIP Daily; http://www.securitypipeline.com/news/185300871 23

MICROSOFT SPARKS BACKLASH BY TYING IE CHANGES TO PATCH.

By packaging a functionality change for Internet Explorer (IE) with a needed security update, Microsoft has alienated some IT professionals, security vendors complained Wednesday, April 12. Along with the 10 patches within the Tuesday, April 11, MS06-013 Security Bulletin, Microsoft bundled changes to IE's handling of ActiveX controls. Those changes, which were prompted by a 2003 $521 million judgment against Microsoft in a patent lawsuit brought by Eolas Technologies Inc. and the University of California, will require users to manually activate controls on some sites. The inclusion of the ActiveX changes "makes everything a mess" for companies deploying and testing Microsoft's monthly patches, said Mike Murray, director of research at vulnerability management vendor, nCircleMurray. Instead, Microsoft should have separated the IE ActiveX changes from the security fixes. "They easily could have deployed it as a separate patch or rolled it into a service pack," said Murray.

Category 23.4 HTML, XML, browsers

2006-04-13 **Mozilla memory corruption information disclosure vulnerabilities**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2006/1356 23

MOZILLA PRODUCTS MEMORY CORRUPTION AND INFORMATION DISCLOSURE VULNERABILITIES.

Multiple vulnerabilities have been identified in Mozilla Firefox, Mozilla Suite, SeaMonkey, and Thunderbird, which may be exploited by remote attackers to take complete control of an affected system, bypass security restrictions, or disclose sensitive information. For details on the 22 flaws outlined by FrSIRT, please see source advisory. Vulnerable products: Firefox versions prior to 1.5; Firefox versions prior to 1.0.8; Mozilla Suite versions prior to 1.7.13; SeaMonkey versions prior to 1.0; Thunderbird versions prior to 1.5.0.2; Thunderbird versions prior to 1.0.8. Solution: Upgrade to Firefox 1.5 or 1.0.8: http://www.mozilla.com/firefox/ Upgrade to Mozilla Suite 1.7.13: http://www.mozilla.org/products/mozilla1.x/ Upgrade to SeaMonkey 1.0: http://www.mozilla.org/projects/seamonkey/ Upgrade to Thunderbird 1.5.0.2 or 1.0.8: http://www.mozilla.com/thunderbird/

Category 23.4 HTML, XML, browsers

2006-04-14 **company IE patch warning Microsoft Internet Explorer IE interference applications**

DHS IAIP Daily; http://news.com.com/2100−1002_3−6061597.html 23

COMPANY WARNS ON IE PATCH.

An Internet Explorer update released earlier last week can interfere with some applications, including Google's Toolbar, according to PatchLink, a maker of patch management software. Other applications affected by the Web browser patch include business software from Oracle's Siebel customer relationship management unit and certain Web applications that use specific versions of Java, PatchLink said Friday, April 14. The problems arise because of changes Microsoft made to how the Web browser handles Web programs called ActiveX controls. The modifications are designed to shield Microsoft from liability in a high-profile patent dispute with Eolas Technologies and the University of California.

Category 23.4 *HTML, XML, browsers*

2006-04-15 **Microsoft Internet Explorer MS IE patent infringement software upgrade patch user interface**

RISKS 24 25

MS IE PATCH ALTERS USER INTERACTIONS WITH EMBEDDED OBJECTS

OK, let's be fair about this, the underlying purpose of the Microsoft patch isn't to break Web pages, though this result was understood and expected.

I haven't seen a detailed discussion of the implications of this situation in RISKS (some venues are calling the issue a "mini-Y2K" -- which is a bit overdramatic), but it *is* important. As of a few days ago, vast numbers of Internet Explorer (IE) users are experiencing Web pages all over the Net which simply don't work as expected any more.

Simplified backstory first. A couple of years ago, Microsoft lost a patent fight over commonly used techniques to embed "active" content into Web pages. While "ActiveX" operations are usually cited in this regard, in reality all manner of embedded active player objects are apparently involved, including Flash, QuickTime, RealPlayer, Java, etc. . . .

In any case, MS decided that they didn't want to pay the associated license fees for the patented techniques (so far, the holders of the patent have seemingly not gone after open source browsers in non-commercial contexts -- such as Firefox -- which is why Firefox is not currently affected by this issue).

Several months ago, MS issued a patch to change IE behavior to what they believe is a non-infringing operation. This requires that users explicitly click embedded objects first (theoretically guided by a small hint message that appears if they happen to mouse over the objects, which will supposedly be visually boxed as a cue), before the objects will become active. In the case of active objects that already require a click to start, this means that *two* clicks will now be needed.

There are variations on this theme. For example, in some cases, playback of video may commence automatically, but the video control buttons reportedly won't be active unless the user clicks them first. Confusing? Yep.

There are ways to redesign Web pages to restore the original behaviors, more or less. But these typically require the use of embedded javascript, which introduces its own complexity and security issues, especially on large sites. . . .

[Commentary by Lauren Weinstein]

Category 23.4 *HTML, XML, browsers*

2006-04-17 **US CERT Technical Cyber Security Alert Mozilla product vulnerabilities**

DHS IAIP Daily; http://www.uscert.gov/cas/techalerts/TA06−107A.html 23

US-CERT TECHNICAL CYBER SECURITY ALERT TA06-107A: MOZILLA PRODUCTS CONTAIN MULTIPLE VULNERABILITIES.

The Mozilla Web browser and derived products contain several vulnerabilities; the most serious of which could allow a remote attacker to execute arbitrary code on an affected system. More detailed information is available in the individual vulnerability notes. See source for more details. Systems affected: Mozilla Web browser, e-mail and newsgroup client; Mozilla SeaMonkey; Firefox Web browser; Thunderbird e-mail client; Mozilla Suite. Note: Any products based on Mozilla components, particularly Gecko may also be affected. Solution: Upgrade to Mozilla Firefox 1.5.0.2, Mozilla Thunderbird 1.5.0.2, or SeaMonkey 1.0.1. According to Mozilla.org, Thunderbird 1.5.0.2 is to be released on April 18, 2006. Users are strongly encouraged to apply the workarounds described in the individual vulnerability notes listed within the source until updates can be applied. Firefox 1.5.0.2: http://www.mozilla.com/firefox/ Thunderbird 1.5.0.2: http://www.mozilla.com/thunderbird/releases/1.5.0.2.html SeaMonkey 1.0.1: http://www.mozilla.org/projects/seamonkey/

Category 23.4 *HTML, XML, browsers*

2006-04-18 **hacker sneak penetration browser vulnerability exploit Microsoft Internet Explorer IE**

DHS IAIP Daily; http://www.it− observer.com/news/6119/hackers_sneak_through_b rowser_vulnerability/ 23

HACKERS SNEAK THROUGH BROWSER VULNERABILITY.

Security experts from MicroWorld Technologies claim that a new exploit, named "Exploit.JS.CVE-2006-1359.c," is used by hackers to sneak into computers through a vulnerability in Internet Explorer (IE). Exploit.JS works by pushing an unexpected and unrecognizable HTML element that crashes IE. Then the Exploit forces IE to execute a malicious program to infiltrate into the computer. The vulnerability stems out from the way in which IE displays Webpages that use unexpected methods to call some HTML objects. Microsoft has already identified this loophole and has released a patch.

Category 23.4 *HTML, XML, browsers*

2006-04-26 **Mozilla Suite Firefox browser Javascript validation vulnerability solution update**

DHS IAIP Daily; http://www.securityfocus.com/bid/13232/discuss 23

MOZILLA SUITE AND FIREFOX XPINSTALL JAVASCRIPT OBJECT INSTANCE VALIDATION VULNERABILITY.

Mozilla Suite and Mozilla Firefox are affected by an input validation vulnerability. This issue is due to a failure in the application to verify input passed to installation objects. Analysis: Firefox and the Mozilla Suite support custom "favicons" through the tag. If a link tag is added to the page programmatically and a javascript URL is used, then script will run with elevated privileges and could run or install malicious software. For a complete list of vulnerable products: http://www.securityfocus.com/bid/13232/info Solution: Mozilla has released and advisory along with upgrades dealing with this issue. For further information: http://www.securityfocus.com/bid/13232/references

---

Category 23.4 *HTML, XML, browsers*

2006-04-26 **Microsoft Internet Explorer IE patch response Web browser**

DHS IAIP Daily; http://www.washingtonpost.com/wp− dyn/content/article/2006/04 /25/AR2006042501910.html 23

IE REVISED IN RESPONSE TO SECURITY CONCERNS, LOSS OF USERS.

Internet users were given a peek Tuesday, April 25, at a revamped version of Microsoft Corp.'s Internet Explorer (IE), a response to criticism that the most popular tool for Web surfing and hacking made users vulnerable to the Internet's dangers and caused them to defect to alternative browsers. A test version of IE 7 is available for download from Microsoft's Website, with tighter security protection and more advanced tools to give the user greater control in navigating the Web, said Dean Hachamovitch, general manager of IE. The company has improved its ability to write secure code, but it's unclear if the latest tools will address other dangers on the Internet, which require users to be more savvy, said Bruce Schneier, chief technical officer at Counterpane Internet Security Inc.

Category 23.4 *HTML, XML, browsers*

2006-04-27 **Microsoft Internet Explorer IE bug vulnerability denial-of-service DoS**

DHS IAIP Daily; http://securitytracker.com/alerts/2006/Apr/1016001.html 23

MICROSOFT INTERNET EXPLORER BUG IN PROCESSING NESTED OBJECT TAGS LETS REMOTE USERS DENY SERVICE.

A vulnerability was reported in Microsoft Internet Explorer. A remote user can cause denial-of-service conditions and may be able to cause arbitrary code to be executed on the target user's system. Analysis: The browser does not properly process certain combinations of nested OBJECT tags. A remote user can create specially crafted HTML that, when loaded by the target user, will trigger a NULL pointer dereference and cause the target user's browser crash. It may also be possible to execute arbitrary code, but code execution was not confirmed in the report. Affected version: 6. No solution was available at the time of this entry.

Category 23.4 *HTML, XML, browsers*

2006-04-27 **Mozilla products software memory corruption code injection access restriction bypass vulnerability solution update**

DHS IAIP Daily; http://www.securityfocus.com/bid/16476/discuss 23

MULTIPLE MOZILLA PRODUCTS MEMORY CORRUPTION/CODE INJECTION/ACCESS RESTRICTION BYPASS VULNERABILITIES.

Multiple Mozilla products are prone to multiple vulnerabilities. These issues include various memory corruption, code injection, and access restriction bypass vulnerabilities. Analysis: Garbage collection hazards have been found in the JavaScript engine where some routines used temporary variables that were not properly protected (rooted). Dynamically changing the style of an element from position: relative to position: static can cause Gecko to operate on freed memory. Calling the QueryInterface method of the built in Location and Navigator objects causes memory corruption that might be exploitable to run arbitrary code. XULDocument.persist() did not validate the attribute name, allowing an attacker to inject XML into localstore.rdf that would be read and acted upon at startup. An upgrade in the XML parser introduced a bug that could read beyond the end of the buffer, often causing a crash. The implementation of E4X introduced an internal "AnyName" object which was unintentionally exposed to Web content. Successful exploitation of these issues may permit an attacker to execute arbitrary code in the context of the affected application. This may facilitate a compromise of the affected computer. For a complete list of vulnerable products: http://www.securityfocus.com/bid/16476/info Solution: Please see the referenced vendor advisories for details on obtaining and applying fixes: http://www.securityfocus.com/bid/16476/references

---

Category 23.4 *HTML, XML, browsers*

2006-04-28 **Microsoft Internet Explorer IE bug second in a week proof-of-concept exploit code**

DHS IAIP Daily; 23
http://www.infoworld.com/article/06/04/28/77853_HNsecondbug_ 1.html

DESPITE DISCOVERY OF SECOND IE BUG, MICROSOFT WILL NOT ISSUE A FIX.

For the second time in a week, hackers have discovered a previously unknown bug in Microsoft Corp.'s Internet Explorer (IE). Although "proof-of-concept" code showing how this vulnerability could be exploited has been published, there are some mitigating factors. Attackers would first need to trick users into visiting a specially coded Webpage and then somehow get them to perform certain actions, such as writing "specific text in a text field," before they could run their malicious software, FrSIRT said. Furthermore, the bug reportedly does not affect the latest versions of Microsoft's Windows and Windows Server 2003 operating systems, FrSIRT said. Because of these factors, Microsoft has decided not to fix the bug in a security update to IE.

Category 23.4 *HTML, XML, browsers*

2006-05-03 **Mozilla Firefox iframe content window vulnerability JavaScript content arbitrary code execution attack solution update**

DHS IAIP Daily; http://www.securityfocus.com/bid/17671/discuss 23

MOZILLA FIREFOX IFRAME.CONTENT WINDOW.FOCUS DELETED OBJECT REFERENCE VULNERABILITY.

Mozilla Firefox is prone to a vulnerability when rendering malformed JavaScript content. An attacker could exploit this issue to cause the browser to fail or potentially execute arbitrary code. Analysis: The memory corruption error when processing a specially crafted HTML script that contains references to deleted objects and the "designMode" property is enabled, which could be exploited by attackers to crash a vulnerable browser or remotely take complete control of an affected system by tricking a user into visiting a malicious Webpage. Vulnerable: Mozilla Firefox 1.5.2; Mozilla Firefox 1.5.1; Mozilla Firefox 1.5 beta 2; Mozilla Firefox 1.5 beta 1; Mozilla Firefox 1.5; Mozilla Firefox 1.5.0.2. Not vulnerable: Mozilla Firefox 1.5.3. Solution: The vendor has released an advisory, along with fixes to address this issue. Please see the referenced advisory for further information: http://www.mozilla.org/security/announce/2006/mfsa2006-30.html

---

Category 23.4 *HTML, XML, browsers*

2006-05-04 **Mozilla Thunderbird e-mail client multiple remote information disclosure vulnerabilities no solution**

DHS IAIP Daily; http://www.securityfocus.com/bid/16881/references 23

MOZILLA THUNDERBIRD MULTIPLE REMOTE INFORMATION DISCLOSURE VULNERABILITIES.

Mozilla Thunderbird is susceptible to multiple remote information disclosure vulnerabilities. These issues are due to the application's failure to properly enforce the restriction for downloading remote content in e-mail messages. Analysis: Thunderbird's HTML rendering engine insufficiently filters the loading of external resources from inline HTML attachments. External files are downloaded even if the "Block loading of remote images in mail messages" option is enabled. These issues allow remote attackers to gain access to potentially sensitive information, aiding them in further attacks. Attackers may also exploit these issues to know whether and when users read e-mail messages. For a complete list of vulnerable products: http://www.securityfocus.com/bid/16881/info Solution: Currently, Security Focus is not aware of any vendor-supplied patches for this issue.

Category 23.4 *HTML, XML, browsers*

2006-05-04 **Mozilla Firefox Thunderbird debug mode insecure temporary file creation vulnerability solution update**

DHS IAIP Daily; http://www.securityfocus.com/bid/14443/discuss 23

MOZILLA SUITE, FIREFOX AND THUNDERBIRD DEBUG MODE INSECURE TEMPORARY FILE CREATION VULNERABILITY.

Mozilla Suite, Firefox, and Thunderbird create temporary files in an insecure manner. Analysis: A local attacker would most likely take advantage of this vulnerability by creating a malicious symbolic link in a directory where the temporary files will be created. When the program tries to perform an operation on a temporary file, it will instead perform the operation on the file pointed to by the malicious symbolic link. For a complete list of vulnerable products: http://www.securityfocus.com/bid/14443/info Solution: The vendor has addressed these issues in subsequent versions of the affected applications. For more information: http://www.securityfocus.com/bid/14443/references

---

Category 23.4 *HTML, XML, browsers*

2006-05-09 **Adobe Dreamweaver remote user SQL injection vulnerability solution update**

DHS IAIP Daily; http://securitytracker.com/alerts/2006/May/1016050.html 23

ADOBE DREAMWEAVER MAY LET REMOTE USERS INJECT SQL CODE.

A vulnerability was reported in Adobe Dreamweaver. A remote user may be able to inject SQL commands. Analysis: Code generated by Dreamweaver server behaviors for the ColdFusion, PHP mySQL, ASP, ASP.NET, and JSP server models may not properly validate user supplied input. A remote user can supply a specially crafted parameter value to execute SQL commands on the underlying database. Affected versions: Dreamweaver 8 and Dreamweaver MX 2004. Solution: The vendor has issued a fix (Dreamweaver 8.0.2 updater), available at: http://www.adobe.com/support/dreamweaver/downloads_updaters. html#dw8 The Adobe advisory is available at: http://www.adobe.com/support/security/bulletins/apsb06-07.html

---

Category 23.4 *HTML, XML, browsers*

2006-05-09 **Mozilla products memory corruption code injection access restriction bypass vulnerability solution update**

DHS IAIP Daily; http://www.securityfocus.com/bid/16476/discuss 23

MULTIPLE MOZILLA PRODUCTS MEMORY CORRUPTION/CODE INJECTION/ACCESS RESTRICTION BYPASS VULNERABILITIES.

Multiple Mozilla products are prone to multiple vulnerabilities. Analysis: These issues include various memory corruption, code injection, and access restriction bypass vulnerabilities. Successful exploitation of these issues may permit an attacker to execute arbitrary code in the context of the affected application. This may facilitate a compromise of the affected computer; other attacks are also possible. For a complete list of vulnerable products: http://www.securityfocus.com/bid/16476/info For more information on obtaining fixes: http://www.securityfocus.com/bid/16476/references

---

23.5 E-mail & instant messaging or chat

Category 23.5 *E-mail & instant messaging or chat*

2000-04-27 **e-mail execution arbitrary code e-mail URL link vulnerability hole**

RISKS; Peacefire http://www.peacefire.org/security/stealthattach/ 20 88

Peacefire reported a new class of exploits using e-mail to force execution of arbitrary code by the Eudora e-mail client when a user clicks on an embedded URL in an HTML-enabled e-mail message. Bennett Haselton, writing in RISKS, said, "Security holes that allow you to run code on a remote user's machine just by sending them e-mail, are extremely dangerous — a hacker could use this to steal or erase any classified data on a remote user's hard drive, even if that user were behind a corporate firewall and had anti-virus software running. A virus writer could use the exploit to write a virus that could spread to almost all Eudora users — numbering in the millions — and potentially do hundreds of millions of dollars' worth of damage. (Unlike most such tricks, this exploit does not require the user to do anything "naive", like run an .exe that is sent to them as an attachment.) USA Today reported last year on the "BubbleBoy" virus, which similarly used a security hole in Microsoft Outlook to cause code to run on a user's machine, simply by reading an e-mail message"

Category 23.5 *E-mail & instant messaging or chat*

2000-05-05 **QA quality assurance design flaw programming language functionality**

RISKS, BBC 20 88
http://news.bbc.co.uk/low/english/sci/tech/newsid_737000/737396.stm

Russ Cage noted a rare burst of insight in the non-technical press about the fundamental reason there are e-mail enabled worms floating around cyberspace: the decision by Microsoft to include programming functionality as part of its office products. Writing in RISKS, he quoted from a BBC news article as follows: "Peter Sommer... told BBC News Online that Microsoft created these by building in to their software the tools needed to customize applications. Microsoft customers are going to have to ask the company to review very carefully the level of functionality that they are putting into their systems. [...] One has got to ask why products are put out which contain these programming languages, which may be of use to perhaps only 3 to 4% of the customers but for everyone else presents a considerable threat. [...] These features are also very difficult to turn off. The lesson from Love Bug is that people must be able to kill off this programming functionality within applications programs."

Category 23.5 *E-mail & instant messaging or chat*

2000-06-14 **antivirus security sandbox restriction script limitations e-mail worms patch fix improvement**

RISKS, Reliable Software Technologies http://www.rstcorp.com/news/jbf.html 20 92

Gary McGraw announced, "Reliable Software Technologies has just released a new program (JustBeFriends) designed to prevent e-mail macro viruses from spreading. It can be used along with or instead of the Microsoft supplied e-mail protection patch. JustBeFriends works will all versions of Outlook and Outlook Express, and is substantially simpler than the Microsoft patch." The program prevents all automated, script-based access to Outlook programs, thus blocking the mechanism used by e-mail enabled worms.

Category 23.5 *E-mail & instant messaging or chat*

2001-07-23 **e-mail bounce management ISP SMTP header**

RISKS 21 56

Robert J. Woodhead suggested a useful improvement in list server software. Writing in RISKS, he explained that AOL bounce messages fail to include the _original_ destination address, making it impossible to fix mailing lists when someone redirects messages to another e-mail address. He wrote, "If mail servers added an "Original-Recipient:" header if they have to forward the e-mail (and there isn't already one in the headers), life would be immeasurably easier for bounce management. A standard for bounce reporting that made life easy for nonhumans would also seem to be an obvious idea."

Category 23.5 *E-mail & instant messaging or chat*

2002-01-04 **denial-of-service DoS attack vulnerability servers instant messaging chat**

NewsScan

AOL FIXES BUG IN INSTANT MESSENGER
AOL Time Warner says it has patched the software on its central servers to fix a problem in the free, downloadable version of the Windows versions of its Instant Messenger (AIM) software that could have allowed a network vandal to flood a victim's computer with data. (San Jose Mercury News 4 Jan 2002)
http://www.siliconvalley.com/docs/news/svfront/aol010402.htm

Category 23.5 *E-mail & instant messaging or chat*

2002-03-10 **e-mail chat vulnerabilities ICAT CVE**

ICAT Metabase

The ICAT Metabase < http://icat.nist.gov/icat.cfm > for the Common Vulnerabilities and Exposures (CVE) database reported the following vulnerabilities involving e-mail or chat for the period from 1 Jan 2001 to 10 Mar 2002:

CAN-2001-0581: Spytech Spynet Chat Server 6.5 allows a remote attacker to create a denial of service (crash) via a large amount (> 100) of connections to port 6387. Published Before: 8/22/2001 Severity: Medium

CAN-2001-0615: Directory traversal vulnerability in Faust Informatics Freestyle Chat server prior to 4.1 SR3 allows a remote attacker to read arbitrary files via a specially crafted URL which includes variations of a '..' (dot dot) attack such as '...' or '....'. Published Before: 8/14/2001 Severity: Medium

CAN-2001-0616: Faust Informatics Freestyle Chat server prior to 4.1 SR3 allows a remote attacker to create a denial of service via a URL request which includes a MS-DOS device name (e.g., GET /aux HTTP/1.0). Published Before: 8/14/2001 Severity: Medium

CAN-2001-0726: Outlook Web Access (OWA) in Microsoft Exchange 5.5 Server, when used with Internet Explorer, does not properly detect certain inline script, which can allow remote attackers to perform arbitrary actions on a user's Exchange mailbox via an HTML e-mail message. Published Before: 12/6/2001 Severity: High

CAN-2001-0792: Format string vulnerability in XChat 1.2.x allows remote attackers to execute arbitrary code via a malformed nickname. Published Before: 10/18/2001 Severity: High

CAN-2001-0857: Cross-site scripting vulnerability in status.php3 in Imp Webmail 2.2.6 and earlier allows remote attackers to gain access to the e-mail of other users by hijacking session cookies via the message parameter. Published Before: 12/6/2001 Severity: Medium

CAN-2001-0945: Buffer overflow in Outlook Express 5.0 through 5.02 for Macintosh allows remote attackers to cause a denial of service via an e-mail message that contains a long line. Published Before: 12/3/2001 Severity: Medium

CVE-2000-1148: The installation of VolanoChatPro chat server sets world-readable permissions for its configuration file and stores the server administrator passwords in plaintext, which allows local users to gain privileges on the server. Published Before: 1/9/2001 Severity: Medium

CVE-2001-0154: HTML e-mail feature in Internet Explorer 5.5 and earlier allows attackers to execute attachments by setting an unusual MIME type for the attachment, which Internet Explorer does not process correctly. Published Before: 5/3/2001 Severity: Medium

---

Category 23.5 *E-mail & instant messaging or chat*

2002-03-11 **cellular phones wireless virus worm malware palmtop**

NewsScan

FOR VANDALS, SMART PHONES NEW AND INVITING TARGETS
Stephen Trilling, research at Symantec, which makes antivirus software, warns: "We should think of smart phones as just another set of computers on the Internet. If they're connected to the Internet they can be used to transmit threats and attack targets, just as any computer can. It's technically possible right now." Recently, several software companies have begun selling antivirus and encryption software for smartphone operating systems made by Palm, Microsoft and the Symbian platform common in Europe. Ari Hypponen enumerates some of the dangers: "If a malicious piece of code gets control of your phone, it can do everything you can do. It can call toll numbers. It can get your messages and send them elsewhere. It can record your passwords." And he adds that it's not that hard to do: "It's possible for anyone to make custom software for this platform. Teens can download development tools and write their own software." (San Jose Mercury News 10 Mar 2002)
http://www.siliconvalley.com/mld/siliconvalley/2833740.htm

Category 23.5 *E-mail & instant messaging or chat*

2002-05-08 **anti-malware e-mail worm virus moderated mailing list design standards**

RISKS 22 06

Mailing list management software often uses a coded REPLY-TO address so that the moderator can simply REPLY to a proposed posting and send it to the entire list. Unfortunately, an anti-virus running on the moderator's workstation does the same when it encounters a virus-infested submission, thus sending the infection out to the entire list without letting the moderator stop it.

In a followup piece, a RISKS contributor noted that the design error is the anti-virus package's use of the REPLY-TO field rather than the RETURN-PATH address. In other words, the sender of the message should be informed that it is virus infected; the recipient of replies may be very different from the sender, as in this case.

Category 23.5 *E-mail & instant messaging or chat*

2002-05-10 **instant messenger online chat quality assurance QA**

NewsScan

SOFTWARE WILL HAVE FLAWS
Microsoft says that the latest versions of its MSN Messenger program contain a "critical" flaw that a hacker could exploit for malicious purposes. At issue is a feature that allows users to congregate in a virtual "chat room" to exchange messages . A Microsoft executive says: "Software always will have flaws. We always do our best to ensure we do not have flaws or vulnerabilities, but while we strive for perfection, we know we're not always going to achieve perfection." (AP/USA Today 9 May 2002)
http://www.usatoday.com/life/cyber/tech/2002/05/09/messenger-flaw.htm

---

Category 23.5 *E-mail & instant messaging or chat*

2002-05-27 **HTML control command language e-mail**

RISKS 22 10

In a newsletter sent to 40,000 recipients, I included a block of HTML code showing a forged header.

The e-mail list software spotted what it thought was the end of the document and inserted the e-mail address of each recipient in that person's copy of the newsletter, making many readers believe that their e-mail address had been distributed to the entire list. Result: hundreds of letters (some nice, some not).

LESSONS:

(1) When designing macros that scan for search strings associated with a particular condition (in this case, the end of a message), it would be wise to test the presumption that the condition is in fact true. In this example, perhaps a second check might verify that there is in fact no further text in the message before inserting the valediction.

(2) When quoting control language (in this case, HTML), and in the absence of some sort of escape character (meaning "the following is literal text, not command language"), we may avoid accidents by using symbol substitution to prevent accidental misreading of the quoted strings as if they were actually to be interpreted.

Category 23.5 *E-mail & instant messaging or chat*

2002-05-29 **instant messaging chat vulnerabilities tunneling**

NewsScan

INSTANT MESSAGING CAN OPEN CORPORATE NETS TO VANDALISM
AOL and Microsoft freely admit that their popular instant messaging systems were designed for chat and not for transmission of sensitive corporate messages, but they are now building secure IM services for use by large customer groups. Why? Because, according to research firm IDC, 54 million employees this year will be using consumer IM systems for work-related purposes. Until they're using more secure instant messaging systems, companies need to be careful of what they do. Security expert Dan Ingevaldson of Internet Security Systems says that free IM systems represent a "huge gaping security risk for companies." (USA Today 28 May 2002)
http://www.usatoday.com/life/cyber/tech/2002/05/29/im-security.htm

---

Category 23.5 *E-mail & instant messaging or chat*

2002-09-04 **instant messaging surveillance workplace communication standards policies telecommuting**

NewsScan

INSTANT MESSAGING A HIT IN CORPORATE WORLD
Businesses with multiple office locations increasingly are finding that instant messaging can provide the real-time connectivity missing in e-mail and voice-mail exchanges. The beauty of IM, as it's called, is not only that it catches the recipient's attention immediately by popping up on his or her screen, but it also tells the sender which recipients are available to communicate at that moment. IM is "absolutely useful in trying to figure out, 'Can I get to this person?'" says a Lehman Brothers managing director. Fans say it's reversing a 20-year trend toward employee insulation, with voice-mail systems that make it difficult to tell whether workers are in the office or out on the golf course. Advocates also note that IM has influenced managers to be more receptive to telecommuting arrangements, because it can verify who is really working from home, or at least is logged onto the computer there. And because failing to answer an IM quickly is considered rude, most workers use the "away from my desk" or "busy" sign when they're absent. "There's a sensation you can't hide," says one long-distance manager. IDC estimates that by the end of last year, 20 million people worldwide were using IM in businesses, and it predicts that number will soar to 300 million by the end of 2005. (Wall Street Journal 4 Sep 2002)

Category 23.5 *E-mail & instant messaging or chat*

2002-10-07 **instant messaging corporate monitoring security encryption authentication**

NewsScan

YAHOO TARGETS BUSINESS WITH CORPORATE IM SERVICE
Yahoo is launching a test version of a new instant-messaging service for business users in the next few months in another bid to diversify its revenue stream beyond advertising. When it's formally launched in early 2003, the Yahoo Messenger Enterprise Edition 1.0 will cost $30 per user per year, which includes software upgrades and support. Yahoo plans to differentiate its corporate IM service by adding security, administrative control and integration features, enabling companies to audit incoming and outgoing messages, as well as add encryption and authenticate users. Competitors Microsoft and AOL are believed to be preparing their own corporate messaging services, and analysts say Yahoo must move quickly to build its customer base and retain loyal users who might be tempted to migrate to rival services. (Wall Street Journal 7 Oct 2002)

Category 23.5 *E-mail & instant messaging or chat*

2002-10-21 **spam penetration pop-up Windows operating systems warnings**

NewsScan

POP-UP SPAM — A DIABOLICAL INVENTION
As if e-mail spam weren't annoying enough — now there's pop-up spam. A Romanian-based company has developed software that can blast computers with pop-up messages through the Messenger function on many Windows operating systems that was originally designed to allow computer network technicians to warn network users of a planned shutdown (not to be confused with Instant Messenger). Gary Flynn, a security engineer at James Madison University, deplores this latest technological development: "It's almost like somebody barging into your office and interrupting you." Zoltan Kovacs, founder of the company that makes the software, responds, "If some people use it for bad things, they should take their own responsibility, but it's their own problem." The new spam technique represents the latest attempt by advertisers to bypass the increasingly sophisticated e-mail filters used by ISPs and individuals, and also circumvents state and other laws designed to curb junk e-mail. (AP 20 Oct 2002)
http://apnews.excite.com/article/20021020/D7MPIALG0.htm

Category 23.5 *E-mail & instant messaging or chat*

2002-12-05 **securities industry SEC regulations record-keeping rules fines archives e-mail retention**

NewsScan

FIRMS FINED FOR NOT FOLLOWING E-MAIL RETENTION SCHEDULE
The Securities and Exchange Commission has fined five major brokerage firms (Deutsche Bank, Goldman Sachs, Morgan Stanley, Salomon Smith Barney, and U.S. Bancorp Piper Jaffray) $1.65 million each for failing to keep employee e-mail for the required retention period. The SEC examines such mail to find cases in which brokers have rated stocks positively and given it a "buy" recommendation to the public, while in private correspondence revealed complete contempt for the same stock. The commission says, "The record-keeping rules are a keystone of the surveillance of brokers and dealers by commission staff and the security industry's self-regulatory bodies." (San Jose Mercury News 4 Dec 2002)
http://www.siliconvalley.com/mld/siliconvalley/4661957.htm

Category 23.5 *E-mail & instant messaging or chat*

2003-03-04 **new vulnerablility Sendmail NIPC advisory server root access CERT CC**

NIPC/DHS

March 03, Department of Homeland Security, National Infrastructure Protection Center — NIPC Advisory 03-004: "Remote Sendmail Header Processing Vulnerability".

The Remote Sendmail Header Processing Vulnerability allows local and remote users to gain almost complete control of a vulnerable Sendmail server. Attackers gain the ability to execute privileged commands using super-user (root) access/control. This vulnerability can be exploited through a simple e-mail message containing malicious code. Sendmail is the most commonly used Mail Transfer Agent and processes an estimated 50 to 75 percent of all Internet e-mail traffic. System administrators should be aware that many Sendmail servers are not typically shielded by perimeter defense applications. A successful attacker could install malicious code, run destructive programs and modify or delete files. Additionally, attackers may gain access to other systems thru a compromised Sendmail server, depending on local configurations. Sendmail versions 5.2 up to 8.12.8 are known to be vulnerable at this time. Due to the seriousness of this vulnerability, the NIPC is strongly recommending that system administrators who employ Sendmail take this opportunity to review the security of their Sendmail software and to either upgrade to Sendmail 8.12.8 or apply the appropriate patch for older versions as soon as possible. Patches for the vulnerability are available from Sendmail at
http://www.sendmail.org. Additional information is available from CERT/CC at
http://www.kb.cert.org/vuls/id/398025.

Category 23.5 *E-mail & instant messaging or chat*

2003-04-24 **new vulnerability Microsoft security bulletin Outlook Express e-mail client patch exploit fix**

NIPC/DHS

April 23, Microsoft — Microsoft Security Bulletin MS03-014: Cumulative Patch for Outlook Express .

A vulnerability exists in the MHTML URL Handler that allows any file that can be rendered as text to be opened and rendered as part of a page in Internet Explorer. As a result, it would be possible to construct a URL that referred to a text file that was stored on the local computer and have that file render as HTML. If the text file contained script, that script would execute when the file was accessed. Since the file would reside on the local computer, it would be rendered in the Local Computer Security Zone. Using this method, an attacker could attempt to construct a URL and either host it on a website or send it via email. If the cumulative patch for Internet Explorer MS03-004 has been installed, known means by which an attacker may place a file onto a user's computer will be blocked. Microsoft has assigned a risk rating of "Critical" to this vulnerability and a patch is available at the Microsoft website.

Category 23.5 *E-mail & instant messaging or chat*

2003-05-06 **AOL ICQ America Online Core Security e-mail execute arbitrary code updating hostile flaw**

NIPC/DHS

May 06, CNET News.com — Security group: AOL's ICQ is flawed.

There are six flaws, two of them critical, in America Online's (AOL) ICQ software, security firm Core Security Technologies warned in an advisory Monday. Three of the vulnerabilities, including one of the critical flaws, occurred in the software's e-mail feature. A bug in the component could allow an attacker to use the way the software handles e-mail to cause it to execute code, if the attacker can impersonate the user's e-mail server. The other critical vulnerability appeared in a feature of ICQ that allows automated updating. Because that component doesn't have adequate security, an attacker could pretend to be sending a legitimate update when in reality the upgrade is hostile code. No one from AOL's ICQ subsidiary was available Monday to comment on the alleged flaws. The advisory is available on the Core Security Technologies website: http://www.coresecurity.com/common/showdoc.php?idx=315ccion=10.

Category 23.5 *E-mail & instant messaging or chat*

2003-05-09 **instant messaging software ICQ America Online Inc. Mirabilis IM client holes firewalls elnterprise**

NIPC/DHS

May 09, Computerworld — Security problems persist with instant messaging.

Security problems relating to the unfettered use of consumer chat software on corporate networks are fueling the adoption of tougher security measures and more commercial-grade products, users and analysts said. Ongoing concerns about instant messaging (IM) security were heightened this week by the disclosure of six vulnerabilities in America Online Inc.'s Mirabilis ICQ IM client software. Security analysts for some time have been warning that unchecked use of such software could cause dangerous holes in enterprise firewalls, leading to sensitive corporate data being exposed on public networks and files being transferred in an unprotected fashion.

Category 23.5 *E-mail & instant messaging or chat*

2003-05-30 **Yahoo IM buffer overflow delete files executable code malicious programmer chat updates**

NIPC/DHS

May 30, CNET News.com — Yahoo issues IM, chat security patches.

Yahoo issued on Friday security patches for its Yahoo Instant Messenger and Yahoo Chat clients in an effort to fix a buffer overflow vulnerability discovered in the software. When users of the software log on to the IM network or enter a chat room, Yahoo is prompting them to install the patches. In addition, the company posted the patches on its Web site. Buffer overflow attacks in Yahoo IM and Yahoo Chat could lead to a number of problems. Users could be involuntarily logged out of an application, or it could allow the introduction of executable code, allowing a malicious programmer to take control of a user's machine, delete files and otherwise wreak havoc with a victim's computer system.

Category 23.5 *E-mail & instant messaging or chat*

2003-08-25 **e-mail attachments scanning virus worm policy**

NewsScan

ISPs TO START SCANNING ATTACHMENTS
Several large U.S. Internet service providers, including Cox Communications, EarthLink and BellSouth, say they are preparing to scan all e-mail attachments for computer viruses before they forward them on to subscribers' accounts. The policy change comes on the heels of a month of e-mail problems caused by the Sobig and Blaster worms, resulting in consumer demand for better security measures on ISP servers. "Virus filtering is quickly becoming one of the check marks for the big ISPs," says Todd Dean, director of data operations and support for Cox. However, the cost of filtering e-mail can be daunting, says Forrester Research analyst Michael Rasmussen. "With ISPs of those sizes, you're easily looking at ongoing costs of several million dollars — not just the cost of purchasing the technology, but making it work with your existing systems, administrative costs and increased support costs associated with customers who are confused about what to do when their ISP tells them they have an e-mail with a virus inside." Several leading ISPs already scan mail, including AOL, Microsoft Network, Comcast, Covad and AOL Time Warner's RoadRunner network, forestalling the possibility of unwary subscribers becoming conduits for further viral infection. "Users should not be asked to protect themselves any more than they should be asked to go buy seat belts and airbags and install them in their own cars," says Alan Paller, research director for the SANS Institute, a security training facility. "That's got to come with their service, even if it comes with an added price." (Washington Post 28 Aug 2003)

Category 23.5 *E-mail & instant messaging or chat*

2003-08-27 **sendmail vulnerability DoS denial service open source remote DNS Linux Unix free() fucntion attacks**

NIPC/DHS

August 27, SearchEnterpriseLinux.com — Sendmail vulnerable to DoS attacks.

Versions 8.12.0 through 8.12.8 of the open-source mail transfer agent Sendmail are vulnerable to remote denial-of-service attacks, according to an alert issued by the FreeBSD Project. The vulnerability is in the code that implements DNS (domain name system) maps. An attacker sending a malformed DNS reply packet could cause Sendmail to call "free ()" on an uninitialized pointer. Such a call could cause a Sendmail child process to crash. Sendmail is widely implemented in enterprises as part of several Linux and Unix distributions. A patch is available on the Sendmail Website: http://Sendmail.org/dnsmap1.html

---

Category 23.5 *E-mail & instant messaging or chat*

2003-09-18 **instant mesasge NYSE Wall Street traders IM records Bank of America**

NewsScan

INSTANT MESSAGE: YOU'RE UNDER ARREST
The investigation of a Wall Street trading scandal (in which a former Bank of America broker has been charged with grand larceny and securities fraud) is the first case that has used a chain of evidence derived from the instant messaging records of licensed brokers and dealers. Instant messaging (IM) systems are now widely used on Wall Street and to a large extent have replaced traditional e-mail. One attorney who consults on electronic communications said a New York Stock Exchange executive's question about instant messaging was: "Wait a minute, is that what my 13-year-old daughter uses at home?" The answer: "I said yes — and your traders." (USA Today 18 Sep 2003)

Category 23.5 *E-mail & instant messaging or chat*

2003-09-24 **Micorosoft MSN hat free expensive indentity requirements personal data accountability actions**

NewsScan

MICROSOFT LAUDED FOR CRACKING DOWN ON CHAT ROOMS
Child advocates are applauding a decision by Microsoft's MSN online service to crack down on its free chat rooms. Ernie Allen of the National Center for Missing & Exploited Children says: "There is no question but that chat rooms generally tend to be very dangerous places for children." MSN's move is intended to force users to identify themselves, so that they can be held accountable for their actions, and so that MSN can contact them when it gets complaints. Of course, ending support for free foreign chat rooms will also help Microsoft reduce MSN's financial loss. Technology analyst Rob Helm explains: "Maintaining any kind of online service is expensive. Putting chat on paid status in the U.S, and turning it off elsewhere is a step toward making MSN profitable." However, Microsoft spokesman Lisa Gurry says that cost savings were "not a factor" in the Microsoft chat-room decision. "This really is all about looking at delivering the safest online experience for folks using our services." (USA Today 24 Sep 2003)

Category 23.5 *E-mail & instant messaging or chat*

2003-09-29 **chat ban india separatists internet yahoo groups forums**

NewsScan

CHAT GROUP BAN OF SEPARATIST GROUP AFFECTS ALL OF INDIA
A government ban on the Internet discussion group of a two-dozen member separatist movement has ended up blocking access to popular, unrelated Yahoo forums in nearly all of India. For technical reasons, Indian Internet service providers were unable to block just the separatist group's site and had to shut down every Yahoo discussion group. Businessman Sushil Devaraj says: "This is more like a dictatorship and goes against the concept of freedom of speech." Economics professor Rajeev Gowda of the Indian Institute of Management complains: "My students have a problem. I discuss my subject with them on Yahoo groups. We have not been able to do it. This heavy-handed action has affected a variety of users who have nothing to do with that group." (AP/Los Angeles Times 29 Sep 2003)

Category 23.5 *E-mail & instant messaging or chat*

2003-09-30 **reuters microsoft messaging instant data voice financial services global communication**

NewsScan

REUTERS/MICROSOFT INSTANT MESSAGING DEAL
The Reuters news and information company and Microsoft will combine their two instant messaging systems as an offering for financial services companies. Reuters executive David Gurle says the goal is "to build a global communications infrastructure for the financial services industry. We want to provide the same functionality for which they now use the phone, but with the added element of data." (New York Times 30 Sep 2003)

Category 23.5 *E-mail & instant messaging or chat*

2003-10-25 **Windows Messenger exploit code Service MS03-043 Linux Unix crashes machines**

NIPC/DHS

October 25, TechWeb News — Attackers gearing up to exploit Windows Messenger security hole.

An exploit code that takes advantage of a critical vulnerability in Microsoft's Windows Messenger Service is out in the wild and could prove as dangerous as this summer's MSBlaster worm if attackers decide to focus their efforts, security analysts said Friday, October 24. Released early last week, the exploit code — which has been crafted to run not only on attackers' Windows machines, but also on Linux and Unix boxes — crashes Windows systems not patched against the vulnerability released October 15 in Microsoft Security Bulletin MS03-043. What concerns security analysts is the speed with which this exploit was produced. The span between the disclosure of the vulnerability by Microsoft and proof of exploit code was just three days. Users can disable Windows Messenger Service by following the instructions in Microsoft's security bulletin: http://www.microsoft.com/technet/treeview/?url=/technet/secu rity/bulletin/MS03-043.asp

---

Category 23.5 *E-mail & instant messaging or chat*

2003-11-14 **new vulnerability Eudora buffer overflow e-mail client spam**

NIPC/DHS

November 11, The Register — Eudora users warned over 'reply to all' trick.

A buffer overflow vulnerability in Eudora version 5.x, the popular email client, creates a mechanism for hackers to compromise targeted PCs. The problem stems from a failure to properly verify the "
From:" and "Reply-To:" when users of vulnerable versions of Eudora select "Reply-To-All". This shortcoming creates a means for hackers to spam users with a maliciously constructed email designed to trigger this buffer overflow condition. Users should update to Eudora 5.1-Jr3 (Japanese) or Eudora 6.0 (English) in order to shore up their security defenses: http://www.eudora.com/

Category 23.5 *E-mail & instant messaging or chat*

2003-11-19 **e-mail server flaw exploit spam relay Microsoft Exchange**

NIPC/DHS

November 14, CNET News.com — Mail server flaw opens Exchange to spam.

Administrators of e-mail systems based on Microsoft's Exchange might have spammers using their servers to send unsolicited bulk e-mail, a consultant warned this week. Aaron Greenspan, a Harvard University junior published a white paper Thursday, November 13, detailing the problem. Greenspan's research concluded that Exchange 5.5 and 2000 can be used by spammers to send anonymous e-mail. He says even though software Microsoft provides on its site certifies that the server is secure, it's not. "If the guest account is enabled (on Exchange 5.5 and 2000), even if your login fails, you can send mail, because the guest account is there as a catchall," he said. "Even if you think you've done everything (to secure the server), you are still open to spammers." The guest account is a way for administrators to let visitors use a mail server anonymously, but because of security issues, the feature is generally not enabled. Exchange servers that had been infected by the Code Red worm and subsequently cleaned will still have the guest account enabled, Greenspan said.

Category 23.5 *E-mail & instant messaging or chat*

2003-11-25 **flaw vulnerability Microsoft Exchange Server 2003 kerberos authentication**

NIPC/DHS

November 24, ZDNet UK — Exchange flaw could open up user accounts.

Microsoft is investigating what may be a serious flaw in Exchange Server 2003, only a month after the software's launch as part of Office System 2003. The bug appears to affect an Exchange component called Outlook Web Access (OWA), which allows users to access their in-boxes and folders via a Web browser. Consumers logging into their Web-based mailbox sometimes find themselves accessing another user's account, with full privileges, according to Matthew Johnson, a network administrator who reported the bug earlier this month on the NTBugtraq security mailing list. Microsoft has said it is investigating the issue and that the flaw appears to occur only when Kerberos authentication is disabled. Kerberos is the method that Microsoft uses for authenticating requests for services. For the moment, the company is advising customers to keep Kerberos authentication enabled, as it is by default, and may issue a patch or more information when its investigation is complete.

Category 23.5 *E-mail & instant messaging or chat*

2003-12-10 **Yahoo instant messaging flaw vulnerability executable code**

NIPC/DHS

December 08, CNET News.com — Yahoo answers IM security flaw.

Yahoo has issued an update to its instant-messaging software, in order to address a security flaw found in the application. The company said the security issue was related to a buffer overflow, which is a common security vulnerability in computer programs written in C and C++ that allows more information to be added to a chunk of memory than it was designed to hold. Typical problems involved in an instant-messaging-related buffer overflow might include an involuntarily log-out of an IM session, a crash of browsing software applications, and a possible introduction of executable code. According to Yahoo, only a small percentage of the company's IM software users might be vulnerable as a result of the flaw. Yahoo said customers who changed their Explorer security settings from "medium" to "low" could be affected. The company said that even in that case, an attacker would have to lure a user of Yahoo IM to view malicious HTML code. Most often this would entail clicking a link sent through IM that leads back to a Web page hosting the code. Before changing an IE security setting to low, individuals are warned by the browser that the setting is considered "highly unsafe." Yahoo said it has not yet heard of any successful attacks based on the buffer flaw. The update is available on the Yahoo Website:
http://messenger.yahoo.com/messenger/security/

Category 23.5 *E-mail & instant messaging or chat*

2004-01-14 **Microsoft security bulletin patch flaw vulnerability fix Exchange Server**

NIPC/DHS;
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS04−002.asp

January 13, Microsoft — Microsoft Security Bulletin MS04-002: Vulnerability in Exchange Server 2003 Could Lead to Privilege Escalation.

A vulnerability exists in the way that Hypertext Transfer Protocol (HTTP) connections are reused when NTLM authentication is used between front-end Exchange 2003 servers providing Outlook Web Access (OWA) and, OWA on Windows 2000 and Windows Server 2003, and when using back-end Exchange 2003 servers that are running Windows Server 2003. Users who access their mailboxes through an Exchange 2003 front-end server and OWA might get connected to another user's mailbox if that other mailbox is (1) hosted on the same back-end mailbox server and (2) if that mailbox has been recently accessed by its owner. Attackers seeking to exploit this vulnerability could not predict which mailbox they might become connected to. The vulnerability causes random and unreliable access to mailboxes and is specifically limited to mailboxes that have recently been accessed through OWA. This vulnerability is exposed if the Website that is running the Exchange Server 2003 programs on the Exchange back-end server has been configured not to negotiate Kerberos authentication, causing OWA to fall back to using NTLM authentication. The only known way that this vulnerability can be exposed is by a change in the default configuration of Internet Information Services 6.0 on the Exchange back-end server. Microsoft has assigned a severity rating of "Moderate" to this issue.

Category 23.5 *E-mail & instant messaging or chat*

2004-01-28 **virus scanners attachment creation update macros conspiracy theory**

RISKS 23 15ff

RISKS OF VIRUS SCANNERS AND MACRO-ENABLED DOCUMENTS

Steve Bellovin writes about his experience upgrading AV software. This AV software product dealt with an e-mail with a viral attachment "in an appropriate permanent fashion." However, Bellovin says, the AV software notified the user of its disinfection with a text file attachment to the previously-infected e-mail. Bellovin thinks it won't be long before a virus mimics this AV software's action, to fool a user into opening a "notification" file. He asks, "Why are the good guys trying to teach people to click on attachments?" In a follow-up article, contributor Paul Tomblin answers this question--Tomblin thinks anti-virus companies need people to click on attachments and get infected in order stay in business. In another follow-up article, Alan J Rosenthal argues that "opening "attachments" is a fact of ms-win life." He says that users have become used to sending each other plain text messages as Word document attachments--which may often be infected--and transmitting malicious code through Word macros. Rosenthal thinks this problem could be solved if Microsoft created an Office suite without macros. This way, he says, users won't be able to transmit malicious code so easily, and "everyone else will be impressed by Microsoft's technical mastery…"

Category 23.5 *E-mail & instant messaging or chat*

2004-03-10 **Microsoft security bulletin vulnerability hole flaw patch fix MSN Messenger privacy**

DHS IAIP Daily; http://www.microsoft.com/technet/security/bulletin/ms04-010.mspx

March 09, Microsoft — Microsoft Security Bulletin MS04-010:

Vulnerability in MSN Messenger Could Allow Information Disclosure. A security vulnerability exists in Microsoft MSN Messenger. The vulnerability exists because of the method used by MSN Messenger to handle a file request. An attacker could exploit this vulnerability by sending a specially crafted request to a user running MSN Messenger. If exploited successfully, the attacker could view the contents of a file on the hard drive without the user's knowledge as long as the attacker knew the location of the file and the user had read access to the file. To exploit this vulnerability, an attacker would have to know the sign-on name of the MSN Messenger user in order to send the request. Microsoft has assigned a risk rating of "Moderate" to this issue and recommends that system administrators consider installing the security update.

Category 23.5 *E-mail & instant messaging or chat*

2004-03-10 **Microsoft security bulletin vulnerability hole flaw patch fix Outlook HTML e-mail**

DHS IAIP Daily; http://www.microsoft.com/technet/security/bulletin/ms04−009. mspx

March 09, Microsoft — Microsoft Security Bulletin MS04-009: Vulnerability in Microsoft Outlook Could Allow Code Execution.

A vulnerability in Outlook 2002 caused by the parsing of specially crafted mailto URLs exists could allow Internet Explorer to execute script code in the Local Machine zone on an affected system. To exploit this vulnerability, an attacker would have to host a malicious Website that contained a Web page designed to exploit the vulnerability and then persuade a user to view the Web page. The attacker could also create an HTML e-mail message designed to exploit the vulnerability and persuade the user to view the HTML e-mail message. After the user has visited the malicious Website or viewed the malicious HTML e-mail message an attacker who successfully exploited this vulnerability could access files on a user's system or run arbitrary code on a user's system. This code would run in the security context of the currently logged-on user. Microsoft has assigned a risk rating of "Important" to this issue and recommends that system administrators install the patch immediately.

Category 23.5 *E-mail & instant messaging or chat*

2004-03-12 **Microsoft security vulnerability hole flaw patch fix Outlook e-mail**

DHS IAIP Daily;
http://www.computerworld.com/securitytopics/security/story/0,10801,90992,00.html

March 10, IDG News Service — Microsoft upgrades fix for Outlook from 'important' to 'critical'.

One day after releasing a trio of security patches, Microsoft is upgrading the seriousness of one of those fixes to from "important" to "critical." The update released in security bulletin MS04-009 fixes a problem with the way the Outlook e-mail software treats URLs that use the "mailto" tag, which allows Website authors to insert links on Web pages that launch Outlook or other e-mail clients. A problem with the way Outlook interprets mailto URLs could allow an attacker to use a specially formatted mailto URL to gain access to files on an affected system or insert and run malicious computer code. Microsoft initially claimed that only computers with the Outlook Today home page were vulnerable to attack. Outlook Today is the home page only until an e-mail account is created, Microsoft said. However, following release of the bulletin, Finnish security researcher Jouko Pynnonen, who discovered the vulnerability, informed the company that malicious hackers could attack vulnerable Outlook installations even if Outlook Today isn't the default home page, the company said. In a revised version of its security bulletin, Microsoft noted the discrepancy. Additional information is available on the Microsoft Website: http://www.microsoft.com/technet/security/bulletin/offmar04. mspx

---

Category 23.5 *E-mail & instant messaging or chat*

2004-03-24 **security vulnerability flaw hole patch fix Web-based electronic e-mail service Hotmail Yahoo**

DHS IAIP Daily; http://www.esecurityplanet.com/trends/article.php/3329821

March 23, eSecurity Planet — Hotmail, Yahoo users at risk of PC takeover.

A potentially serious security flaw found in Web-based e-mail services offered by Microsoft and Yahoo could put millions of PCs at risk of takeover, an Internet security consultant GreyMagic warned Tuesday, March 23. The advisory warned that attackers could inject malicious code by simply sending an e-mail to an unsuspecting Hotmail or Yahoo user. The vulnerability only affects Hotmail and Yahoo running on Microsoft's Internet Explorer (IE) browser. Successful exploit could lead to theft of a user's login and password, disclosure of the content of any e-mail in the mailbox and disclosure of all contacts within the address book. Additionally, the attacker could manipulate the system to automatically send e-mails from the mailbox and to exploit vulnerabilities in IE to access the user's file system and eventually take over his or her machine. Microsoft has fixed the vulnerability and Hotmail is no longer vulnerable.

Category 23.5 *E-mail & instant messaging or chat*

2004-03-26 **intant messenging IM threat CERT CC social engineering spam virus back door**

NIPC/DHS

March 25, New York Times — When instant messages come bearing malice.

Perpetrators are using Instant Messenging (IM) to deliver spam , unleash viruses, and create back doors into the systems of unsuspecting users. The CERT Coordination Center says IM users are especially susceptible to "social engineering," meaning attacks that prey on human foibles by enticing people with promises of free products, pornography and interesting-sounding links. When two people communicate through instant messaging, the messages are relayed as plain text through an IM service's central servers before they reach the recipient. An unscrupulous systems administrator could easily train a program to search for words, passwords or combinations of numbers to harvest critical personal information. The lack of privacy is compounded when IM messages travel over public wireless networks like those at cafes, airports and hotels where security levels are kept low to give users easy access to the network. IM users can transfer files to each other and give others access to their shared-files folder. These folders sometimes contain family photographs and documents with names, addresses and telltale financial information, "all the little pieces of information that actually might help someone assume a person's identity," said Fred Felman of Zone Labs.

Category 23.5 *E-mail & instant messaging or chat*

2004-04-13 **Micrsoft security bulletin update Windows critical Outlook e-mail client**

DHS IAIP Daily; http://www.microsoft.com/technet/security/bulletin/ms04−
013. mspx

April 13, Microsoft — Microsoft Security Bulletin MS04-013 Cumulative Security Update for Outlook Express.

This is a cumulative update that includes the functionality of all the previously-released updates for Outlook Express 5.5 and Outlook Express 6. Additionally, it eliminates a new vulnerability that could allow an attacker who successfully exploited this vulnerability to access files and to take complete control of the affected system. This could occur even if Outlook Express is not used as the default e-mail reader on the system. Microsoft has assigned a risk rating of "Critical" to this issue and recommends that customers install this update immediately.

Category 23.5 *E-mail & instant messaging or chat*

2004-04-27 **new e-mail attack denial-of-service servers NDN flooding spoofed addresses**

DHS IAIP Daily; http://searchsecurity.techtarget.com/originalContent/0,28914
2,sid14_gci961512,00.html

April 27, SearchSecurity.com — E-mail attack could swamp e-mail servers.

Several researchers have identified a new e-mail attack that can be used to swamp enterprise e-mail servers, as well as some secondary systems. Experiments revealed that nearly 60% of general and 30% of Fortune 500 systems and domains could be leveraged for an attack. Security consultant Stefan Frei, who operates a Swiss e-mail portal, discovered a way that malicious users could swamp e-mail servers and accounts. In early April he reported it in a paper coauthored with software architect Ivo Silvestri and professional services director Gunter Ollmann. In the report, the trio explained how an attack could happen, beginning with a spoofed e-mail originator at the target. A message is sent to multiple invalid recipients. The system sends NDNs flooding back to the spoofed address. The assault can be further multiplied by adding an attachment to the initial message. The researchers recommend mail server changes to lessen the problem--such as not accepting mail for invalid recipients, limiting the maximum number of recipients, generating few and small error messages and validating input data. All of these fixes don't help a target ward off an attack. As Ollmann pointed out, about the only option is to block systems at the ISP level by, perhaps, blacklisting offending mail servers.

Category 23.5 *E-mail & instant messaging or chat*

2004-05-07 **buffer overflow vulnerability Eudora e-mail email**

DHS IAIP Daily; http://www.esecurityplanet.com/prevention/article.php/335117
1

May 07, eSecurity Planet — 'Critical' buffer overflow found in Eudora.

Security researchers have discovered a "highly critical" security flaw in QUALCOMM's Eudora e-mail client that could lead to the execution of malicious code on vulnerable systems. Paul Szabo, a computer systems officer at the University of Sydney, reported the flaws in versions 6.1, 6.0.3 and 5.2.1 of Eudora and warned that Windows users were at risk of complete system takeover. According to Szabo's advisory, the vulnerability is due to a boundary error within the URL-handling functionality. A malicious hacker could exploit the hole with an e-mail containing a specially crafted link. Research firm Secunia has tagged a "highly critical" rating on the flaw and recommends that Eudora users be wary of other serious vulnerabilities in the mail client.

Category 23.5 *E-mail & instant messaging or chat*

2004-05-18 **vulnerability Microsoft Outlook e-mail client illegal actions update issued**

DHS IAIP Daily; http://news.earthweb.com/ent−news/article.php/3355411

May 18, earthwebnews.com — Outlook 2003 bypass flaw reported.

Security researchers have discovered a vulnerability in the Microsoft Outlook 2003 software that could allow malicious hackers to perform illegal actions through e-mails. According to an alert from Secunia, the flaw could let attackers sneak past the security settings in the Outlook 2003 e-mail program and attempt to load harmful code to vulnerable PCs. Outlook 2003 is designed to protect the user by opening mails in a restricted security zone to prevent the use of active scripting or download of harmful files. This can be exploited to start a download sequence of arbitrary files, which in turn causes Internet Explorer to prompt the user whether to download the file," according to the alert, which carries a "moderately critical" rating. Combined with another flaw that deals with "Predictable File Location Weakness," Secunia said it was possible to launch the malicious file without any warning. Affected software include Outlook 2003, Office 2003 Student and Teacher Edition, Office 2003 Standard Edition, Office 2003 Small Business Edition and Office 2003 Professional Edition. The company recommends that users filter HTML and Rich Text Format messages until a fix is issued by the software giant. Alert found at http://secunia.com/advisories/11629/

Category 23.5 *E-mail & instant messaging or chat*

2004-06-03 **e-mail makeover instant messaging IM RSS features**

NewsScan

E-MAIL NEEDS A MAKEOVER

Forget about spam -- even your "wanted" e-mail is clogging your in-box now, right? E-mail is "broken," says Eric Hahn, former CTO of Netscape and current CEO of antispam firm Proofpoint. "We need to make metaphoric changes. The [file-folder] metaphor was designed back when we were talking about getting five messages a day." Today, many folks receive 10 to 20 times that number and filing each one just takes too much time. "People hate filing. They hate it in paper. They hate it in e-mail. Could you imagine what it would be like to have to file Web pages just to get back to them?" Hahn suggests that in addition to overhauling the filing function, software developers should find a way to combine instant-messaging software with e-mail software. "Doesn't it seem odd that IM is separate from e-mail? Why are those conversations so fundamentally different?" he asks. Ben Gross, a researcher at the University of Illinois-Urbana-Champaign, says that in addition to incorporating IM, e-mail software developers need to integrate RSS readers into their products, so that users can view updates to a Web page without having to download the whole Web page into a browser. Some e-mail software developers are already experimenting with new approaches: Microsoft's Outlook 2003 and Google's Gmail service include a "group by conversation" feature that enables users to view related e-mails sent to and from a single person.
(Wired.com 3 Jun 2004)

Category 23.5 *E-mail & instant messaging or chat*

2004-06-14 **e-mail security threat early warning Internet traffic virus worm**

NewsScan

E-MAIL SECURITY FIRMS FOCUS ON EARLY WARNING

E-mail security companies are using a new technique to monitor Internet traffic that will allow them to identify virus outbreaks earlier and take a more proactive role in preventing hacker damage. The technology surveys traffic across a large number of organizations and searches for anomalies that might indicate malicious code activity. It then takes immediate action to slow down or block delivery, providing a head-start over conventional methods that analyze viruses and then rely on antivirus firms to identify and stop them. "We've seen we can gain four or five hours on the virus," says Scott Weiss, CEO of IronPort, which uses the early-warning technology. "Four to five hours is life for the network administrator." Suspicious traffic patterns that might signal viral outbreak include an increased volume in messages from specific senders and messages with similar subject lines or containing a particular type of attachment file. The computers can then tip off e-mail software to destroy or quarantine the suspect messages. "It's the start of a big trend," predicts Matt Cain, an analyst with Meta Group. (Wall Street Journal 14 Jun 2004)

Category 23.5 *E-mail & instant messaging or chat*

2004-06-28 **Verisign e-mail security service blacklists identification authentication I&A**

NewsScan

VERISIGN TACKLES E-MAIL SECURITY

VeriSign has unveiled a new e-mail protection service that uses custom blacklists, fingerprinting and heuristic tools to calculate the probability that a particular message is spam by examining a pattern of characteristics in the message. The company has begun free trials of the service, and VeriSign says it plans to add more features, including sender ID verification and domain authentication. "The introduction of this service will help enterprises restore the productivity gains from e-mail communication that are now under threat from spam and viruses," says VeriSign executive VP Judy Lin. (CNet News.com 28 Jun 2004)

Category 23.5 *E-mail & instant messaging or chat*

2004-07-14 **e-mail privacy management policy Electronic Frontier Foundation EFF complaint**

NewsScan

E-MAIL PRIVACY: DON'T COUNT ON IT

A recent federal appeals court ruling giving e-mail less protection than other types of communication has inspired privacy advocates to reemphasize the need for caution in the use and management of e-mail. Kevin Bankston of the Electronic Frontier Foundation warns: "Under this decision, any node on the Internet that passes e-mails could flip a switch and start looking at any e-mail that passed through it," and Marc Rotenberg of the Electronic Privacy Information Center says that until Congress or the courts change the law "the best practice is not to put into e-mail something that you are concerned might be disclosed to a third party." And privacy expert J.J. Luna gives this piece of good advice: "Never sell a computer with a hard drive to anyone, for any reason." (Wall Street Journal 14 Jul 2004)

Category 23.5 *E-mail & instant messaging or chat*

2004-08-09 **AOL Instant Messenger IM critical vulnerability buffer overflow attack**

DHS IAIP Daily; http://searchsecurity.techtarget.com/originalContent/0,28914
2,sid14_gci999090,00.html

August 09, SearchSecurity.com — 'Highly critical' flaw in AOL Instant Messenger.

AOL Instant Messenger (AIM) has a vulnerability attackers could use to compromise computers and launch arbitrary code, IT security firm Secunia said Monday, August 9. AIM 5.x contains a boundary error within the handling of "Away" messages that can be exploited to cause a stack-based buffer overflow. "A malicious Website can exploit this via the AIM URI handler by passing an overly long argument to the 'goaway?message' parameter," the advisory said. "Successful exploitation may allow execution of arbitrary code on a user's system when...a malicious Website is visited with certain browsers." Secunia said the vulnerability has been confirmed in version 5.5.3595 and that other versions may also be affected. The firm also noted that "various other issues were also reported, where a large amount of resources can be consumed on a user's system." The advisory said the vendor was contacted but has not responded, and recommends users switch to an alternative product.

Category 23.5 *E-mail & instant messaging or chat*

2004-08-13 **Yahoo Messenger Portable Network Graphics PNG libpng vulnerability plug**

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1635855,00.asp

August 13, eWEEK — Yahoo plugs PNG security hole.

Yahoo Inc. has posted a security update for its Windows version of Yahoo Messenger to fix a series of vulnerabilities in the PNG (portable network graphics) library, or libpng. The library provides a set of graphics routines for PNG files; PNG is an alternative graphics format to GIF. The PNG library holes, as previously reported, could allow an attacker to crash programs or execute attack code. Yahoo released the fix for users of Yahoo Messenger 6.0 for Windows because it uses the open-source PNG format in limited areas of its IM client to display images, said Yahoo spokesperson Terrell Karlsten. According to a security note on the Yahoo Messenger Website, there have been no known exploits of the vulnerabilities. Yahoo learned of the PNG library vulnerabilities from a U.S. Computer Emergency Readiness Team security bulletin issued last week. Additional information is available on the Yahoo Website: http://messenger.yahoo.com/security/update5.html

---

Category 23.5 *E-mail & instant messaging or chat*

2004-08-19 **Mutt e-mail client PGP GnuPG vulnerability spoof messages social engineering attacks**

DHS IAIP Daily; http://www.securityfocus.com/bid/10929

August 19, SecurityFocus — Mutt PGP/GnuPG verified e-mail signature spoofing vulnerability.

Mutt PGP/GnuPG versions 1.3.28 and 1.5.6 contain a vulnerability that allows malicious users to send e-mail that spoofs a successfully verified PGP/GnuPG e-mail message. If a user employs Mutt with a specific configuration, this vulnerability could allow a malicious user to spoof e-mail from trusted sources. This will likely increase the effectiveness of social engineering attacks. Altering the configuration of Mutt to use colors may assist in determining if e-mail messages are spoofed.

Category 23.5 *E-mail & instant messaging or chat*

2004-08-28 **Gaim instant messaging client software vulnerabilities**

DHS IAIP Daily; http://www.zone−h.org/advisories/read/id=5443

August 28, Zone-H.org — New Gaim vulnerabilities reported.

Gaim contains several security issues that might allow an attacker to execute arbitrary code or commands. Gaim fails to do proper bounds checking under various circumstances. These vulnerabilites could allow an attacker to crash Gaim or execute arbitrary code or commands with the permissions of the user running Gaim. Upgrade to the latest edition of Gaim: http://gaim.sourceforge.net/downloads.php

---

Category 23.5 *E-mail & instant messaging or chat*

2004-09-08 **Trillian instant messaging IM client MSN module buffer overflow vulnerability no update issued**

DHS IAIP Daily; http://secunia.com/advisories/12487/

September 08, Secunia — Trillian MSN module buffer overflow vulnerability.

A vulnerability exists in Trillian 0.74i, which can be exploited by malicious people to execute arbitrary code on a compromised system. Trillian is a chat client currently supporting IRC, AIM, ICQ, MSN Messenger, and Yahoo! Messenger. There is no solution available at this time.

Category 23.5 *E-mail & instant messaging or chat*

2004-09-29 **instant messaging IM worm JPEG flaw**

DHS IAIP Daily; http://security.itworld.com/4340/040929imworm/page_1.html

September 29, IDG News Service — Instant messaging worm exploits JPEG flaw.

Security experts have spotted the first attempts to create an Internet worm that propagates using instant messages. Researchers at The SANS Institute's Internet Storm Center (ISC) have had two reports of users receiving messages on America Online Inc.'s Instant Messenger service that lured them to Websites containing malicious code, said Johannes Ullrich, chief technology officer at ISC, on Wednesday, September 29. The malicious code attempts to install "backdoor" software on the user's PC that gives remote attackers control over the machine and the victim's instant messenger contacts list, Ullrich said.

Category 23.5 *E-mail & instant messaging or chat*

2004-11-16 **Imail IMAP service buffer overflow vulnerability code execution attack**

DHS IAIP Daily; http://secunia.com/advisories/13200/

November 16, Secunia — Imail IMAP service delete command buffer overflow vulnerability.

A vulnerability has been reported in IMail Server, which can be exploited by malicious users to compromise a vulnerable system. The vulnerability can be exploited to cause a stack-based buffer overflow by passing a "DELETE" command with an overly long argument (about 300 bytes). Successful exploitation allows execution of arbitrary code. No vendor solution is available.

Category 23.5 *E-mail & instant messaging or chat*

2004-11-20 **Google Gmail zx variable remote user cross site scripting attack vulnerability**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Nov/1012289.html

November 20, SecurityTracker — Gmail 'zx' variable input validation bug lets remote users conduct cross-site scripting attacks.

A remote user can access the target user's cookies (including authentication cookies), if any, associated with the Gmail site, access data recently submitted by the target user via Web form to the site, or take actions on the site acting as the target user. It is reported that the zx variable is not properly validated. A remote user can create a specially crafted URL that, when loaded by a target user, will cause arbitrary scripting code to be executed by the target user's browser. From SecurityTracker's testing, it appears that this flaw has been corrected, but that was not confirmed in the report.

Category 23.5 *E-mail & instant messaging or chat*

2004-11-29 **instant messaging IM logging storage retrieval archiving**

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/10293868.htm

SMARTER IM-ING

Now there's a new service called IM Smarter that stores copies of conversations for later retrieval, a feature that could become quite handy as instant messaging makes inroads into the corporate world. Inventor David Weekly characterizes IM Smarter as an electronic "secretary" that takes notes and alerts you to important events. "The logging will appeal to people who passed notes in school and would keep them in a shoe box. And there are people who use IM for business purposes and want to keep those conversations." IM Smarter's storage capabilities lend fuel to an emerging debate over how ephemeral instant message conversations should be. Many IM-ers assume their conversations disappear when they (and their correspondents) log off. The IM Smarter service is currently free, but Weekly hopes to add advertising to support it, and eventually launch an ad-free premium service that allows users to set up IM alerts for tracking changes to Web sites or eBay auctions. (San Jose Mercury News 29 Nov 2004)

Category 23.5 *E-mail & instant messaging or chat*

2004-12-08 **Internet security instant messaging IM peer-to-peer virus worm threat tracking**

DHS IAIP Daily; http://www.computerweekly.com/articles/article.asp?liArticle ID=135694&liArticleTypeID=1&liCategoryID=6&liChannelID=22&li FlavourID=1&sSearch=&nPage=1

December 08, ComputerWeekly — Group formed to track IM threats.

A group of Internet security and instant messaging (IM) providers have teamed up to detect and thwart the growing threat of IM and P2P (peer-to-peer) viruses and worms. The consortium, led by corporate IM software suppliers, is setting up a threat center to analyze and warn against the vulnerabilities. It is offering free alerts and e-mail notifications of risk assessments and threat management for subscribers. The group's formation follows evidence that security threats against IM and P2P networks are growing. The group includes Imlogic, McAfee, Sybari Software, Yahoo, America Online and Microsoft. The effort is being co-ordinated at the IMlogic Threat Center at http://www.imlogic.com/im_threat_center/index.asp

---

Category 23.5 *E-mail & instant messaging or chat*

2005-01-13 **Google mail Gmail flaw accident hack Unix community source code boundaries no update issued**

DHS IAIP Daily; http://www.vnunet.com/news/1160489

ACCIDENTAL HACK REVEALS GMAIL FLAW

A Unix community group has reported a flaw in Google's free Gmail email service which it warns could compromise user information. Two members of HBX Networks, going by the monikers 'Hairball' and 'MrYowler,' were testing a Perl script that would send out a newsletter. When they tried to reply to the test email the page displayed HTML code which included the names and passwords of other users. The problem appears to come from poorly defined code boundaries on Google's mail server. The community group members do not propose a workaround beyond informing Google of the problem.

Category 23.5 *E-mail & instant messaging or chat*

2005-02-03 **Eudora e-mail client vulnerability system compromise code execution attack**

DHS IAIP Daily; http://secunia.com/advisories/14104/

EUDORA SYSTEM COMPROMISE VULNERABILITIES

A vulnerability was reported in Eudora, which can be exploited by malicious people to compromise a user's system. The vulnerabilities are caused due to unspecified errors within the viewing of e-mails and handling of stationary and mailbox files. Successful exploitation allows execution of arbitrary code with the privileges of the user running Eudora. Update to version 6.2.1: http://www.eudora.com/products/

Category 23.5 *E-mail & instant messaging or chat*

2005-02-14 **Open webmail input validation flaw vulnerability cross site scripting code execution attack**

DHS IAIP Daily; http://securitytracker.com/alerts/2005/Feb/1013172.html

OPEN WEBMAIL INPUT VALIDATION FLAW IN 'LOGINDOMAIN' LETS REMOTE USERS CONDUCT CROSS-SITE SCRIPTING ATTACKS

A vulnerability was reported in Open WebMail. A remote user can conduct cross-site scripting attacks. The software does not properly validate user-supplied input in the 'logindomain' parameter. A remote user can create a specially crafted URL that, when loaded by a target user, will cause arbitrary scripting code to be executed by the target user's browser. Upgrade to 2.50 after 20050212 or apply patch available at: http://openwebmail.org/openwebmail/download/cert/patches/SA- 05:01/

Category 23.5 *E-mail & instant messaging or chat*

2005-02-18 **instant messaging IM Yahoo Messenger remote user spoof filename vulnerability file transfer code execution attack update issued**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2005/Feb/1013237.html

YAHOO! MESSENGER LETS REMOTE USERS SPOOF FILENAMES DURING FILE TRANSFER

A vulnerability was reported in Yahoo! Messenger in the file transfer feature. A remote user may be able to cause a target user to execute arbitrary code. Yahoo! Messenger does not properly display files with long filenames in the file transfer dialog windows. A remote user can send a specially crafted, long filename containing whitespace and two file extensions to spoof the filename. Update to version 6.0.0.1921, available at: http://messenger.yahoo.com/

Category 23.5 *E-mail & instant messaging or chat*

2005-03-02 **Trillian instant messaging chat software PNG buffer overflow vulnerability system compromise no update issued**

DHS IAIP Daily; http://www.k−otik.com/english/advisories/2005/0221

TRILLIAN PNG IMAGE FILE PROCESSING BUFFER OVERFLOW VULNERABILITY

A critical vulnerability was reported in Trillian, which may be exploited by attackers to execute arbitrary commands. The problem occurs when processing specially crafted PNG image files and could be exploited by a attackers to compromise a vulnerable system. There is no solution at this time.

Category 23.5 *E-mail & instant messaging or chat*

2005-03-10 **secure instant messaging IM companies businesses meet privacy concern unauthorized use detection**

DHS IAIP Daily;
http://www.computerworld.com/softwaretopics/software/groupwa
re/story/0,10801,100298,00.html

COMPANIES TURN TO SECURE INSTANT MESSAGING TO MEET PRIVACY CONCERNS

With the use of instant messaging (IM) on an upswing, companies concerned about security, regulatory and privacy issues are sometimes turning to secure IM solutions that allow only authorized users access to IM – while stopping others from sending instant messages. Available software provides businesses with control and administration of all IM activity by their workers, including dynamic detection and routing of IM use on the network, and prevention of unauthorized IM usage. Lawrence Orans, an analyst at Gartner Inc., said IM technology tools can now increase security because they allow businesses to set policies on permitted IM usage. While some companies do little to monitor their employees' IM use, the potential for viruses and network attacks will make it more important that they pay attention to potential problems, he said. "It will increasingly become risky to look the other way," Orans said. Another analyst, Robert Mahowald at IDC Inc., warned that there are still pitfalls to instant messaging, even with the use of secure applications. "You've significantly increased your chances of blocking [viruses and other problems] by having a secure IM solution in place," Mahowald said. "But it doesn't completely solve the problem."

Category 23.5 *E-mail & instant messaging or chat*

2005-03-16 **PHPOpenChat file inclusion vulnerability system compromise no update issued**

DHS IAIP Daily; http://secunia.com/advisories/14600/

PHPOPENCHAT "SOURCEDIR" FILE INCLUSION VULNERABILITY

A vulnerability in PHPOpenChat was reported, which can be exploited by malicious people to compromise a vulnerable system. Input passed to the "sourcedir" parameter in "contrib/yabbse/poc.php" is not properly verified, before it is used to include files. This can be exploited to include arbitrary files from external and local resources. Successful exploitation requires that "register_globals" is enabled. There is no solution at this time.

Category 23.5 *E-mail & instant messaging or chat*

2005-03-22 **instant messaging IM threat hacker spread malicious code research**

DHS IAIP Daily; http://www.vnunet.com/news/1162084

HACKERS INCREASINGLY SPREADING MALICIOUS CODE VIA INSTANT MESSAGING.

Attacks using instant messaging (IM) as an unprotected backdoor in enterprises are reaching epidemic proportions, industry experts have warned. Analyst firm IDC Research said that the problem is leading to a sharp hike in highly sophisticated IM attacks that spread malicious code and worms directly into organizations without any end-user intervention. "Hackers and virus writers have realized that the next vulnerable area for attack within an organization is to spread malicious code via IM," said Brian Burke, research manager for security products at IDC. Hackers are increasingly using IM as a vector for phishing scams and for so-called 'pharming' attacks, malicious redirects where thousands of IM users are persuaded to click on a link to a bogus, malware-infected Website. According to security firm Websense, incidents involving hackers using IM soared by 300 percent during the first quarter of 2005, compared with the fourth quarter of 2004. "Social engineering and vulnerabilities within IM client technologies are being used to gain access to hosts," said Dan Hubbard, senior director of security and technology research at Websense.

Category 23.5 *E-mail & instant messaging or chat*

2005-03-29 **Smail-3 mail from buffer overflow signal handling vulnerabilities design errors code execution attack no update issued**

DHS IAIP Daily; http://secunia.com/advisories/14733/

SMAIL-3 "MAIL FROM" BUFFER OVERFLOW AND SIGNAL HANDLING VULNERABILITIES.

Some vulnerabilities in Smail-3, which potentially can be exploited by malicious, local users to gain escalated privileges and by malicious people to compromise a vulnerable system. A boundary error within the SMTP server when handling email addresses can be exploited to cause a heap-based buffer overflow by passing an overly long string to the "MAIL FROM" command. Some design errors exist within the signal handling code. This may potentially be exploited by malicious, local users to execute arbitrary code with escalated privileges. There is no solution at this time.

Category 23.5 *E-mail & instant messaging or chat*

2005-04-05 **instant messaging IM chat security threat rise IMLogic industry consortium virus worm spam phishing attacks**

DHS IAIP Daily;
http://news.com.com/IM+threats+rise+sharply%2C+report+confir ms/2100−7349_3−5655267.html

INSTANT MESSAGING THREATS RISING SHARPLY, REPORTS CONFIRM

According to a report issued Tuesday, April 5, by the IMlogic Threat Center – an industry consortium led by security software maker IMlogic – the quantity of instant messaging (IM) threats increased 250 percent in the first quarter of 2005, compared with the same period last year. The research, which tracks viruses, worms, spam and phishing attacks sent over public IM networks, also contends that reported incidents of newly discovered IM threats have grown by 271 percent this year. In addition, the study found that more than 50 percent of the incidents reported to the Threat Center during the first quarter of 2005 involved attacks at workplaces where freely available IM software such as AOL Instant Messenger, MSN Messenger, Windows Messenger, and Yahoo Messenger is used. Based on that data, the consortium advises that companies take a closer look at managing IM security issues. Report: http://imlogic.com/news/press_107.asp

---

Category 23.5 *E-mail & instant messaging or chat*

2005-04-19 **virus writing focus e-mail instant messaging IM shift automatic spread MSN Messenger Visual Basic VB programming language**

DHS IAIP Daily; http://www.vnunet.com/news/1162557

REPORT SAYS VIRUS WRITERS TURNING FROM E-MAIL TO IM

Email worms are falling out of favor with the hacking community, according to a report investigating malicious Internet activity. Instead malware authors are increasingly subverting vulnerable instant messenger (IM) systems and using network viruses that do not require user interaction to spread. Other threats identified include botnets and increasingly intrusive adware. The report, " Malware Evolution. January-March 2005," from security firm Kaspersky Labs notes that viruses for IM systems started to appear late last year but are only now appearing in volume. Seven out of every eight IM worms attack Microsoft's MSN Messenger service. "Improved antivirus technologies, and increased user awareness of security issues are clearly forcing virus writers and hackers to use new approaches to access users' information and systems," said Alexander Gostev, senior virus analyst at Kaspersky Labs. The study identifies 40 individual IM worms in the first quarter of the year, the majority written in one of the simplest computer languages, Visual Basic (VB). It noted that use of this language indicates the authors are relatively unsophisticated coders, since VB is not widely used by experts because it is so slow to run. Report: http://www.viruslist.com/en/analysis?pubid=162454316

Category 23.5 *E-mail & instant messaging or chat*

2005-05-03 **NetWin Dmail Server vulnerabilities no update issued**

DHS IAIP Daily; http://www.security.org.sg/vuln/dmail31a.html

NETWIN DMAIL SERVER HAS TWO VULNERABILITIES.

NetWin DMail is a scalable mail server that can either be used as a small personal mail server or as an ISP mail system. An authentication bypass vulnerability was found in DMail's mailing list server (dlist.exe). This vulnerability may be remotely exploited to view logs generated by the mailing list server (dlist.exe) or to shut it down. The second is a format string vulnerability that exists in the admin commands of dsmtp.exe. The vendor has been informed of these vulnerabilities but no solution is currently available.

Category 23.5 *E-mail & instant messaging or chat*

2005-05-11 **Gaim instant messaging IM software MSN protocol bug flaw denial of service DoS**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2005/May/1013942.html

GAIM BUGS IN PROCESSING MSN MESSAGES AND CERTAIN URLS LET REMOTE USERS DENY SERVICE

Two vulnerabilities were reported in Gaim in the processing of MSN messages and certain URLs. A remote user can cause the application to crash. A remote user can send an instant message containing a specially crafted URL that will cause a buffer overflow. Jabber and SILC protocols are affected. Other protocols may also be affected. A remote user can send a specially crafted MSN message to trigger a pointer error and cause the client to crash. The vendor has issued a fixed version (1.3.0), available at: http://gaim.sourceforge.net/downloads.php

---

Category 23.5 E-mail & instant messaging or chat

2005-08-04 **instant messaging IM threat trend multiple network attack**

DHS IAIP Daily; http://www.techweb.com/wire/security/167101004

NEW TREND FOUND IN IM ENTERPRISE THREATS

Nearly a quarter more new viruses threatening corporate computers through employee use of public instant-messaging networks were discovered last month, including one that reflected a new trend of attacking multiple IM systems, a security firm said. A total of 42 new threats were tracked in July, a 24 percent increase over the previous month, San Diego-based Akonix Systems said. July had the second highest number of new threats seen by Akonix since the beginning of the year. The highest was in April, when 48 were found. Five new viruses were discovered in July, including Rants, Prex, Kirvo, Hagbard and Lamar. The Akonix Security Center also found new variants of previous malware, including Kelvir, Bropia, Opanki and Oscabot. Of particular concern was the Rants virus, which was found on two different IM networks, David Jaros, director of product marketing for Akonix, said. In April, Akonix started seeing the same virus written for separate networks, such as AIM from America Online and Yahoo Messenger. Since then, the security firm has seen several multi-network viruses. "The virus writers are no longer focusing on one network," Jaros said. "They're broadening the number of users as potential targets."

Category 23.5 E-mail & instant messaging or chat

2005-11-02 **instant messaging IM secure productive AOL MSN Yahoo merger**

DHS IAIP Daily; ttp://www.esecurityplanet.com/best_practices/article.php/3561171

SECURE AND PRODUCTIVE WORKPLACE INSTANT MESSENGING

With the possible merger of AOL's AIM, MSN Messenger and Yahoos Messenger there will approximately 275 million users communicating over the internet. This has led to a vital part of the workday for many individuals. One of the advantages is that instant messaging allows for inexpensive communication between individuals. In addition, more recently there is now have video conferencing or voice-chats with minimal fuss and no extra charges. There are some perceived disadvantages to using IM, which includes lost productivity. However, one way to deal with this is to provide appropriate training to employees about proper usage of IM and that it should be treated much like e-mail.

Category 23.5 E-mail & instant messaging or chat

2005-11-30 **instant messaging IM threats November 2005 skyrocket**

DHS IAIP Daily; http://www.messagingpipeline.com/news/174402978;jsessionid=XKU0HNGVXMREEQSNDBCCKH0CJUMEKJVN

INSTANT MESSAGING THREATS SKYROCKET IN NOVEMBER

Akonix Systems, the San Diego, CA, provider of instant messaging (IM) security systems, said that its Security Center team tracked 62 IM-based attacks in November, a 226-percent increase over last month. The most significant new finding was that viruses no longer discriminate against specific IM systems, and can have a far costlier impact in terms of potential damage. Akonix reported that 36 percent of the IM attacks hit more than one public network and 13 percent of the attacks had the capability to spread through all four major IM networks. The Akonix Security Center noted that 58 of the worms detected were variants of previous worms, while four new worms were introduced during November. "November marked the highest number of IM threats that we have ever seen to date, proving that hackers see this real-time communications medium as a wide-open security hole in corporate networks," said Don Montgomery, vice president of marketing at Akonix Systems, in a prepared statement.

Category 23.5 E-mail & instant messaging or chat

2006-01-04 **instant messaging IM exploit WMF vulnerability study**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/holes/story/0,10801,107455,00.html 23

ATTEMPTS TO EXPLOIT WMF VULNERABILITY BY INSTANT MESSAGING MULTIPLY

Security researchers have logged more than 70 variations of instant messages (IM) attempting to exploit the Windows Metafile (WMF) vulnerability since the first were reported on Saturday, December 31. Malicious WMF files can be distributed via a number of channels, including e-mail, Websites, peer-to-peer file sharing services and IM systems. An attacker may be able to gain control of an IM user's computer by sending such a file, or a link to a Website where one is hosted, through an IM system and then tricking the recipient into clicking on the file or link. The first attempts to do this were logged on Saturday morning, when security researchers at Kaspersky Labs Ltd. Received reports of a wave of attacks on Dutch users of the MSN Messenger service. They had received messages inviting them to click on a link to a Website containing an image with the name "xmas-2006 FUNNY.jpg." Anyone following the link would set in motion a chain of events, beginning with the download of a Trojan horse identified by Kaspersky as Trojan-Downloader.VBS.Psyme.br. This in turn would try to install a bot named Backdoor.Win32.SdBot.gen, which would then receive instructions over an Internet Relay Chat (IRC) channel to download IM-Worm.Win32.Kelvir.

Category 23.5 E-mail & instant messaging or chat

2006-01-18 **vulnerability Mozilla Thunderbird e-mail client execute arbitrary programs**

DHS IAIP Daily; http://www.securiteam.com/windowsntfocus/5CP0J2KHFO.html 23

MOZILLA THUNDERBIRD ATTACHMENT SPOOFING VULNERABILITY

Mozilla Thunderbird displays attachments in a wrongful manner which allows attackers to spoof attachments and convince users to execute arbitrary programs. The vulnerability is caused due to attachments not being displayed correctly in mails. This can be exploited to spoof the file extension and the associated file type icon via a combination of overly long filenames containing white spaces and "Content-Type" headers not matching the file extension. Successful exploitation may lead to malware being saved to the desktop. Vulnerable systems include Mozilla Thunderbird versions 1.0.2, 1.0.6, and 1.0.7; Mozilla Thunderbird version 1.5 is immune.

Category 23.5 E-mail & instant messaging or chat

2006-02-07 **IBM Lotus Domino LDAP remote denial-of-service vulnerability exploit no solution**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2006/0458 23

IBM LOTUS DOMINO LDAP SERVER REMOTE DENIAL-OF-SERVICE VULNERABILITY.

A vulnerability has been identified in IBM Lotus Domino, which could be exploited by remote attackers to cause a denial of service. This flaw is due to an error in the LDAP service that fails to properly handle malformed requests sent to port 389/TCP, which could be exploited by remote attackers to cause a denial of service by sending a specially crafted LDAP request to a vulnerable system. Solution: The FrSIRT is not aware of any official supplied patch for this issue.

Category 23.5 E-mail & instant messaging or chat

2006-02-10 **IBM Lotus Domino iNotes Client script insertion vulnerabilities exploit**

DHS IAIP Daily; http://secunia.com/advisories/16340/ 23

IBM LOTUS DOMINO INOTES CLIENT SCRIPT INSERTION VULNERABILITIES.

Some vulnerabilities have been reported in Lotus Domino iNotes Client, which can be exploited by malicious people to conduct script insertion attacks. Analysis: 1) Attached files (e.g. ".html" files) are opened in the context of the site if the user clicks on it. This can be exploited to execute arbitrary JavaScript code in the context of the user's session. 2) The e-mail subject is not properly sanitized before being displayed to the user as the browser title. This can be exploited to execute arbitrary JavaScript in the context of the user's session when the user views a received e-mail. 3) It is possible to bypass certain security checks related to "javascript:" URLs by inserting "
" in the middle of the URL. This can be exploited to execute arbitrary JavaScript code in the context of the user's session. 4) The attachment filename is not properly sanitized before being displayed to the user. This can be exploited to execute arbitrary JavaScript in context of the user's session when the user views a received e-mail. Solution: Update to version 6.5.5 or 7.0.1.

Category 23.5 *E-mail & instant messaging or chat*

2006-02-21 **Microsoft Kaspersky Lab error e-mail trouble Antigen security software**

DHS IAIP Daily; http://news.com.com/Kaspersky+update+zaps+Microsoft+antiviru s/2100−1002_3−6041792.html?tag=cd.top 23

MICROSOFT AND KASPERSKY LAB HAVE RECOVERED FROM ERROR CAUSING SIGNIFICANT E-MAIL TROUBLES.

Microsoft and Kaspersky Lab have recovered from an error that caused significant e-mail troubles for some users of Microsoft's Antigen e-mail security software. Antigen users started receiving updates for their Kaspersky Lab antivirus engine again on Tuesday, February 21. Microsoft and Kaspersky had put those on hold after a flawed update caused trouble last week, representatives for Microsoft and Kaspersky said Tuesday. "As far as both parties are concerned, the problems have been addressed and its business as usual," said Steve Orenberg, president of Kaspersky's North American operations. The problems left some people without fully functional e-mail systems for as long as 10 hours. The culprit was a routine update to the Kaspersky antivirus engine, which was distributed early Thursday morning, February 16. Microsoft in the afternoon offered the previous version of the engine for download to solve the problem. While halting the updates for the Kaspersky engine for several days meant that one engine wasn't updated, users were still protected by the other engines and updates.

Category 23.5 *E-mail & instant messaging or chat*

2006-03-22 **US CERT Cyber Security alert Sendmail vulnerability race condition solution upgrade**

DHS IAIP Daily; http://www.uscert.gov/cas/techalerts/TA06−081A.html 23

US-CERT TECHNICAL CYBER SECURITY ALERT TA06-081A: SENDMAIL RACE CONDITION VULNERABILITY.

A race condition in Sendmail may allow a remote attacker to execute arbitrary code. Sendmail contains a race condition caused by the improper handling of asynchronous signals. In particular, by forcing the SMTP server to have an I/O timeout at exactly the correct instant, an attacker may be able to execute arbitrary code with the privileges of the Sendmail process. Systems affected: Sendmail versions prior to 8.13.6. Solution: Upgrade Sendmail: Sendmail version 8.13.6 has been released to correct this issue: http://www.sendmail.org/8.13.6.html Patches to correct this issue in Sendmail versions 8.12.11 and 8.13.5 are also available. Version 8.12.11: ftp://ftp.sendmail.org/pub/sendmail/8.12.11.p0 Version 8.13.5: ftp://ftp.sendmail.org/pub/sendmail/8.13.5.p0

Category 23.5 *E-mail & instant messaging or chat*

2006-03-28 **F-Secure Messaging Security Gateway Sendmail code execution vulnerability solution update**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2006/1139 23

F-SECURE MESSAGING SECURITY GATEWAY SENDMAIL CODE EXECUTION VULNERABILITY.

A vulnerability in Sendmail may permit a specially crafted attack to take over the Sendmail MTA process, allowing a remote user to execute commands and run arbitrary programs on the system. Analysis: F-Secure Messaging Security Gateway Appliances use Sendmail. The vulnerability may permit a specially crafted attack to take over the Sendmail MTA process, allowing a remote user to execute commands and run arbitrary programs on the system. Affected products: F-Secure Messaging Security Gateway X200 version 3.1.0 and prior; F-Secure Messaging Security Gateway X200 version 3.2.4 and prior; F-Secure Messaging Security Gateway P600 version 3.1.0 and prior; F-Secure Messaging Security Gateway P600 version 3.2.4 and prior; F-Secure Messaging Security Gateway P800 version 3.1.0 and prior; F-Secure Messaging Security Gateway P800 version 3.2.4 and prior. Solution: Hotfixes are automatically distributed through the delivery system.

Category 23.5 *E-mail & instant messaging or chat*

2006-04-04 **McAfee WebShield SMTP remote format string vulnerability arbitrary code execution solution update**

DHS IAIP Daily; http://www.securityfocus.com/bid/16742/references 23

MCAFEE WEBSHIELD SMTP REMOTE FORMAT STRING VULNERABILITY.

McAfee WebShield SMTP 4.5 MR1a is susceptible to a remote format string vulnerability. There exists a format string vulnerability within the McAfee WebShield SMTP server which allows an attacker to execute arbitrary code on the host computer via an unauthenticated connection. With successful exploitation, an unauthenticated attacker is able to obtain SYSTEM access. Solution: The vendor has released a patch (P0803), along with version 4.5 MR2 to address this issue. Users of affected packages should contact the vendor for further information on obtaining fixes.

Category 23.5 *E-mail & instant messaging or chat*

2006-04-05 **sendmail asynchronous signal handling remote code execution vulnerability privilege grant solution update**

DHS IAIP Daily; http://www.securityfocus.com/bid/17192/references 23

SENDMAIL ASYNCHRONOUS SIGNAL HANDLING REMOTE CODE EXECUTION VULNERABILITY.

Sendmail is prone to a remote code execution vulnerability. Analysis: Compromise of networks and machines using affected versions of Sendmail may lead to exposure of confidential information, loss of productivity, and further network compromising. An attacker does not need to entice any kind of user interaction to trigger this vulnerability. Successful exploitation would grant an attacker the privileges that the Sendmail server daemon is running with. For a complete list of vulnerable products: http://www.securityfocus.com/bid/17192/info Solution: The vendor has released version 8.13.6 to address this issue. For further solution details: http://www.securityfocus.com/bid/17192/solution

---

Category 23.5 *E-mail & instant messaging or chat*

2006-04-20 **Microsoft Outlook Express patch erases addresses quality assurance flaw**

DHS IAIP Daily; http://www.informationweek.com/news/showArticle.jhtml;jsessionid=SSYKRYB5EYMMKQSNDBGCKHSCJUMEKJVN?articleID=186500318 23

MICROSOFT PATCH 'ERASES' OUTLOOK EXPRESS ADDRESSES.

Another Microsoft patch from the batch released last week is apparently causing problems, at least according to numerous Windows users on the Redmond, WA, developer's official message boards. After applying the patch from security bulletin MS06-016, say dozens of users, their Outlook Express e-mail client's address book disappeared and form-style messages can't be sent. The problem said users, including several Microsoft MVPs, was the MS06-016 patch (also tagged as KB911567). Uninstalling the patch returned the address book to its prior state and allowed template-based messages to be e-mailed normally.

Category 23.5 *E-mail & instant messaging or chat*

2006-05-09 **US CERT Microsoft Windows Exchange Server vulnerabilities execute arbitrary code**

DHS IAIP Daily; http://www.uscert.gov/cas/techalerts/TA06−129A.html 23

US-CERT TECHNICAL CYBER SECURITY ALERT TA06-129A: MICROSOFT WINDOWS AND EXCHANGE SERVER VULNERABILITIES.

Microsoft has released updates that address critical vulnerabilities in Microsoft Windows and Exchange Server. Exploitation of these vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary code or cause a denial-of-service on a vulnerable system. Systems affected: Microsoft Windows; Microsoft Exchange Server. Microsoft Security Bulletin Summary for May 2006 addresses vulnerabilities in Microsoft Windows and Exchange Server. Further information is available in the following US-CERT Vulnerability Notes: VU#303452: http://www.kb.cert.org/vuls/id/303452 VU#945060: http://www.kb.cert.org/vuls/id/945060 VU#146284: http://www.kb.cert.org/vuls/id/146284 Solution: Microsoft has provided updates for these vulnerabilities in the Microsoft Security Bulletin Summary for May 2006: http://www.microsoft.com/technet/security/bulletin/ms06-may. mspx Microsoft Windows updates are also available on the Microsoft Update site: https://update.microsoft.com/microsoftupdate/v6/muoptdefault .aspx?ln=en&returnurl=https://update.microsoft.com/microsoft update/v6/default.aspx?ln=en-us

---

23.6 Web-site infrastructure, general Web security issues

Category 23.6 *Web-site infrastructure, general Web security issues*

1997-01-03 **Web**

RISKS 18 77 ff

A Swedish correspondent reported in RISKS that AltaVista includes the keywords from a user's most recent search in the URL for inline advertisements. This practice, which is undocumented on the search page, compromises the privacy of users.

Category 23.6 *Web-site infrastructure, general Web security issues*

1997-01-05 **Netscape**

RISKS 18 74

A new bug in Netscape 3.0, 3.01 and 4.01 beta 1 allows a Web site to obtain a browser's e-mail address.

Category 23.6 *Web-site infrastructure, general Web security issues*

1997-01-13 **security Web e-commerce**

Computerworld Web site

O'Reilly & Associates published a survey of 648,613 Web sites in which they found that only 10% of the sites use SSL and only 0.5% offer third-party authentication (necessary for customers to be sure that they are dealing with the business they think they are connected to and not an imposter-site).

Category 23.6 *Web-site infrastructure, general Web security issues*

1997-03-27 **electronic commerce Web browser hole SSL**

Inter@ctive Week, RISKS

A newly-discovered hole in Web security allows information from a secure transaction to be captured by subsequent Web sites. Eugene Spafford and Steve Bellovin concur that the problem is a serious issue that will require major re-engineering to surmount. Patches are expected to take weeks.

Category 23.6 *Web-site infrastructure, general Web security issues*

1999-02-10 **e-commerce credit card personal information password privacy**

RISKS 20 20

Prof. Ross Anderson of Cambridge University analyzed requirements on the AMAZON.COM online bookstore for credit card number, password, and personal details such as phone number. He identified several risks: (1) merchant retention of credit card numbers poses a far higher risk of capture than of capture in transit; (2) adding a password increases the likelihood of compromise because so many naïve users choose bad passwords and then write them down; (3) even the British site for Amazon contravenes European rules on protecting consumer privacy; (3) such practices make it easier for banks to reject their clients' claims of fraudulent use of their credit-card numbers.

Category 23.6 *Web-site infrastructure, general Web security issues*

2000-05-15 **Web programming QA quality assurance vulnerability fix**

RISKS, Zope (http://www.zope.org/Members/jim/ZopeSecurity/ClientSideTrojan 20 89

Chris Adams summarized a widespread vulnerability in Web-site administration tools: "Basically, an attacker could create a page that redirected to site's admin interface or a form that submitted to it (possibly using JavaScript for automatic submission); in any case, the effect was that any use who was logged in as a site administrator could have an attacker execute arbitrary commands in their security context merely by following a link. If this was carefully set up using JavaScript and frames, it's more than possible that the admin would never notice what had happened. This attack would be particularly effective against online news sites and anyone else for whom it is common to receive many URLs every day as submissions." Adams pointed out that an easy fix was to make it more difficult to guess the form parameters for generating the URLs: "given that you need to have a random identifier that is not leaked to third parties for meaningful session management, an obvious step is to put in a parameter in the form that must match the user's session ID (e.g. Confirm=346593045 instead of Confirm=true)."

Category 23.6 *Web-site infrastructure, general Web security issues*

2000-05-26 **cache certificate user interface error QA quality assurance design flaw vulnerability exploit**

RISKS, CERT-CC http://www.cert.org/advisories/CA-2000-08.html 20 89

Kevin Fu reported in RISKS that Netscape Navigator has a flaw in the user interface for dealing with invalid certificates: "Within one Netscape session, if a user clicks on "continue" in response to a "hostname does not match name in certificate," then that certificate is incorrectly validated for future use in the Netscape session, REGARDLESS of the hostname or IP address of other servers that use the certificate. It seems that the "Certificate Name Check" warning will cache a certificate as valid for any hostname or IP address in the future. In this way, if an adversary tricks a user into accepting an invalid certificate at a seemingly benign site, then the user can then be tricked if he/she ever visits a malicious site using the same certificate. A `continue' click on a seemingly benign SSL web server might end up taking away server authentication from visiting https://www.a-site-that-you-give-private-info.com/ that has poisoned DNS." Fu concludes that this case raises serious questions:
(1) A user interface should be explicit; "Continue" is an insufficient indicator of function.
(2) Implementing security is hard, and the failure of Netscape should raise warning flags about implementation by other companies who invent their own security solutions.

Category 23.6 *Web-site infrastructure, general Web security issues*

2000-06-01 **malicious code executable compression stupidity risk management sneakernet air gap copyright UCITA license dissemination control**

RISKS 20 90

Avi Rubin complained in RISKS about how Microsoft distributed a white paper — by offering a self-extracting executable file. "Of all companies, Microsoft should be the last one to encourage users to get into the habit of downloading .exe programs and running them. . . . The problem is that it is very difficult to know that a program is harmless, just because it does something that you expect it to do. I could not believe that this is how Microsoft distributes its white papers. It is beyond comprehension."

In the next issue of the RISKS Forum Digest, Paul Wallich suggested that putting a document into an executable file might be a way of restricting distribution: "Bundling the file into an executable, however, arguably meets the requirements of the Digital Millennium Copyright Act for a technological copy-protection mechanism, which makes unauthorized redistribution of the text a serious crime (where `serious' means `you could go to jail for more than a year'). . . . If you view control, rather than dissemination, as the goal of putting documents on a web site, it's easy to comprehend."

Category 23.6 *Web-site infrastructure, general Web security issues*

2000-06-29 **confidentiality Web security failure**

RISKS 20 94

Keith Rhodes reported in RISKS, "In Australia, someone claimed to have accessed a Treasury Department Web site www.gstassist.gov.au that had essentially no security. By indexing from 1 to 17,000, he was able to obtain the bank records of that many registered GST Startup certificate suppliers. (There were apparently 27,000 records in all, but access stopped when the site was disabled.) He then sent e-mail to each these companies (which can honour a $200 GST-related rebate on computers, software, services and other items required for small and medium companies to prepare for Australia's new taxation system) with its own relevant details."

Category 23.6 *Web-site infrastructure, general Web security issues*

2000-07-18 **QA quality assurance Web design encryption false information cleartext transmission**

RISKS 20

The Royal Mail Web site claimed that it was using encrypted traffic to capture credit-card information when in fact it was not. An alert RISKS contributor, Gary Barnes noticed that his browser was in HTTP mode rather than HTTPS mode. Two weeks after he reported the problem, the incorrect protocol and the incorrect assurance of security were still in place. He wrote, "The RISK here is that customers will believe a web site that says `all orders sent from your computer to our servers [...] will be secured through the use of encryption technology', especially when the organisation responsible is as `trustworthy' as Royal Mail, and then trustingly send their unencrypted card details over the Internet. There's also the RISK that once alerted to such mistakes companies won't or can't act to fix the problem in a timely fashion, or at least remove their incorrect boasts of being `secure'."

Category 23.6 *Web-site infrastructure, general Web security issues*

2000-08-03 **confidentiality passwords e-mail access design Web security flaw vulnerability management process operations**

RISKS 21 03

During the month of July, an internal search page allowing access to user IDs and passwords was made world-readable on Switzerland's second-largest ISP. Over 700 accounts were compromised on the Sunrise ISP due to at least 20 different searches. Such a lapse is a violation of the European Directive on Data Privacy. Peter Kaiser, writing in RISKS, pointed out that storing unencrypted passwords is a terrible idea, let alone when the only protection was security by obscurity. He also pointed out to the ISP that their practice of soliciting user passwords in unsecured HTTP (instead of HTTPS) was a bad idea, but his warnings were ignored.

Category 23.6 *Web-site infrastructure, general Web security issues*

2000-08-16 **Web site URL ID strings data diddling modification access public relations privacy**

RISKS 21

The dangerous practice of encoding identifiers in URLs was exposed once again by Paul van Keep in RISKS, who reported that the < annapa.com > Web site allows anyone to alter the identifier in the URL for an account to access other accounts. Unfortunately, the company belittled the exploit, claiming that it was somehow restricted to "IT-specialists" only and therefore not a significant vulnerability.

Category 23.6 *Web-site infrastructure, general Web security issues*

2000-08-17 **Web site security log files accessibility access controls attributes**

RISKS 21 02

The Canadian _Globe and Mail _ (sometimes referred to as the _Groan and Wail_) Web site has world-readable log files that record, among other things, the exact IP address and search string of every request.

Category 23.6 *Web-site infrastructure, general Web security issues*

2000-08-25 **user identification policy problem vulnerability error flaw design stupidity confidentiality**

RISKS 21

Hotmail makes buddy lists available to anyone who registers an e-mail account using the name of an expired account. However, as Jay Ashworth noted in RISKS, more important is that allowing reuse of an identifier opens up enormous potential for impersonation and fraud.

Category 23.6 *Web-site infrastructure, general Web security issues*

2000-08-27 **Web design flaw inconsistency**

RISKS 21 04

Daniel P. B. Smith noted in RISKS that the eBay online auction Web site shows a time counter on each auction's Web page. Unfortunately, although the counter is updated in real time, the rest of the status information — including how many bids there are — does not get updated as frequently. He goes on to describe an embarrassing situation where he accepted an early, lower bid because he never received updates from eBay about a later, higher bid.

Category 23.6 *Web-site infrastructure, general Web security issues*

2000-10-03 **Web design glitch bug unknown access typo search confidentiality world readable medical information**

RISKS 21 09

Mistyping a search keyword on the Florida Department of Health's Web site caused the mystified user to access sensitive files including names, addresses and medical information. The state CIO apologized for the glitch and said the Health Department would continue investigating the glitch to find the cause and stop recurrence of such errors.

Category 23.6 *Web-site infrastructure, general Web security issues*

2000-10-24 **Web design flaw URL confidentiality**

RISKS 21 09

The New Jersey EZPASS Web site was shut down after it became clear that anyone could access the billing information for other users by altering a URL to transform it into someone else's URL. [MORAL: don't design Web sites so that identification information is encoded in URLs.]

Category 23.6 *Web-site infrastructure, general Web security issues*

2001-03-16 **e-commerce electronic data interchange EDI vulnerabilities weakness audit government tax confidentiality integrity penetration**

RISKS 21 28

Dave Stringer-Calvert, writing in RISKS, reported a finding by the GAO of lax security in IRS electronic filing systems:

"Even as the IRS was assuring taxpayers last year that electronic filing of tax returns was secure, serious shortcomings existed that could have allowed hackers to view and even change information on returns, a government watchdog agency said. The General Accounting Office found no evidence that hacking had occurred, but it said its investigators were able to gain unauthorized access to the tax agency's electronic filing system, which will handle a third of all federal returns this year. The GAO cited the IRS for lax security controls and for not requiring encryption of electronic returns. The report also said the IRS sent out $2.1 billion in refunds to taxpayers whose returns were not properly authorized."

Category 23.6 *Web-site infrastructure, general Web security issues*

2001-05-01 **buffer overflow QA quality assurance Web server**

NIPC Daily Report

Microsoft has released security bulletin MS01-023 regarding a security flaw that could allow a hacker to gain complete control of a Web site running IIS 5.0 server software for Windows 2000. The security vulnerability results because the ISAPI extension contains an unchecked buffer in a section of code that handles input parameters. This could enable a remote attacker to conduct a buffer overrun attack and cause code of their choice to run on the server. Such code would run in the Local System security context. This would give the attacker complete control of the server. Additional information regarding this vulnerability can be found at
http://www.microsoft.com/technet/security/bulletin/MS01-023.asp. (Source: Microsoft Corporation, 1 May)

Category 23.6 *Web-site infrastructure, general Web security issues*

2001-05-02 **criminal hacker tool exploit Web servers vulnerabilities rootkit patch**

NIPC Daily Report

A hacker, using the name "Dark Spyrit," released a program on 2 May designed to exploit the security hole in Windows 2000 Web servers. The program will give anyone with limited technical knowledge the ability to completely control a Windows 2000 server running version 5 of Microsoft's Internet Information Server (IIS) Web software. The creation of the exploit code for the flaw came as no surprise to Microsoft. "Customers who have applied the patch don't have to worry," the company said in a statement. "Customers who haven't applied the patch should take this as a reminder to do so immediately." (Source: ZDNet News, 3 May) (NIPC Comment: The NIPC issued Advisory 01-011 on 2 May, reporting the vulnerability in Microsoft s Internet Information Services (IIS) 5.0. www.nipc.gov/warnings/advisories/2001/01-011.htm.)

Category 23.6 *Web-site infrastructure, general Web security issues*

2001-06-12 **distributed computing Web design denial of service availability saturation**

RISKS 21 48

Steve Loughran noted in RISKS that the SETI@home screensaver that does computations for the Search for Extraterrestrial Intelligence project inadvertently caused a problem when Internet access to the SETI@home site became inaccessible. Seems the screensaver repeatedly attempted to "phone home" and saturated the Network Address Translation (NAT) pool of addresses. Mr Loughran noted, "The article closes by saying the problem was "solved" by increasing the number of available NAT addresses, although of course that didn't fix the problem, merely caused it to 'go away'. A real solution would be to have the screen-saver software implement incremental backoff and other mechanisms designed to gracefully handle a complete loss of remote server access. One would hope that the authors of the next generation of distributed computation applications take heed of the lessons of the current batch."

However, a staff member from SETI@home noted later, "One of the risks of developing any software is that problems experienced by users will be associated with the design of the software, not the failure of other components. The GUI version of SETI@home, upon connection failure, retries the connection twice at 45 second intervals. After the third failure the program waits 60 minutes before retrying. The UNIX version waits 60 minutes between connection failures. Apart from this report, I am unaware of any TCP/IP implementation that is unable to support 3 connection attempts per hour."

Category 23.6 *Web-site infrastructure, general Web security issues*

2001-08-31 **cross-site scripting vulnerability Web hack e-commerce digital cash e-wallet e-mail patch**

NewsScan

HOTMAIL HACKABLE WITH ONE LINE OF CODE [31 Aug 2001]
Security consultant Jeremiah Grossman was able to break through Microsoft's Hotmail and Passport protection schemes with just one line of code. Microsoft has patched the code, but Grossman says he could do it again in eight hours of work. His hacking experiment used a "cross-site scripting" technique that attaches invasive code onto programs used to make Web pages more interactive. Grossman calls them "a breeding ground for new types of Web security vulnerabilities," and Shawn Hernan of the Computer Emergency Response Team at Carnegie Mellon University says that "it's easy to dream up very, very bad scenarios." (USA Today 31 Aug 2001)
http://www.usatoday.com/life/cyber/tech/2001-08-31-hotmail-security.htm

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2001-12-06 **Internet security architecture implementation failure penetration vulnerability hacking intrusion**

RISKS 21 81

Peter G. Neumann summarized an article entitled, "Security hole at WorldCom left internal computer networks at risk" from the Associated Press:

"A security hole at WorldCom Inc. left internal networks at several of the nation's top companies (e.g., AOL Time Warner, Bank of America, CitiCorp, News Corp., JP Morgan, McDonald's Corp., Sun Microsystems) open to hackers. Adrian Lamo, a consultant in San Francisco, worked with WorldCom to fix the months-old problem over the weekend. There is no evidence that the security hole had been exploited, although it was possible to reconfigure or shut down corporate networks. Lamo: ``These networks were never designed to be connected to the Internet, They were private circuits running between locations." [Source: eponymous AP item, 05 Dec 2001, PGN-ed] "
http://www.siliconvalley.com/docs/news/tech/080991.htm

Category 23.6 *Web-site infrastructure, general Web security issues*

2002-01-07 **Web site design ActiveX operating system compatibility standards security**

RISKS 21 86

Koos van den Hout noted in RISKS that the mcafee.com Web site "shows a pop-up asking me to enable an ActiveX plug-in. . . . The fact that I am using a different operating system for which an ActiveX plug-in isn't available at all has never crossed the mind of whoever designed that." As he continued his browsing, he found that when he used the text-based Lynx 2.8.2 browser for Unix, he was told to lower the security setting for his browser -- in terms clearly indicating that the designer was taking MS Internet Explorer for granted.

Category 23.6 *Web-site infrastructure, general Web security issues*

2002-01-10 **confidentiality SSL https implementation failure URL QA quality assurance**

RISKS 21 86

Skip La Fetra pointed out in RISKS that some Web sites boasting of SSL and HTTPS connections construct URLs that contain sensitive details of a transaction. In his example, one page constructed a URL "https://securesite.com/verification.htm?name=3Dyyyyyy,CardNumber=3D12345=6789,ExpirationDate=3D12/31/2001" which Being part of the URL "address", this information included his name, address, credit card number, and expiration date. Such URLs _can_ be intercepted and the information abused despite the encryption of the page contents.

Category 23.6 *Web-site infrastructure, general Web security issues*

2002-01-10 **SSL https e-mail insecure transmission privacy design**

RISKS 21 86

J. Debert noted an inconsistency in attempts to protect consumer privacy:
>ATT allows customers to send form mail using SSL on their Web site. This is to keep their customer's info and the message private.

But their people include the entire message in plaintext e-mail messages sent in response defeating the purpose of the secure form.<

Category 23.6 *Web-site infrastructure, general Web security issues*

2002-02-11 **credit card Internet security risks bank failure government regulators**

NewsScan; http://www.usatoday.com/life/cyber/tech/2002/02/08/nextbank.htm

NEXTBANK BECOMES FIRST INTERNET BANK TO FAIL
Federal regulators have shut down Phoenix-based NextBank, whose principal business was issuing credit cards over the Internet. The government's Office of the Comptroller of the Currency said that NextBank's "unsafe and unsound practices" (making loans to poor-credit customers who were unable to handle payments) made it unlikely that the bank would be able "to pay its obligations in the normal course of business" without federal assistance. The Federal Deposit Insurance Corporation (FDIC) will begin mailing checks today to the bank's customers for the amount of their insured deposits. (AP/USA Today 8 Feb 2002)

Category 23.6 *Web-site infrastructure, general Web security issues*

2002-02-13 **vulnerability remote control shutdown penetration**

NewsScan; CERT® Advisory CA-2002-03 http://www.cert.org/advisories/CA-2002-03.html

SECURITY EXPERTS ISSUE WARNING [13 Feb 2002]
CERT/CC, a center of Internet security expertise, at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University, is warning computer users of a network security flaw that could allow a computer to be invaded remotely by vandals who could take over and shut down the system. Shawn Herman of CERT says that virtually every network uses a multitude of devices that may have the security flaw. To see a list of potential vulnerabilities and what to do about them, go to http://www.cert.org/. (New York Times 13 Feb 2002)
http://partners.nytimes.com/2002/02/13/technology/13NET.html

Category 23.6 *Web-site infrastructure, general Web security issues*

2002-03-10 **Web server vulnerabilities ICAT CVE**

ICAT Metabase

The ICAT Metabase < http://icat.nist.gov/icat.cfm > for the Common Vulnerabilities and Exposures (CVE) database reported 76 vulnerabilities involving Web servers out of a total of 1241 for the period from 1 Jan 2001 to 10 Mar 2002. This represents about 6% of all vulnerabilities logged for that period. Overall, for the entire period since the CVE began recording vulnerabilities in 1995, Web servers are named in 199 of the 3677 vulnerabilities or about 5% of the total.

Category 23.6 *Web-site infrastructure, general Web security issues*

2002-03-11 **quality assurance QA Web design I&A identification authentication password failure flaw goofball idiots fools stupidity absurd**

RISKS 21 94

Grant Bayley reported that in Australia, an error in the programming for the Web-based registration system for names in the .org.au, .gov.au, and .edu.au domains allowed anyone to change ownership details of any domain instantly without even knowing the right password. Such a hole would have allowed complete hijacking of every non-commercial domain in Australia, including police forces and state governments.

Category 23.6 *Web-site infrastructure, general Web security issues*

2002-03-14 **design QA quality assurance Web URL discounts confidentiality**

RISKS 22 01

Saab USA sent out a promotion offering discounts to people who used a Web site with unique URLs for each recipient. Unfortunately, the URLs used sequential ID numbers. Entering a randomly-generated URL resulted in access to the name and address of some other recipient of the offer. In addition, there was nothing to stop users from printing more than one of the supposedly mutual discount offers available on the Web site, thus resulting in more discounts than the company apparently intended to offer. When Ron Gut, who reported on this case to RISKS, tried to use Saab's contact form to suggest improvements, he discovered that the form did not work with Netscape v4.7.

Category 23.6 *Web-site infrastructure, general Web security issues*

2002-03-27 **identity theft confidentiality online auction I&A identification authentication denial of service Web design passwords timeout inactivation lock penetration brute force dictionary attack password cracking**

RISKS, http://zdnet.com.com/2100-1106-868306.html 21 98

E-bay acounts are not protected by any limitation on the number of incorect logons; far from including a lockout, the service does not even impose a timeout. The system is ripe for brute-force, automated password-cracking. According to Scott Nicol, writing in RISKS, e-Bay chose this strategy to preclude denial-of-service attacks that become too easy when an account is locked simply because of repeated bad passwords. [MK notes: This is a classic example of the tradeoffs that different security measures impose: add a delay and you have made the attacker's job easier if their goals is DoS – they just have to send the same wrong password often enough to initiate another timeout. A reasonable approach would be to leave the zero-knowledge approach and look for patterns of attack so that the system can selectively respond to _attacks_ and not to _mistakes_.]

Category 23.6 *Web-site infrastructure, general Web security issues*

2002-04-22 **vulnerabilities buffer overflow database server arbitrary code**

Security Wire Digest 4 31

Shawna McAlearney wrote in Security Wire Digest about an important patch:

>Microsoft last week [mid-April 2002] urged SQL Server users to immediately patch a vulnerability that could allow an attacker to run code of choice on a target machine.

Ranked as a "moderate" threat by Microsoft, the "SQL Extended Procedure Functions Contain Unchecked Buffers" flaw affects SQL Server 7.0/2000. Those versions provide extended stored procedures that fail to validate input correctly, making them susceptible to buffer overflows.

An attacker exploiting the flaw could cause the SQL Server service to fail, or run code in the security context in which SQL Server is running--by default set to domain user. Microsoft says the precise privileges the attacker could gain depend upon the specific security context that the service runs in.

Category 23.6 *Web-site infrastructure, general Web security issues*

2002-05-05 **privacy browser QA quality assurance bugs flaws weaknesses vulnerabilities exploits demonstrations**

RISKS, http://www.newsbytes.com/news/02/176077.html 22 05

Brian McWilliams wrote in Newsbytes:

Security flaws in privacy features added to Microsoft's Web browser could enable attackers to perform several privacy-robbing attacks, including hijacking victims' MSN Messenger accounts, a security researcher warned. According to Thor Larholm, a developer with Denmark-based Internet portal Jubii.dk, "severe" bugs in the "Privacy Report" feature in Internet Explorer version 6 can be exploited "in effect removing all privacy." Last week, Larholm posted an advisory and harmless demonstrations of the flaws at his personal Web site. One example showed how the browser bugs enable a Web site to launch programs that exist on the user's hard disk. Another demo page silently sends a message to users in the target's MSN Messenger contact list….

Category 23.6 *Web-site infrastructure, general Web security issues*

2002-05-18 **Web design failure QA quality assurance SSL HTTPS credit card**

RISKS 22 07

VeriSign sells security services such as the "Code Signing Digital ID." However, reported Daniel Norton in RISKS, when you fill out your subscription form on line, the information including your credit-card data is sent in the clear using HTTP instead of HTTPS with SSL.

Category 23.6 *Web-site infrastructure, general Web security issues*

2002-05-20 **cumulatative patch weakness flaws QA quality assurance**

Security Wire Digest 4 39

Advisory MS-02-023 caused a fuss because GreyMagic Software complained that the cumulative patch contained major flaws. Shawna McAlearney summarized the situation as follows in Security Wire Digest:

>
GreyMagic says Microsoft misunderstood what it called a cross-site scripting problem. "They only patched a symptom of this vulnerability, not its root cause," says GreyMagic. "The problem is not plain cross-site scripting, the problem is that dialogArguments' security restrictions are bypassed and it is passed to the dialog even though it shouldn't be."

GreyMagic now also contends that Microsoft failed to provide a sufficient patch for an earlier flaw.

"MS02-023 also allegedly patches the cssText issue we found back in February, but the patch is weak and can be easily circumvented," says GreyMagic. "So far we have a bulletin full of errors, which was partly fixed by Microsoft; an incomplete patch to the dialogArguments critical vulnerability, leaving IE 5.0 and IE 5.5 exposed; and a useless patch to the cssText vulnerability, leaving all users exposed to (a) critical vulnerability."

Causing further confusion is the "content-disposition: inline" IE flaw discovered by the LAC Corp. that "allows for downloading of a file and its automatic execution under several circumstances without the knowledge of the user."

Microsoft earlier dismissed LAC's advisory as "inaccurate" and having "nothing to do with either Internet Explorer or the security patch" released last year to fix a similar vulnerability, according to a Newsbytes report. MS02-023 acknowledges that IE 5.01/6 are vulnerable to the attack reported by LAC.
<

Category 23.6 *Web-site infrastructure, general Web security issues*

2002-05-23 **fraud loop lockout availability Web design priority I&A identification authentication child protection credit card**

RISKS 22 09

Daniel P. B. Smith presented an interesting case of bad design in his submission to RISKS. He needed to change the privacy settings on his Microsoft Passport account and, while he was at it, he had the idea of altering his name and age on the Web form presented for editing his profile. Unfortunately, he changed his name to Mickey Mouse and claimed he was born on 2001-04-01. This false entry then immediately locked him out of the profile editor because "he" was under 13! The only way to change the record was to create a new account that would allow him to alter the records for his "child." [MK comments: Personally, I don't like the idea of supplying false information to _anyone_. If you don't agree to the terms of a contract, don't accept the contract. The other message I glean from this case is that when you design a fail-safe mechanism, don't convert a process or account from a higher priority to a lower priority without confirming that the change is correct. In this case, a message informing the user, "If you change the birthday to indicate that you are less than 13 years old, you will lose the ability to update your profile" could have prevented the problem.]

Category 23.6 *Web-site infrastructure, general Web security issues*

2002-06-18 **quality assurance QA alert vulnerability snafu problem bug notification patch**

FindLaw Download This 90

SECURITY FLAW IN WEB SOFTWARE
A security bug was found in software used by millions of Web sites. Private experts alerted users and the FBI's computer security division. Problem is, they didn't tell the maker of the software. Then they issued the wrong prescription for fixing the problem. The incident Monday involving Apache's Web software shows that the system to insulate the Internet from attack - a joint effort of the government and private companies - is still a long way from perfect.
http://news.findlaw.com/ap/ht/1700/6-18-2002/20020618023004_3.html

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2002-06-18 **MS IIS alert vulnerability Web server flaw bug weakness patch**

FindLaw Download This 90

MICROSOFT DISCLOSES SOFTWARE FLAW
Microsoft Corp. acknowledged a serious flaw Wednesday in its Internet server software that could allow sophisticated hackers to seize control of Web sites, steal information and use vulnerable computers to attack others online. The software, which runs about one-third of the world's Web sites, is used by millions of businesses and organizations but less commonly by home users. Microsoft made available a free patch for customers using versions of its Internet Information Server software with its Windows NT or Windows 2000 operating systems. The server software included within Microsoft's newer Windows XP operating system was not affected by the security flaw.
http://news.findlaw.com/ap/ht/1700/6-12-2002/20020612170005_59.html

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2003-01-15 **list top ten Web security vulnerabilities common HTTP exploits**

NIPC/DHS

January 13, Government Computer News — Open-source group names top 10 Web vulnerabilities.

The Open Web Application Security Project has released a list of the top 10 vulnerabilities in Web applications and services. The group said it wants to focus government and private-sector attention on common weaknesses that require immediate remediation. In the longer term, this list is intended to be used by development teams and their managers during project planning," the report noted. "Ultimately, Web application developers must achieve a culture shift that integrates security into every aspect of their projects." OWASP is a volunteer open-source community project created to bring attention to security for online apps. The OWASP vulnerabilities are well known, but continue to represent significant risk because they are widespread. They can be exploited by code in HTTP requests that are not noted by intrusion detection systems and are passed through firewalls and into servers despite hardening. The complete report and list of vulnerabilities is available on the organization's Web site, www.owasp.org.

Category 23.6 *Web-site infrastructure, general Web security issues*

2003-02-06 **Microsoft security bullentin Internet Explorer vulnerability patch**

NIPC/DHS

February 05, Microsoft — Microsoft Security Bulletin MS03-004: Cumulative patch for two vulnerabilities involving Internet Explorer's cross-domain security model.

A flaw in Internet Explorer could allow a malicious web site operator to access information in another internet domain, or on the user's local system by injecting specially crafted code when certain dialog boxes were presented to the user. In the worst case, this vulnerability could allow an attacker to load a malicious executable onto the system and execute it. The attacker would have no way to force a user to a malicious web site. The vulnerability results because it is possible when using dialog boxes to bypass the cross-domain security model that Internet Explorer implements. A related cross-domain vulnerability allows Internet Explorer's showHelp() functionality to execute without proper security checking. In this scenario, the attacker could open a showHelp window to a known local file on the visiting user's local system and gain access to information from that file by sending a specially crafted URL to a second showHelp window. The attacker could also potentially access user information or run code of attacker's choice. Microsoft has assigned a risk rating of "Critical" to these vulnerabilities. A patch is available at the Microsoft website:
http://www.microsoft.com/windows/ie/downloads/critical/81084 7/default.asp. Applying the patch, however, will disable the HTML Help functionality because HTML Help was one of the attack vectors. Users who apply this patch are also encouraged to download the HTML Help update after applying this cumulative patch in order to restore HTML Help functionality.

Category 23.6 *Web-site infrastructure, general Web security issues*

2003-02-19 **list top ten Web security vulnerabilities common HTTP exploits**

NIPC/DHS

February 18, Government Computer News — Open Source group releases list of top 10 Web vulnerabilities.

The Open Web Application Security Project released a list of the top ten vulnerabilities in Web applications and services on Tuesday. The group said it wants the list to focus government and private-sector attention on common vulnerabilities "that require immediate remediation." "Also, in the longer term, this list is intended to be used by development teams and their managers during project planning," the report reads. OWASP is a volunteer Open Source community project created to bring attention to Web application security. It patterned its list on the SANS Institute's and FBI's top 20 list of network vulnerabilities. Like the SANS-FBI list, the OWASP vulnerabilities are well known and have been recognized for years, but continue to represent significant risks because they remain common. They can be exploited by code in http requests that are passed through firewalls and into servers despite hardening and are not noted by intrusion detection systems. The complete report is available from the OWASP Website at www.owasp.org.

Category 23.6 *Web-site infrastructure, general Web security issues*

2003-03-06 **new vulnerability critical Macromedia Flash player Internet media software patch fix**

NIPC/DHS

March 04, IDG News Service — Macromedia reports critical hole in Flash player.

Macromedia Inc. warned Monday of a "critical" security flaw in the latest version of its Flash animation player and advised users to install an updated to fix the problem. The security flaw affects Version 6 of the Macromedia Flash Player, which was released a year ago this month and has been installed on an estimated 75% of PCs worldwide, according to the company. The vulnerability affects the integrity of the player's "sandbox," which is supposed to act as a cordoned-off area where Flash code retrieved from the Web can be run safely, without access to a user's files. The flaw could allow a malicious hacker to run native code on a user's computer, outside the sandbox, possibly without the user's knowledge, according to information on the company's Web site. No users had reported having been affected by the problem as of Monday evening, a Macromedia representative said. Nevertheless, the company advised users to download a new version of the player — Version 6.0.79.0 — from its Web site immediately. The bulletin, with a link to the download site, is at www.macromedia.com/v1/handlers/index.cfm?ID=23821.

Category 23.6 *Web-site infrastructure, general Web security issues*

2003-03-10 **BIND domain name server vulnerability fix Internet Software Consortium**

NIPC/DHS

March 05, CNET News — Net consortium ties flaws to BIND.

Domain name servers are used to match domain names to numerical Internet Protocol addresses. As the vast majority of these run BIND (Berkeley Internet Name Domain), the software essentially runs the Internet. The Internet Software Consortium (ISC), the group responsible for maintaining the software, released a new version of BIND on Monday, with their Web site billing it as a maintenance release. However, on Wednesday the site had been updated, saying that the ISC had been made aware of vulnerabilities in BIND, adding that upgrading was "strongly recommended." BIND 9.2.1 is vulnerable to a remote buffer overflow bug when installed with the "libbind" nondefault option. Previous versions may also be vulnerable to problems associated with the commonly used OpenSSL library, but again this is a nondefault installation option and has more to do with the SSL library than BIND itself. An updated version of BIND is available at the ISC website: http://www.isc.org/products/BIND/.

Category 23.6 *Web-site infrastructure, general Web security issues*

2003-03-14 **new vulnerability buffer overflow Opera software browser fix**

NIPC/DHS

March 13, eSecurity Planet — Opera rushes out another security fix.

Norway-based Opera Software has pushed out a new version of its Opera 7 browser because of issues surrounding security. The bug, which affects both versions 6.x and 7.x, was detected in the browser's handling of filenames when showing the "Download Dialog" box. "The problem is that very long filenames are handled incorrectly. This allows a malicious website to create a filename that causes a buffer overflow which can be exploited to execute arbitrary code," according to an alert from IT security services firm Secunia. In releasing the new Opera 7.03 version, the company confirmed the Secunia findings. Secunia warned that exploits for the vulnerability are in the wild for Windows, noting that "exploitation does not require user interaction as Web sites can spawn the "Download Dialog" automatically."

Category 23.6 *Web-site infrastructure, general Web security issues*

2003-03-18 **new vulnerability Internet Information Server IIS Microsoft buffer overflow advisory**

NIPC/DHS

March 17, Department of Homeland Security — Unchecked buffer in Microsoft Internet Information Server (IIS), Advisory 03-005.

A security vulnerability is present in a Windows component used by WebDAV. A buffer overflow vulnerability exists in Microsoft IIS 5.0 running on Microsoft Windows 2000. Microsoft Windows 2000 and IIS Version 5.0 support the World Wide Web Distributed Authoring and Versioning (WebDAV) protocol. IIS 5.0 is installed and running by default on Microsoft Windows 2000 server products. An attacker could exploit the vulnerability by sending a specially formed HTTP request to a machine running Windows 2000 server and IIS Version 5.0. The request could cause the server to fail or to execute code of the attacker's choice. The code would run in the security context of the IIS service which, by default, runs in the LocalSystem context. Although Microsoft has supplied a patch for this vulnerability and recommends customers install the patch immediately, additional tools and preventive measures have been provided that customers can use to block the exploitation of this vulnerability while they are assessing the impact and compatibility of the patch. As an initial workaround Administrators can implement Microsoft's URL Scan tool to limit the lengths of URLs passed to the IIS system. Administrators are urged to update IDS signature files as relevant signatures become available; monitor FW, IDS, and other perimeter security devices for probes against port 80 and/or attempts to exploit this vulnerability; monitor information sources for additional alerts regarding possible attack activity; and report any relevant activity (increased port 80 probing or activity, web server crashes, etc.) to your agency Incident Response Capability and FedCIRC. The patch and additional information about this vulnerability are available on the Microsoft Website in Microsoft Security Bulletin MS03-007: Unchecked Buffer In Windows Component Could Cause Web Server Compromise:
http://www.microsoft.com/technet/treeview/default.asp?url=/t echnet/security/bulletin/MS03-007.asp See also CERT Advisory CA-2003-09: Buffer Overflow in Microsoft IIS 5.0 available at
http://www.cert.org/advisories/CA-2003-09.html

Category 23.6 *Web-site infrastructure, general Web security issues*

2003-03-26 **new exploit Microsoft Windows 200 flaw Internet Information Server IIS patch fix**

NIPC/DHS

March 24, CNET News.com — Program exploits Windows 2000 flaw.

A Venezuelan security consultant has released a small program designed to compromise Microsoft Internet Information Service servers that haven't had a recent security hole patched. Monday's public release of the program's source code—known in security parlance as an exploit—will allow less technically knowledgeable system administrators to test for the existence of the vulnerability or allow less skillful miscreants to attack servers. "I released (the code) to enlighten the public and to promote system security for administrators unfamiliar with these exploits," said Rafael Nunez, information security consultant for Scientech de Venezuela and a former hacker. The flaw, which Microsoft said could be exploited through the World Wide Web Distributed Authoring and Versioning (WebDAV) component of Internet Information Service (IIS) 5.0, allows an attacker to take control of the server. Microsoft declined to comment on the issue, except to say that customers should patch their systems. Nunez stressed that system administrators need to patch their systems before a virus writer uses the vulnerability as a vector for a computer worm.

Category 23.6 *Web-site infrastructure, general Web security issues*

2003-04-04 **new vulnerabilities software Real RealPlayer Apple Quicktime heap corruption**

NIPC/DHS

April 02, CNET News.com — Holes found in RealPlayer, QuickTime.

There are serious security holes in two popular digital media players: RealNetworks' RealPlayer and Apple Computer's QuickTime. In both cases, updates are available to remedy the problem. RealNetworks is warning that by creating a specifically corrupted Portable Network Graphics file, an attacker could cause "heap corruption." Doing so would allow the attacker to execute code on the victim's machine. The vulnerable software uses an older data-compression library within the RealPix component of the player, leaving the system vulnerable. The vulnerability affected the following versions of the software: RealOne Player, RealOne Player v2 for Windows, RealPlayer 8 for Windows, RealPlayer 8 for Mac OS 9, RealOne Player for Mac OS X, RealOne Enterprise Desktop Manager and RealOne Enterprise Desktop. Meanwhile, security firm iDefense warned this week of an exploitable buffer overflow vulnerability in versions 5.x and 6.0 of Apple's QuickTime Player that could affect computers with Microsoft's Windows. A URL containing 400 characters will overrun the allocated space on the system, allowing the attacker to assume control of the system, iDefense said.

Category 23.6 *Web-site infrastructure, general Web security issues*

2003-04-07 **new vulnerability exploit patch fix Apache Web server denial-of-service**

NIPC/DHS

April 03, — Latest Apache release fixes DOS vulnerability.

The latest release of Apache 2.0, version 2.0.45, fixes a number of security vulnerabilities including an as-yet-undisclosed flaw that could be used to launch a denial of service attack against machines running the Apache Web server, according to information released by the Apache Software Foundation (ASF). Apache 2.0 users are encouraged to upgrade. Other, lower priority security leaks and bug fixes were also included in the 2.0.45 release. However, a known DOS vulnerability that affects those systems running Apache on the OS/2 platform remains open. The latest Apache version was "too important" to delay release until the OS/2 fix could be included, the ASF said. OS/2 users will have to wait for the release of 2.0.46 to get a fix for that problem, the ASF said.

Category 23.6 *Web-site infrastructure, general Web security issues*

2003-04-15 **XML security standard show intergration interoperability**

NIPC/DHS

April 11, IDG News Service — XML security standard touted at show.

A group of application security vendors affiliated with the Organization for the Advancement of Structured Information Standards (OASIS) will next week announce a proposal for an XML standard for application vulnerabilities at the RSA Conference hosted by RSA Security in San Francisco. The group, made up of Citadel Security Software, GuardedNet, NetContinuum, SPI Dynamics and Teros, is promoting the development of the Application Vulnerability Description Language (AVDL), which is intended to standardize information about application vulnerabilities, enabling different products to share vulnerability information in a heterogeneous network environment, according to a statement released by the five companies. If widely adopted, the AVDL standards will enable customers to deploy diverse security technology to protect their network without having to sacrifice integration and interoperability, according to Wes Wasson, chief security strategy officer at NetContinuum.

Category 23.6 *Web-site infrastructure, general Web security issues*

2003-04-24 **new patch exploit fix vulnerability Microsoft security bulletin Internet Explorer browser sofware**

NIPC/DHS

April 23, Microsoft — Microsoft Security Bulletin MS03-015: Cumulative Patch for Internet Explorer.

This cumulative patch eliminates the following four vulnerabilities: 1) A buffer overrun vulnerability in URLMON.DLL; 2) A vulnerability in the Internet Explorer file upload control; 3) A flaw in the way Internet Explorer handles the rendering of third party files; 4) A flaw in the way modal dialogs are treated by Internet Explorer. In addition, this patch includes a fix for Internet Explorer 6.0 SP1 that corrects the method by which Internet Explorer displays help information in the local computer zone. This patch also sets the Kill Bit on the Plugin.ocx ActiveX control in order to ensure that the vulnerable control cannot be reintroduced onto users' systems and to ensure that users who already have the vulnerable control on their system are protected. Like the previous Internet Explorer cumulative patch released with bulletin MS03-004, this cumulative patch will cause window.showHelp( ) to cease to function if you have not applied the HTML Help update. Microsoft has assigned a risk rating of "Critical" to this vulnerability and a patch is available at the Microsoft website.

Category 23.6 *Web-site infrastructure, general Web security issues*

2003-05-01 **crackers wreak havoc physica world ACM conference privacy electronic society web-based order forms google attack**

NewsScan

MALICIOUS CRACKERS COULD WREAK HAVOC IN PHYSICAL WORLD
Researchers participating in a recent ACM conference on privacy in an electronic society have described how automated order forms on the Web could be exploited to send tens of thousands of unwanted catalogs to a business or an individual. The resulting deluge not only would pose an inconvenience to the victim, but likely would swamp the local post office charged with delivery, said Avi Rubin, technical director of the Information Security Institute at Johns Hopkins University. "People have not considered how easily someone could leverage the scale and automation of the Internet to inflict damage on real-world processes." Using Google to locate online order forms and simple software to fill in fields such as "name" and "address," "it could be set up to send 30,000 different catalogs to one person or 30,000 copies of one catalog to 30,000 different recipients," said Rubin. The technique could also be used to exploit the increasingly common Web-based forms used to request repair service, deliveries or parcel pickups. Rubin and his fellow researchers suggested Web sites could take steps to prevent such attacks, including setting up online forms so that they cannot easily be picked up by a search engine, or using HTML coding to create an online form so it no longer contains easily recognized field names, such as "name." Another strategy could be to include a Reverse Turing Test — a step in each form that requires human input. (Science Daily 1 May 2003)

Category 23.6 *Web-site infrastructure, general Web security issues*

2003-05-29 **MS03-018 Microsoft Security Bulletin patches CSS Cross Site Scripting redirection buffer overrun IIS 4.0 5.0 5.1**

NIPC/DHS

May 29, Microsoft — Microsoft Security Bulletin MS03-018: Cumulative Patch for Internet Information Service.

This patch supercedes all previous patches released for IIS 4.0 and IIS 5.0. It also fixes the following vulnerabilities affecting IIS 4.0, 5.0 and 5.1: a Cross-Site Scripting (CSS) vulnerability affecting IIS 4.0, 5.0 and 5.1 involving the error message that's returned to advise that a requested URL has been redirected; a buffer overrun that results because IIS 5.0 does not correctly validate requests for server side includes; a denial of service vulnerability that results because of a flaw in the way IIS 4.0 and 5.0 allocate memory requests when constructing headers to be returned to a web client; a denial of service vulnerability that results because IIS 5.0 and 5.1 do not correctly handle an error condition when an overly long WebDAV request is passed to them. This patch, rated "Important," requires the patch from Microsoft Security Bulletin MS02-050 to be installed.

Category 23.6 *Web-site infrastructure, general Web security issues*

2003-06-04 **MS03-020 cumulative patch internet explorer buffer overflow arbitrary code malicious functionality window.showHelp() update Microsoft Security Bulletin**

NIPC/DHS

June 04, Microsoft — Microsoft Security Bulletin MS03-020: Cumulative Patch for Internet Explorer.

This cumulative patch includes the functionality of all previously released patches for Internet Explorer 5.01, 5.5 and 6.0, and eliminates two vulnerabilities: a buffer overrun vulnerability that occurs because Internet Explorer does not properly determine an object type returned from a web server, and a flaw that results because Internet Explorer does not implement an appropriate block on a file download dialog box. It could be possible for an attacker to exploit this vulnerability to run arbitrary code on a user's system. This cumulative patch will cause window.showHelp( ) to cease to function if you have not applied the HTML Help update. Microsoft has assigned a risk rating of "Critical" to this patch.

Category 23.6 *Web-site infrastructure, general Web security issues*

2003-06-25 **Internet Explorer IE flaw unearth worm microsoft buffer overflow vulnerability BugTraq**

NIPC/DHS

June 25, CNET News.com — IE flaw could unearth worm.

A vulnerability in Microsoft's Internet Explorer could result in the creation of a serious Internet worm, security experts have warned. However, there is no proof that the vulnerability foretells the execution of arbitrary code. The buffer overflow vulnerability is triggered by a malicious Java script that can be embedded in an HTML document. When a Web page or HTML file containing the malicious script is viewed by Internet Explorer, versions 5 and 6, the buffer is overrun and the browser crashes. The code was posted to the BugTraq security mailing list early Sunday morning. Microsoft wasn't pleased with the premature revelation of the vulnerability before its security teams got a chance to look into the matter. There is currently no patch unavailable.

Category 23.6 *Web-site infrastructure, general Web security issues*

2003-07-09 **Apache http server denial service DoS open-source bug fix**

NIPC/DHS

July 09, internetnews.com — DoS holes plugged in Apache HTTP Server.

The Apache Software Foundation on Monday released a new version of its open-source Web server project to plug four potentially serious security holes. The latest update to the Apache 2.0 HTTP Server (version 2.0.47) is described as a security and bug fix release to plug holes that could lead to denial-of-service attacks. The Foundation warned that the SSLCipherSuite directive being used to upgrade from a weak ciphersuite to a strong one could result in the weak ciphersuite being used in place of the strong one. The previous Apache HTTP Server version also contains a bug in the prefork MPM where certain errors returned by accept() on rarely accessed ports could cause temporal DoS. Another DoS security vulnerability, caused when target host is IPv6, was also patched. Apache explained that ftp proxy server can't create IPv6 socket. The Apache Foundation also warned older versions of the server would crash when going into an infinite loop because of too many subsequent internal redirects and nested subrequests.

Category 23.6 *Web-site infrastructure, general Web security issues*

2003-10-20 **Microsoft Internet Explorer buy music online complaint Justice Department**

NewsScan

CHALLENGE TO THE WEB WEAVED BY MICROSOFT
The U.S. Justice Department and 19 states have complained to U.S. District Judge Colleen Kollar-Kotelly about a design feature of Windows that compels consumers who buy music online to use only Microsoft's Internet Explorer browser and guides them to a Microsoft Web site. The dispute may become the first test of the Microsoft antitrust settlement approved by a federal court in October 2002. In response, a Microsoft executive said, "We believe that the use of Internet Explorer by the Shop-for-Music-Online link in Windows is consistent with the design rules established by the consent decree, and we will continue to work with the government to address any concerns. At issue is a design feature in Windows XP called "Shop for Music Online," which lets consumers purchase compact discs from retailers over the Internet, but when consumers click the link to buy music, Windows opens Microsoft's browser software even if consumers have indicated that they prefer using rival browser software. (AP/San Jose Mercury News 20 Oct 2003)

Category 23.6 *Web-site infrastructure, general Web security issues*

2003-11-02 **website abandoned sites weblogs y2k out-of-date content dissapear**

NewsScan

WEB LITTERED WITH ABANDONED SITES
The Web is cluttered with pages and whole sites long ago forgotten by their creators — political campaigns from yesteryear, personal projects that lost their pizzazz, and even Y2K sites that commemorate a catastrophe that never happened. And while it's easy to imagine losing interest in the effort required to update and maintain a Web site, the same phenomenon is evident among the Web's latest obsession — blogging. One study of 3,634 weblogs found that two-thirds had not been updated for at least two months and about 25% hadn't changed since the day they were launched. "Some would say, 'I'm going to be too busy but I'll get back to it,' but never did," says Jeffrey Henning, chief technology officer with Perseus Development Corp., which conducted the study. But while some users resent slogging through out-of-date content, others complain that sites disappear too quickly. "I do hear pretty frequently not so much that there's deadwood, but that sites go away without a trace," says Steve Jones, a communications professor at the University of Illinois at Chicago. (AP/Tampa Bay Online 2 Nov 2003)

Category 23.6 *Web-site infrastructure, general Web security issues*

2003-11-13 **France Telecom insecure Website Internet security**

RISKS 23 3

A heavily used RISKY website: France Telecom

Contributor Peter Kaiser complains about the insecure French Telecom website, francetelecom.com. Kaiser found that this Website requested sensitive personal and financial information despite "no outward indication of security -- that is, no "locked/unlocked" symbol." When he approached a France Telecom service rep Kaiser was told: "Thousands of orders are placed on francetelecom.com every day, we have…not been informed of problems encountered as a result of orders made on our site." Kaiser fears that such insecure e-commerce is a risk to both France Telecom and its customers. But he is consoled that identity theft cases as a result of France Telecom's practice will not be taken lightly by European courts.

Category 23.6 *Web-site infrastructure, general Web security issues*

2003-11-13 **new critical vulnerability Microsoft security bulletin Internet Explorer browser software patch fix exploit**

NIPC/DHS

November 11, Microsoft — Microsoft Security Bulletin MS03-048: Cumulative Security Update for Internet Explorer.

There are three vulnerabilities that involve the cross-domain security model of Internet Explorer, which keeps windows of different domains from sharing information. These vulnerabilities could result in the execution of script in the My Computer zone. After the user has visited a malicious Website or viewed a malicious HTML e-mail message an attacker who exploited one of these vulnerabilities could access files on a user's system, and run arbitrary code on a user's system in the security context of the user. Another vulnerability involves the way zone information is passed to an XML object within Internet Explorer. This vulnerability could allow an attacker to read local files on a user's system. Finally, there is a vulnerability that involves performing a drag-and-drop operation during dynamic HTML (DHTML) events in Internet Explorer. This vulnerability could allow a file to be saved in a target location on the user's system if the user clicks a link. No dialog box would request that the user approve this download. Microsoft has assigned a risk rating of "Critical" to this issue and recommends that system administrators install this patch immediately.

Category 23.6 *Web-site infrastructure, general Web security issues*

2003-11-25 **Web browser software Opera security flaw vulnerability exploit**

NIPC/DHS

November 24, CNET News.com — Opera update seals security holes.

A new version of Opera, released Friday, November 21, fixes two vulnerabilities in the Web browser. The vulnerabilities, disclosed to the BugTraq security mailing list, allow rogue Web sites to take control of a victim's computer by exploiting weaknesses in the way the browser handles "skin" files, or configuration files that can change the look of a program. An advisory, written by Jouko Pynnonen of Finland, describes scenarios that would allow an attacker to seize control of systems running Opera, all of which require some degree of user interaction to be successfully exploited. "In order to be exploited, these vulnerabilities require the victim to visit a Web page created by a malicious user," he wrote. Though Pynnonen says one vulnerability affects Windows systems only, the second vulnerability, a buffer overflow, will allow an attacker to take control of Linux-based systems. "The directory traversal problem doesn't exist on Linux...Other versions weren't tested," the advisory read, noting also that "the buffer overflow can be produced on Linux, too."

Category 23.6 *Web-site infrastructure, general Web security issues*

2003-11-28 **vulnerability scripting Internet Explorer browser software hacker**

NIPC/DHS

November 25, The Register — Scripting flaws pose severe risk for IE users.

A set of five unpatched scripting vulnerabilities in Internet Explorer creates a mechanism for hackers to compromise targeted PCs. The vulnerabilities, unearthed by Chinese security researcher Liu Die Yu along with Proof of Concept exploits, enable malicious Websites and viruses to bypass the security zone settings in IE6. Used in combination, the flaws might be exploited to seize control of vulnerable PCs. Microsoft has yet to patch the flaws. But users can protect themselves against the flaws by disabling active scripting or by using an alternative browser. Thomas Kristensen of Secunia said the five distinct vulns could used in combination to install executables. Secunia advises all IE users to disable active scripting. The drawback of this workaround is that with some Websites certain functions won't work unless scripting is enabled. IE users should define any sites they need to use as trusted so that they can continue to use scripting on those sites alone, Kristensen said. The original advisory is available here:
http://www.secunia.com/advisories/10289/

Category 23.6 *Web-site infrastructure, general Web security issues*

2003-12-12 **new vulnerability flaw exploit Internet Explorer browser software**

NIPC/DHS

December 12, eWEEK — Internet Explorer spoofing vulnerability found.

Security researchers confirmed a vulnerability in Internet Explorer 6 Tuesday, December 9, that could let an attacker display a fake URL in the browser's address bar in an attempt to disguise the real domain, an advisory from security company Secunia Ltd said. Using the security hole, an attacker could trick users into providing sensitive information or download malicious software by leading them to think that they are visiting a trusted site, the advisory said. A Microsoft spokesperson on Wednesday said that the company knows of no exploits of the reported hole or of any users being affected but said in a statement that it is "aggressively investigating the public reports." Microsoft may provide a fix through its monthly patch release cycle or a separate patch, depending on the outcome of the investigation, the spokesperson said. The Secunia advisory is available here:
http://www.secunia.com/advisories/10395

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-01-14 **patch flaw vulnerability fix Sun ONE buffer overflow**

NIPC/DHS; http://www.esecurityplanet.com/prodser/article.php/3298031

January 12, esecurityplanet.com — Buffer overflow plugged in Sun ONE web server.

Sun Microsystems on Monday, January 12, warned of a buffer overflow vulnerability in its Sun ONE/iPlanet Web Server product. The firm said the flaw could be exploited by a remote user to crash the Web server, which is a type of denial-of-service attack. Independent research firm Secunia has rated the security hole as "moderately critical." The vulnerability affects the Sun ONE/iPlanet Web Server 6.0 Service Pack 5 and earlier versions on the HP-UX platform. Sun has issued a new service pack to fix the flaw, noting that there are no workarounds. The susceptible products are a crucial part of Sun's Web services initiative which falls under Sun Open Net Environment (Sun ONE) brand. The Sun ONE brand includes the Sun ONE Web Server, Sun ONE Portal Server, Sun ONE Application Server, Sun ONE Directory Server, Sun ONE Identity Server, Sun ONE Messaging Server and the Sun ONE Integration Server (all formerly iPlanet products). A service pack is available online: http://wwws.sun.com/software/download/products/3f186391.html

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-01-23 **new flaw vulnerability patch fix OpenSSL protocol SSL Sun**

NIPC/DHS; http://www.esecurityplanet.com/prodser/article.php/3301661

January 21, eSecurityPlanet — Sun Cluster vulnerable to OpenSSL flaw.

Sun Microsystems on Wednesday, January 21, warned that systems running Sun Cluster 3.x with SunPlex Manager configured were at risk of takeover because of known flaws in the OpenSSL protocol. In a security advisory, Sun recommended that the SunPlex Manager be disabled until a comprehensive patch is ready, warning that exploitation of the vulnerability could lead to arbitrary code execution and denial-of-service (DoS) scenarios. Independent research firm Secunia is rating the vulnerability as "moderately critical." The confirmation of the system access and DoS vulnerabilities comes more than three months after the OpenSSL flaw was made public. Last October, the OpenSSL Project released new versions of its implementation of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols to plug multiple vulnerabilities. All versions of OpenSSL up to and including 0.9.6j and 0.9.7b and all versions of SSLeay were updated. The OpenSSL project said any application that makes use of OpenSSL's ASN1 library to parse untrusted data was also susceptible. The OpenSSL holes carry a "highly critical" rating. More information can be found at http:/sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/57475

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-02-04 **Microsoft Internet Explorer software patch inconsistent user complaint**

DHS IAIP Daily; http://news.zdnet.co.uk/internet/security/0,39020375,3914548
7,00.htm

February 04, ZDNet — Users report inconsistent results from latest IE patch.

Microsoft's latest security patch for its Internet Explorer (IE) browser doesn't always work, users report. The fix was supposed to disable a commonly used feature that allows usernames and passwords to be transferred within a URL. However, some users have found that even after the patch is deployed, the "feature" is still active. Microsoft said it has not as yet received any complaints from users experiencing the problems, but tests by ZDNet UK confirm that even after the latest patch is applied, IE still allows URLs containing password and user information to access Internet resources. However, at this stage it is still unclear why some users find the patch works, while others are still left vulnerable.

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-05-18 **WS-I SOAP Web services security**

DHS IAIP Daily; http://www.esecurityplanet.com/trends/article.php/3355231

May 18, eSecurity Planet — WS-I clears basic security hurdle.

Web services security, a bugbear in the adoption of distributed computing architectures, is one step closer to being finalized. The Web Services Interoperability Organization (WS-I) said it has finished its Basic Security Profile Working Group Draft and is making it available in order to solicit feedback from the Web services community. The Basic Security Profile addresses transport security, SOAP messaging security and other security considerations as well as the interoperability characteristics of two main technologies: HTTP over Transport Layer Security and Web Services Security: SOAP Message Security. Naturally, the Basic Security Profile is expected to synch with other WS-I profiles and work with some existing specifications used to provide security, including the OASIS Web Services Security 1.0 specification, which passed muster last month. When the document is cleaned up and finalized, possibly later this year, it is expected to usher in a raft of new customers to Web services, and by extension service-oriented architectures (SOA).

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-07-29 **phpMyAdmin PHP MySQL administration Web development vulnerability**

DHS IAIP Daily; http://www.securityfocus.com/bid/10629/info/

July 29, SecurityFocus — phpMyAdmin multiple input validation vulnerabilities.

phpMyAdmin is prone to multiple vulnerabilities. The issues result from insufficient sanitization of user-supplied data. By constructing a URI request for the phpMyAdmin 'left.php' script an attacker may specify and add an arbitrary SQL server. A remote attacker may exploit this vulnerability to replace server configurations and as a result introduce a malicious SQL server into the phpMyAdmin controlled server list. It is also reported that a malicious database table name beginning with """ will escape the quotes in a PHP eval() statement and will thereby permit an attacker to execute arbitrary PHP code. The vendor has released version 2.5.7, patch level 1 addressing this vulnerability: http://sourceforge.net/index.php

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-07-30 **spam anti-spam pop-up blocker Federal Trade Commission FTC settlement extortion**

NewsScan

POP-UP COMPANY AGREES TO PIPE DOWN

D Squared Solutions, a San Diego company founded by two college sudents, has settled with the Federal Trade Commission after agreeing to desist mass-mailing pop-up ads using the Messenger function enabled on many Windows operating systems. D Squared has also agreed to stop peddling
software that would have blocked the very ads it was sending. The company's founders have not admitted any wrongdoing and face no penalties. Their lawyers claimed the pair were not trying to extort consumers with their ads and one attorney suggested that such ads are "annoyances you have to deal with in a free society." (AP 30 July 2004)

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-08-02 **IBM directory server Tivoli vulnerability ldap user exploit fix published**

DHS IAIP Daily; http://www.securityfocus.com/bid/10841

August 02, SecurityFocus — IBM Tivoli Directory Server LDACGI Directory Traversal Vulnerability.

IBM Tivoli Directory Server is reported to contain a directory traversal vulnerability in its Web front-end application. This issue presents itself due to insufficient sanitization of user-supplied data. This issue allows remote attackers to view potentially sensitive files on the server that are accessible to the 'ldap' user. This may aid an attacker in conducting further attacks against the vulnerable computer. A fix for Versions 3.2.2 is available here: http://www-1.ibm.com/support/docview.wss?uid=swg24006917 A fix for Version 4.1 is available here: http://www-1.ibm.com/support/docview.wss?uid=swg24006209

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-08-03 **Web server vulnerability note US-CERT BlackJumboDog**

DHS IAIP Daily; http://www.kb.cert.org/vuls/id/714584

August 03, US-CERT — Vulnerability Note VU#714584: BlackJumboDog contains a boundary error in the handling of FTP commands.

BlackJumboDog is a multi-function server for Microsoft Windows, providing FTP, Email, Web, and Proxy services. It is reported that version 3.6.1 contains a buffer overflow vulnerability. BlackJumboDog fails to check the length of FTP commands passed to it. Using specially crafted FTP commands, a remote user can trigger a buffer overflow condition possibly leading to code execution on the server. This issue has been resolved in version 3.6.2 of BlackJumboDog: http://homepage2.nifty.com/spw/software/bjd/download.html

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-08-04 **Mozilla Firefox Thunderbird vulnerabilities**

DHS IAIP Daily; http://secunia.com/advisories/10856/

August 04, Secunia — Mozilla multiple vulnerabilities.

The vendor has released details about some older vulnerabilities in Mozilla, Mozilla Firefox, and Thunderbird. These can potentially be exploited by malicious people to conduct spoofing attacks, compromise a vulnerable system, or cause a DoS (Denial of Service). The vulnerabilities have reportedly been fixed in: Mozilla 1.7 and higher, Firefox 0.9 and higher, and Thunderbird 0.7 and higher.

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-08-04 **portable network graphics PNG library vulnerability open source US-CERT**

DHS IAIP Daily; http://www.us−cert.gov/cas/techalerts/TA04−217A.html

August 04, US-CERT — Technical Cyber Security Alert TA04-217A: Multiple Vulnerabilities in libpng.

The Portable Network Graphics (PNG) image format is used as an alternative to other image formats such as the Graphics Interchange Format (GIF). The libpng is a popular reference library available for application developers to support the PNG image format. Several vulnerabilities exist in the libpng library, the most serious of which could allow a remote attacker to execute arbitrary code on an affected system. Users should apply the appropriate patch or upgrade as specified by vendor. More detailed information about these vulnerabilities is available in individual vulnerability notes on the US-CERT Website.

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-08-04 **PHP Bulletin Board phpBB SQL injection vulnerability query patch**

DHS IAIP Daily; http://www.securityfocus.com/bid/10868/info/

August 04, SecurityFocus — phpBB Fetch All SQL injection vulnerability .

It is reported that phpBB Fetch All is susceptible to an SQL injection vulnerability. This issue is due to a failure of the application to properly sanitize user-supplied input before using it in an SQL query. The successful exploitation of this vulnerability depends on the implementation of the web application that includes phpBB Fetch All as a component. It may or may not be possible to effectively pass malicious SQL statements to the underlying function. Successful exploitation could result in compromise of the application, disclosure or modification of data or may permit an attacker to exploit vulnerabilities in the underlying database implementation. The vendor has released version 2.0.12 to address this issue: http://prdownloads.sourceforge.net/phpbbfetchall/phpbb_fetch _all-2.0.12.zip?downloa

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-08-04 **PuTTY telnet SSH software vulnerability malicious server connection**

DHS IAIP Daily; http://secunia.com/advisories/12212/

August 04, Secunia — PuTTY unspecified system compromise vulnerability.

A vulnerability in PuTTY can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to an unspecified error and may allow execution of arbitrary code on a user's system. Successful exploitation requires that a user has been tricked into connecting to a malicious server. Users should upgrade to version 0.55.

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-08-05 **Opera Internet browser flaw computer hijack e-mail exposure**

DHS IAIP Daily; http://www.esecurityplanet.com/patches/article.php/3391281

August 05, internetnews.com — Critical flaws spoil Opera tune.

Alternative Web browser firm Opera Software has issued a fix for its Opera browser after a security research firm reported a potentially dangerous security bug. Opera rolled out a new version (7.54) and confirmed that users of previous versions were at risk of computer hijack. GreyMagic, the research outfit that discovered the vulnerabilities, said a successful attack would allow read-access to files on the victim's file system and read access to lists of files and folders on the victim's computer. Malicious hackers could also gain access to read incoming and outgoing e-mails on Opera's M2 mail program, which is built into the browser. The flaws also could result in cookie theft, URL-spoofing for phishing attacks and the spillage of a user's browsing history. GreyMagic also released a proof-of-concept demonstration that presents the user's files and directories in an Explorer-like manner, allowing the user to browse his/her own file system using the vulnerability.

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-08-05 **Board Power Internet forum technology vulnerability cross-site scripting attack**

DHS IAIP Daily; http://www.kb.cert.org/vuls/id/744590

August 05, US-CERT — Vulnerability Note VU#744590: Board Power forum contains cross-site scripting vulnerability in the 'action' parameter of 'icq.cgi'.

Board Power is a forum application available for multiple operating systems. It is reported that Board Power v2.04 PF contains a cross-site scripting vulnerability. Board Power fails to filter malicious content passed into the "action" parameter of icq.cgi. Other versions may be affected. It appears that Board Power is no longer supported and has not been updated since 2000 by the developers (The Webmaster Guide, Inc.). The victim will be presented with information which the compromised site did not wish their visitors to be subjected. This could be used to "sniff" sensitive data from within the web page, including passwords, credit card numbers, and any arbitrary information the user inputs. Likewise, information stored in cookies can be stolen or corrupted. US-CERT is currently unaware of a practical solution to this problem.

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-08-10 **Apache Webserver vulnerabilities HP VirtualVault HP11 Webproxy patch issued**

DHS IAIP Daily; http://secunia.com/advisories/12246

August 10, Secunia — HP VirtualVault / Webproxy multiple vulnerabilities in Apache.

HP has confirmed some vulnerabilities in Apache affecting HP VirtualVault and HP 11 Webproxy, which can be exploited by malicious people to cause a DoS (Denial of Service), bypass security restrictions, or compromise a vulnerable system. The vulnerabilities affect servers running HP-UX release B.11.04 with VirtualVault A.04.50 - A.04.70 or Webproxy A.02.00 - A.02.10 installed. Install patches available at: http://itrc.hp.com

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-08-10 **Microsoft security bulletin Exchange Server vulnerability cross site scripting spoofing**

DHS IAIP Daily; http://www.microsoft.com/security/bulletins/200408_exchange.
mspx

August 10, Microsoft — Microsoft Security Bulletin MS04-026: Vulnerability in Exchange Server 5.5 Outlook Web Access Could Allow Cross-Site Scripting and Spoofing Attacks.

A cross-site scripting and spoofing vulnerability exists in Outlook Web Access for Exchange Server 5.5 that could allow an attacker to convince a user to run a malicious script. An attacker who successfully exploited the vulnerability could manipulate Web browser caches and intermediate proxy server caches, and put spoofed content in those caches. They may also be able to exploit the vulnerability to perform cross-site scripting attacks. Microsoft has assigned a risk rating of "Moderate" to this issue and recommends that customers consider applying the security update. Customers who have customized any of the ASP pages that are listed in the File Information section in this document should back up those files before they apply the update because those ASPs will be overwritten when the update is applied. Any customizations would then have to be reapplied to the new ASP pages.

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-08-13 **content management system JetboxOne vulnerability database information disclosure vulnerability US-CERT**

DHS IAIP Daily; http://www.kb.cert.org/vuls/id/586720

August 13, US-CERT — Vulnerability Note VU#586720: JetboxOne leaves account database unencrypted.

JetboxOne is an open-source content management system that is written in PHP. An information disclosure vulnerability exists because JetboxOne does not encrypt account information stored in the admin (user) and webuser (standard user) tables of a MySQL database. Any user with the ability to query the database may be able to view confidential account information. This may lead to unauthorized access to other accounts. US-CERT is currently unaware of a practical solution to this problem.

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-08-13 **content management system JetboxOne vulnerability code execution vulnerability US-CERT**

DHS IAIP Daily; http://www.kb.cert.org/vuls/id/417408

August 13, US-CERT — Vulnerability Note VU#417408: JetboxOne may allow unauthorized users to execute arbitrary code.

JetboxOne, an open-source content management system, could allow an attacker with "AUTHOR" privileges to upload arbitrary files to the image folder via the upload image control. The vulnerability exists because the type of file being uploaded is not verified as a valid image file e.g. GIF, JPEG. Once uploaded, the attacker is then able to request the file, which will be interrpreted by the JetboxOne application. Based on the file type this may permit a malicious user to execute the arbitrary code on the compromised system. Currently, the vulnerability has been demonstrated on version 2.0.8. However, it may also exist in previous versions, but they are as of yet untested. US-CERT is currently unaware of a practical solution to this problem.

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-08-16 **Website services security problems XML code authentication hacking**

DHS IAIP Daily;
http://www.computerworld.com/developmenttopics/development/s
tory/0,10801,95197,00.html

August 16, Computerworld — Web services security: trouble in transit.

The shareable design of Web services, which gives companies the benefit of easily exchanging data and applications with business partners, also makes them vulnerable to security breaches. Hackers have found ways to tweak the XML code used to tag the data so activity that's actually an attack appears to be valid. According to experts, hackers have three methods for breaching Web services and XML security: identity-based attacks, in which a hacker poses as an authorized user to gain access to Web services; malicious-content attacks, in which an intruder forces a Web server to perform an unauthorized activity; and operational attacks, in which a hacker manipulates an XML message to tie up server resources. But although the methods are known, safeguarding Web services is difficult because multiple elements must be locked down--the servers, the messages and the applications. Companies must first secure their Web servers and then decide which business partners and employees will have access to them, how they'll connect to them and which authentication method to use.

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-08-20 **MySQL buffer overflow vulnerability DNS lookup**

DHS IAIP Daily; http://www.zone−h.org/advisories/read/id=5365

August 20, zone-h — MySQL "mysql_real_connect" buffer overflow vulnerability.

A vulnerability in MySQL could potentially allow malicious people to compromise a vulnerable system. The "mysql_real_connect()" function doesn't properly verify the length of IP addresses returned by a reverse DNS lookup of a hostname. This could potentially be exploited to cause a buffer overflow and execute arbitrary code. Successful exploitation requires that the attacker is able to return a malicious DNS reply when a MySQL user connects to a server. This has been reported in MySQL 4.0.20 and prior. It has been reported that this can't be exploited on the Linux and OpenBSD platforms. This issue will be fixed in the upcoming 4.0.21. Original Advisory: http://bugs.mysql.com/bug.php?id=4017

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-08-20 **Mozilla buffer overflow vulnerability POP3 protocol**

DHS IAIP Daily; http://www.kb.cert.org/vuls/id/561022

August 20, US-CERT — Vulnerability Note VU#561022: Mozilla contains a buffer overflow in the SendUidl() function.

Post Office Protocol Version 3 (POP3) is a mail protocol that provides a means for retrieving email from a remote server. This protocol is supported by Mozilla, Firefox, and Thunderbird. These clients contain a vulnerability that allows malformed POP3 responses to trigger a buffer overflow condition in the SendUidl() function. Such responses can be sent by a remote POP3 server and could result in arbitrary code execution. Exploitation of this vulnerability would require a user to connect to a malicious POP3 server. This issue has been resolved in Mozilla 1.7, Firefox 0.9, and Thunderbird 0.7.2:
http://www.mozilla.org/projects/security/known-vulnerabiliti es.html

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-08-23 **buffer overflow Netscape Network Security Services NSS suite Secure Sockets Layer SSL**

DHS IAIP Daily; http://xforce.iss.net/xforce/alerts/id/180

August 23, Internet Security Systems — Netscape NSS Library remote compromise.

A vulnerability exists in the Netscape Network Security Services (NSS) library suite which may result in remote compromise of products making use of this library for Secure Sockets Layer (SSL) communication. If the SSLv2 protocol is enabled on vulnerable servers, a remote unauthenticated attacker may trigger a buffer overflow condition and execute arbitrary code. This has the potential to result in complete compromise of the target server, and exposure of any information held therein. SSL is often used to secure sensitive or valuable communications, making this a high-value target for attackers. A vendor-supplied update for the NSS library is available: ftp.mozilla.org/pub/mozilla.org/security/nss/releases/NSS_3_9_2_RTM

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-08-23 **Mozilla Firefox Thunderbird vulnerability X.509 certificate verification failure**

DHS IAIP Daily; http://www.kb.cert.org/vuls/id/784278

August 23, US-CERT — Vulnerability Note VU#784278: Mozilla allows certificate to be imported even when the DN is the same as that of a built-in CA root certificate.

Mozilla version 1.7.7 fails to verify that the Distinguished Name (DN) of an X.509 certificate is unique when importing it. A denial of service occurs when Mozilla imports a specially crafted self-signed certificate that has the same DN as an existing Certificate Authority (CA) root certificate. Exploitation of this vulnerability can be automated causing the certificate to be imported without any user intervention. A remote attacker could cause a denial of service against the certificate store, preventing the user from accessing SSL websites. This issue has been resolved in Mozilla 1.7.2, Firefox 0.9.3, and Thunderbird 0.7.3: http://www.mozilla.org/projects/security/known-vulnerabilities.html

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-08-24 **Sun Solaris Apache vulnerabilities denial of service DoS code execution attack**

DHS IAIP Daily; http://sunsolve.sun.com/pub−cgi/retrieve.pl?doc=fsalert/5762 8

August 24, Sun Microsystems — Sun Solaris multiple Apache vulnerabilities.

Multiple vulnerabilities exist in Apache for Solaris, which can be exploited to bypass certain security restrictions, cause a DoS (Denial of Service), or potentially compromise a vulnerable system. The Apache HTTP process normally runs as the unprivileged uid "nobody." The ability to execute arbitrary code as the unprivileged uid "nobody" may lead to modified web content, denial of service, or further compromise. While a final vendor solution is pending, patches are available at: http://sunsolve.sun.com/tpatches

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-09-02 **Opera 7.23 Internet Web browser embed tag HTML crash vulnerability**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Sep/1011142.html

September 02, SecurityTracker — Opera 'embed' tag error lets remote users crash the browser.

A vulnerability exists in the Opera browser 7.23 build 3227 in the processing of the 'embed' tag. A remote user can create HTML that, when loaded by the target user, will cause the target user's browser to crash. Update to version 7.51: http://www.opera.com/

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-09-02 **secure shell OpenSSH SSH default configuration unsafe CVS**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Sep/1011143.html

September 02, SecurityTracker — OpenSSH default configuration may be unsafe when used with anonymous SSH services.

A configuration vulnerability exists in the default configuration of OpenSSH 3.9 and prior when used with anonymous public services such as anonymous CVS. A remote user can connect to arbitrary hosts via the target service. Affected sites can place the following statement in their '/etc/ssh/sshd_config' configuration file to prevent attacks: AllowTcpForwarding no

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-09-03 **Juniper Network NetScreen IDP SSH server file overwrite vulnerability secure copy scp**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Sep/1011144.html

September 03, SecurityTracker — Juniper Networks NetScreen-IDP may let remote SSH Servers overwrite files in certain cases.

A vulnerability exists in Juniper Networks NetScreen IDP that could allow a remote SSH server to overwrite arbitrary files on the target system in certain situations. This is due to an underlying directory traversal vulnerability in scp, the report said. This could lead to a remote SSH server being able to overwrite arbitrary files on the target system in certain situations. Original advisory and resolutions: http://www.juniper.net/support/security/alerts/adv59739.txt

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-09-15 **Internet Web browser session fixation attack vulnerability no solution**

DHS IAIP Daily; http://www.westpoint.ltd.uk/advisories/wp−04−0001.txt

September 15, Westpoint Security Advisory — Several Internet browsers have session fixation vulnerability.

A vulnerability was reported in Microsoft Internet Explorer, KDE Konqueror, Mozilla Firefox, and Opera that may allow a remote user to set cookies on via a non-secure server to be sent to a secure server as part of a Session Fixation Attack. This flaw may allow remote users to hijack a target user's session. No solution is currently available; refer to Westpoint Security Advisory for workarounds.

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-09-20 **Sun Java NSS library heap buffer overflow SSLv2 vulnerability update issued**

DHS IAIP Daily; http://secunia.com/advisories/12599

September 20, Secunia — Sun Java Enterprise System NSS library vulnerability.

Sun has acknowledged a vulnerability in the NSS library included with Sun Java Enterprise System. This vulnerability was originally reported on August 25 and is caused due to a boundary error within the parsing of records during SSLv2 connection negotiation. The vulnerability can be exploited to cause a heap-based buffer overflow by sending a specially crafted client hello message with an overly long record. Successful exploitation allows execution of arbitrary code with the privileges of an application linked to the vulnerable library. Original advisory and workaround: http://sunsolve.sun.com/search/document.do?assetkey=1-26-576 43-1

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-09-30 **OpenSSL temporary file creation vulnerability update issued**

DHS IAIP Daily; http://www.securityfocus.com/bid/11293

September 30, SecurityFocus — OpenSSL unspecified insecure temporary file creation vulnerability.

OpenSSL is affected by an unspecified insecure temporary file creation vulnerability. This issue is likely due to a design error that causes the application to fail to verify the existance of a file before writing to it. Updates available at: ftp://ftp.trustix.org/pub/trustix/updates/

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-10-19 **Microsoft Internet Explorer vulnerabilities code execution privilege escalation update Windows XP SP2**

DHS IAIP Daily; http://www.us−cert.gov/cas/techalerts/TA04−293A.html

October 19, US-CERT — Technical Cyber Security Alert TA04-293A: Multiple Vulnerabilities in Microsoft Internet Explorer.

Microsoft Internet Explorer (IE) contains multiple vulnerabilities, the most severe of which could allow a remote attacker to execute arbitrary code with the privileges of the user running IE. Microsoft Security Bulletin MS04-038 describes a number of IE vulnerabilities, including buffer overflows, cross-domain scripting, spoofing, and "drag and drop." The impacts of these vulnerabilities vary, but an attacker may be able to execute arbitrary code with the privileges of the user running IE. Solutions: Apply the appropriate patch as specified by Microsoft Security Bulletin MS04-038; disable Active scripting and ActiveX controls; upgrade to Windows XP Service Pack 2. Microsoft Security Bulletin MS04-038: http://www.microsoft.com/technet/security/bulletin/ms04-038. mspx

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-10-27 **website blocking Bush foreign access controls**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A2668-2004Oct27.html

BUSH WEB SITE BLOCKS FOREIGN VISITORS

The Bush-Cheney campaign has cut off access to its Web site by anyone outside the U.S. or Canada. Instead, those visitors will see the message: "Access denied. You don't have permission to access www.georgewbush.com on this server." The move comes a week after a crippling hacker attack that took down the Web site for six hours. Security experts say that while it's not usual for Web sites to block traffic from specific Internet addresses or from certain countries notorious for churning out spam, the Bush-Cheney campaign's move is probably unprecedented. "I've never heard of a site wholesale blocking access from the rest of the world," says Johannes Ulrich, CTO for the SANS Internet Storm Center. "I guess they decided it just wasn't worth the trouble to leave it open to foreign visitors." Jonah Sieger, a founding partner for Connections Media, which does consulting work with Democratic candidates, says it doesn't make sense for the Bush-Cheney folks to "consciously block access to anybody. Maybe the next thing they'll try is to block Democrats and people in blue states from coming to the site." (Washington Post 27 Oct 2004)

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-11-01 **browsers Internet Explorer Firefox Safari Mozilla Opera study**

NewsScan; http://news.com.com/Study+Firefox+still+gaining+on+Internet+Explorer/2100-1032_3-5435176.html

IE LOSING GROUND TO OPEN SOURCE BROWSERS

Microsoft's Internet Explorer browser is still the overwhelming market leader, but the percentage of Americans using open-source alternatives Mozilla and Firefox inched up to 6% in October from 3.5% in June. Apple's Safari and the Opera browsers combined were employed by just a little over 1% of users, according to online research firm WebSideStory. The results were gleaned by sensors embedded on major Web sites that identified which browsers visitors were using to access the sites. And although Mozilla and Firefox constitute a miniscule portion of the browser market, some analysts say their steady rise may signal a trend. "What we're seeing is (Mozilla and Firefox) looking more like a vanguard than a flash in the pan," says WebSideStory analyst Geoff Johnston. (CNet News.com 1 Nov 2004)

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-11-04 **Apache Web server software Space Headers denial of service DoS vulnerability update issued**

DHS IAIP Daily; http://secunia.com/advisories/13045/

November 04, Secunia — Apache "Space Headers" denial of service vulnerability.

A vulnerability has been discovered in Apache, which can be exploited by malicious people to cause a DoS (Denial of Service). The vulnerability is caused due to an error in the parsing routine for headers with a large amount of spaces. This can be exploited by sending some specially crafted requests with a large amount of overly long headers containing only spaces. The vulnerability has been fixed in version 2.0.53-dev.

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-11-09 **Microsoft Internet Explorer URL Handler vulnerability Windows XP SP2 update**

DHS IAIP Daily; http://secunia.com/advisories/13124/

November 09, Secunia — Microsoft Internet Explorer "res:" URI Handler file identification vulnerability.
A vulnerability has been discovered in Internet Explorer, which can be exploited by malicious sites to detect the presence of local files. An "Access is Denied" error will be returned if a site in the "Internet" zone tries to open an existing local file in the search window using the "res:" URI handler. This can be exploited to determine the presence of specific programs or files in the system directories and on the desktop. The vulnerability has been confirmed on a fully patched system with Internet Explorer 6.0 and Microsoft Windows XP SP1. The vulnerability does not affect systems running Windows XP with SP2 installed.

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-11-10 **spoofing vulnerability Microsoft Internet Security and Acceleration ISA server 200 Proxy 2.0 update issued**

DHS IAIP Daily; http://www.microsoft.com/technet/security/bulletin/ms04−039. mspx

November 10, Microsoft — Spoofing vulnerability in Microsoft Servers.

A spoofing vulnerablity exists in Microsoft Internet Security and Acceleration (ISA) Server 2000 and Microsoft Proxy Server 2.0 that could enable an attacker to spoof trusted Internet content. Users could believe they are accessing trusted Internet content when in reality they are accessing malicious Internet content, for example a malicious Website. Microsoft rates this vulnerability as Important and recommends users install updates described in Microsoft Security Bulletin MS04-039 available through the Source link below.

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-11-10 **Microsoft Internet Explorer IE buffer overflow vulnerability code execution attack Windows XP SP2 update**

DHS IAIP Daily; http://www.uscert.gov/cas/techalerts/TA04−315A.html

November 10, US-CERT — Technical Cyber Security Alert TA04-315A: Buffer Overflow in Microsoft Internet Explorer.

Microsoft Internet Explorer (IE) 6.0 and later contain a buffer overflow vulnerability that could allow a remote attacker to execute arbitrary code with the privileges of the user running IE. A buffer overflow vulnerability exists in the way IE handles the SRC and NAME attributes of various elements, including FRAME, IFRAME, and EMBED. Because IE fails to properly check the size of the NAME and SRC attributes, a specially crafted HTML document can cause a buffer overflow in heap memory. Reports indicate that this vulnerability is being exploited by malicious code propagated via e-mail. IE opens and displays an HTML document that exploits the vulnerability. This malicious code may be referred to as MyDoom or Bofra. Until a complete solution is available from Microsoft, consider the following workarounds: install Windows XP SP2 (SP2 does not appear to be affected by this vulnerability), disable Active scripting, do not follow unsolicited links, read and send e-mail in plain text format, and maintain updated anti-virus software.

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-11-11 **phone companies cybersecurity AT&T Sprint network security programs filtering viruses**

NewsScan; http://online.wsj.com/article/0

PHONE COMPANIES TACKLE CYBERSECURITY

As owners of some of the worlds biggest Internet conduits, telephone companies like AT&T and Sprint are in a prime position to monitor Internet activity and stop mischief makers long before they reach the desktops of corporate customers. AT&T recently launched a network security system called Internet Protect and Sprint offers a similar service called IP Defender. Meanwhile, Internet security firm McAfee is marketing a "Clean Pipes" service designed to help carriers purge attacks as they traverse carrier networks. Other big players in the cybersecurity realm include IBM, Symantec and VeriSign, and equipment makers like Cisco and Juniper Networks are embedding security features into their data-routing gear as well. A recent study by Symantec shows a fourfold increase in the number of new viruses attacking Windows computers, to 4,496 in the first half of 2004 -- the largest increase the company has ever documented. Based on numbers like that, Yankee Group predicts that the managed security services market will expand from $1.5 billion in 2002 to $3.7 billion in 2008. (Wall Street Journal 11 Nov 2004)

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-11-14 **Microsoft Internet Explorer Windows XP SP2 vulnerability code execution attack no update issued**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Nov/1012234.html

November 14, SecurityTracker — Microsoft Internet Explorer on XP SP2 remote user vulnerability.

A remote user can bypass the file download security mechanism in Windows XP SP2 and can execute arbitrary scripting code in the local computer zone to take full control of the target user's system. No solution is currently available.

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-11-18 **Microsoft Internet Explorer vulnerabilities Windows XP SP2 no update**

DHS IAIP Daily; http://secunia.com/advisories/13203/

November 18, Secunia — Microsoft Internet Explorer vulnerabilities.

Two vulnerabilities have been reported in Internet Explorer, which can be exploited by malicious people to bypass a security feature in Microsoft Windows XP SP2 and trick users into downloading malicious files. 1) Microsoft Windows XP SP2 has a security feature which warns users when opening downloaded files of certain types. The problem is that if the downloaded file was sent with a specially crafted "Content-Location" HTTP header in some situations, then no security warning will be given to the user when the file is opened. 2) An error when saving some documents using the Javascript function "execCommand()", can be exploited to spoof the file extension in the "Save HTML Document" dialog. There is no solution at this time.

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-11-20 **Microsoft Internet Explorer IE unauthorized download vulnerability no update issued**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Nov/1012288.html

November 20, SecurityTracker — Microsoft IE Custom 404 error message and execCommand SaveAs permit unauthorized downloads.

A remote user can create HTML that, when loaded by the target user, will prompt the user to download a file but will bypass the XP SP2 executable download warning messages. A remote user can invoke the execCommand 'SaveAs' function via a custom HTTP 404 Not Found error message to download arbitrary files to the target user's system without the XP SP2 warning messages. It is reported that Internet Explorer (IE) does not properly process URLs with certain extraneous characters. A remote user can create a custom HTTP 404 error message and pass this message to the execCommand Method to bypass the 'File Download' and 'File Open' security warnings. There is no solution at this time.

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-11-22 **Sun Java JavaScript plugin vulnerability Virtual Machine code execution attack**

DHS IAIP Daily; http://www.idefense.com/application/poi/display?id=158

November 22, iDEFENSE — Sun Java Plug-in Java-to-Javascript bug lets remote applets execute arbitrary code.

Remote exploitation of a design vulnerability in Sun Microsystems Inc.'s Java Plug-in technology allows attackers to bypass the Java sandbox and all security restrictions imposed within Java Applets. The problem specifically exists within the access controls of the Java to Javascript data exchange in Web browsers using Sun's Java Plug-in technology. The vulnerability allows Javascript code to load an unsafe class which should not normally be possible from a Java Applet. Successful exploitation allows remote attackers to execute hostile Applets that can access, download, upload or execute arbitrary files as well as access the network. A target user must be running a browser on top of a vulnerable Java Virtual Machine to be affected. The vendor has issued a fixed version (1.4.2_06), available at: http://java.sun.com/j2se/1.4.2/download.html

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-11-29 **vulnerabilities Mozilla Firefox Safari Opera browsers patches**

NewsScan; http://www.internetnews.com/security/article.php/3440971

NEW BROWSER VULNERABILITY TARGETS NON-IE MODELS, TOO

Since its debut, Microsoft's Internet Explorer browser has been plagued by a steady stream of "flaw discovery" announcements followed by the requisite patches. Usually those flaws are exclusive to the Microsoft model, but a new vulnerability also affects the Mozilla Browser, Mozilla Firefox, Opera and Apple Safari browsers. This latest bug, called the Infinite Array Sort Denial of Service Vulnerability, causes the affected browsers to execute an infinite JavaScript array sort, which in turn causes a crash. The flaw was discovered by independent security researcher Berend-Jan Wever, who also uncovered the IFRAME vulnerability that affects banner ads. (InternetNews 29 Nov 2004)

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-11-29 **WS FTP file transfer protocol server buffer overflow vulnerability code execution attack no update issued**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Nov/1012353.html

November 29, SecurityTracker — WS_FTP buffer overflow lets remote users execute arbitrary code. A remote user can execute arbitrary code on the target system. It is reported that a remote authenticated user can trigger a buffer overflow in several FTP commands. The SITE, XMKD, MKD, and RFNR FTP commands are affected. A remote user can cause the FTP service to crash or execute arbitrary code. No solution is available at this time.

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-11-30 **CuteFTP file transfer protocol server denial of service DoS vulnerability code execution attack no update issued**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Nov/1012366.html

November 30, SecurityTracker — CuteFTP Professional FTP reply error remote denial of service.

A remote FTP server can cause the target connected FTP client to crash. It is reported that a connected FTP server can send a specially crafted reply code (generally larger than "500") and specially crafted text larger than 65530 bytes to cause the client to crash. Only replies to certain commands are affected. This flaw could possibly be exploited to execute arbitrary code. No solution is available at this time.

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-12-01 **Microsoft security bulletin update Internet Explorer IE vulnerability code execution privilege escalation attack**

DHS IAIP Daily; http://www.microsoft.com/technet/security/bulletin/MS04−
040. mspx

December 01, Microsoft — Microsoft Security Bulletin MS04-040: Cumulative Security Update for Internet Explorer.

A vulnerability exists in Internet Explorer that could allow remote code execution on an affected system. An attacker could exploit the vulnerability by constructing a malicious Web page that could potentially allow remote code execution if a user visited a malicious Website. If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system. Microsoft has assigned a risk rating of "Critical" to this issue and recommends that customers install the update immediately.

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-12-02 **Cisco CNS Network Registrar DNS DHCP server denial of service DoS vulnerability update issued**

DHS IAIP Daily; http://www.cisco.com/warp/public/707/cisco−sa−20041202−
cnr.s html

December 02, Cisco Security Advisory — Cisco CNS Network Registrar denial of service vulnerability.

Cisco CNS Network Registrar Domain Name Service /Dynamic Host Configuration Protocol (DNS/DHCP) server for the Windows Server platforms is vulnerable to a Denial of Service attack when a certain crafted packet sequence is directed to the server. Cisco CNS Network Registrar version 6.0 through 6.1.1.3 are affected by CSCeg27625. However, all versions up to and including version 6.1.1.3 are also affected by CSCeg27614. Cisco has made free software available to address this vulnerability for all affected customers.

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-12-03 **Apple Darwin Streaming Server null byte denial of service DoS attack update issued**

DHS IAIP Daily;
http://www.idefense.com/application/poi/display?id=159&type=
vulnerabilities&flashstatus=true

December 03, iDEFENSE — Apple Darwin Streaming Server DESCRIBE null byte denial of service vulnerability.

Remote exploitation of an input validation vulnerability in Apple Computer Inc.'s Darwin Streaming Server allows attackers to cause a denial of service condition. The vulnerability specifically occurs due to insufficient sanity checking on arguments to DESCRIBE requests. A remote attacker can send a request for a location containing a null byte to cause a denial of service condition, thereby preventing legitimate users from accessing streamed content. Updates are available at: http://www.apple.com/support/downloads//

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-12-07 **Unicenter Remote Control access management server vulnerability update issued**

DHS IAIP Daily; http://secunia.com/advisories/13311/

December 07, Secunia — Unicenter Remote Control arbitrary URC Management Server access vulnerability.

A vulnerability has been reported in Unicenter Remote Control (URC), which can be exploited by malicious users to access arbitrary URC Management Servers. The vulnerability is caused due to an unspecified error in the URC Management Console allowing users to connect to another URC Management Server and make arbitrary configuration changes on the systems managed by this server. Successful exploitation reportedly requires that a user has been authenticated by the underlying OS. Updates available at: http://supportconnectw.ca.com/public/rco_controlit/infodocs/ securitynotice.asp

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-12-09 **Microsoft Internet Explorer IE 6.0 file transfer protocol FTP command injection vulnerability Windows 2000 2K SP4 XP SP2 no update issued**

DHS IAIP Daily; http://secunia.com/advisories/13404/

December 09, Secunia — Microsoft Internet Explorer FTP command injection vulnerability.

A vulnerability has been reported in Microsoft Internet Explorer, which can be exploited by malicious people to conduct FTP command injection attacks. The vulnerability is caused due to insufficient input validation of FTP URIs. This can be exploited by e.g. a malicious website to inject arbitrary FTP commands in a FTP session using a specially crafted pathname containing "%0A" characters. The vulnerability has been confirmed on a fully patched system with Internet Explorer 6.0 and Microsoft Windows 2000 SP4 / XP SP2. There is no solution at this time.

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-12-10 **MIMEsweeper SMTP PDF denial of service DoS vulnerability**

DHS IAIP Daily; http://secunia.com/advisories/13411/

December 10, Secunia — MIMEsweeper for SMTP PDF file processing denial of service.

A vulnerability has been reported in MIMEsweeper for SMTP, which can be exploited by malicious people to cause a DoS (Denial of Service). The vulnerability is caused due to an error within the Security Service when processing PDF files. This can be exploited to crash the Security Service by sending an e-mail containing a specially crafted PDF file as attachment. Apply MIMEsweeper for SMTP 5.0 Service Pack 1: http://www.clearswift.com/download/info.aspx?ID=562

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-12-13 **phpBB PHP bulletin board Web software vulnerabilities directory traversal attack update issued**

DHS IAIP Daily; http://secunia.com/advisories/13421/

December 13, Secunia — phpBB Attachment Mod two vulnerabilities.

Two vulnerabilities have been reported in the Attachment Mod module for phpBB, which can be exploited by malicious people to compromise a vulnerable system. An input validation error can be exploited to add, remove, and execute files outside the upload directory via directory traversal attacks. Secondly, an error in the handling of multiple file extensions within "mod_mime" can be exploited to upload malicious script files. The vulnerabilities have been reported in version 2.3.10. Update to version 2.3.11: http://sourceforge.net/project/showfiles.php?group_id=66311

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-12-14 **phpMyAdmin PHP MySQL Web scripting software update issued**

DHS IAIP Daily; http://secunia.com/advisories/13424/

December 14, Secunia — phpMyAdmin two vulnerabilities.

Two vulnerabilities exist in phpMyAdmin, which can be exploited by malicious people to compromise a vulnerable system and by malicious users to disclose sensitive information. An input validation error in the handling of MySQL data allows injection of arbitrary shell commands. Input passed to "sql_localfile" is not properly sanitized in "read_dump.php" before being used to disclose files. Successful exploitation requires access to the phpMyAdmin interface, and that PHP safe mode is disabled and the UploadDir mechanism to be active. The vulnerabilities have been fixed in version 2.6.1-rc1.

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-12-14 **zgv xzgv integer overflow vulnerabilities compromise code execution attack update issued**

DHS IAIP Daily; http://secunia.com/advisories/13449/

December 14, Secunia — zgv/xzgv multiple integer overflow vulnerabilities.

Multiple vulnerabilities have been reported in zgv/xzgv, which potentially can be exploited by malicious people to compromise a vulnerable system. The vulnerabilities are caused due to various integer overflows when processing images. These can be exploited to cause buffer overflows via images containing specially crafted headers. Successful exploitation may allow execution of arbitrary code when a malicious image is viewed. Apply patches: http://rus.members.beeb.net/xzgv-0.8-integer-overflow-fix.di ff

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-12-16 **Cisco Unity default usernames passwords Exchange vulnerability update issued**

DHS IAIP Daily; http://secunia.com/advisories/13483/

December 16, Secunia — Cisco Unity default usernames and passwords vulnerability.

A security issue has been reported in Cisco Unity versions 2.x, 3.x, and 4.x (prior to version "4.0(5)") when integrated with Exchange, which can be exploited by malicious people to access administrative functions. The problem is that Cisco Unity creates certain user accounts with default passwords when integrated with Exchange. Successful exploitation provides access to certain administrative functions. A vendor solution is available at: http://www.cisco.com/warp/public/707/cisco-sa-20041215-unity .shtml

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-12-16 **PHP Web scripting language multiple vulnerabilities update issued**

DHS IAIP Daily; http://secunia.com/advisories/13481/

December 16, Secunia — PHP multiple vulnerabilities.

Multiple vulnerabilities have been reported in PHP, which can be exploited to gain escalated privileges, bypass certain security restrictions, gain knowledge of sensitive information, or compromise a vulnerable system. Update to version 4.3.10 or 5.0.3: http://www.php.net/downloads.php

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-12-16 **Samba security integer overflow heap based buffer overflow vulnerability update issued**

DHS IAIP Daily; http://secunia.com/advisories/13453

December 16, Secunia — Samba security descriptor parsing integer overflow vulnerability.

A vulnerability has been reported in Samba versions 2.x and 3.0.x up to and including version 3.0.9, which can be exploited by malicious users to compromise a vulnerable system. The vulnerability is caused due to an integer overflow within smbd when handling security descriptors. This can be exploited to cause a heap-based buffer overflow by requesting an extremely large amount of security descriptors. Successful exploitation allows execution of arbitrary code, but requires that the user has proper credentials to access a share. Apply patch for Samba 3.0.9: http://us1.samba.org/samba/ftp/patches/security/samba-3.0.9-CAN-2004-1154.patch

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-12-17 **Symantec Brightmail software vulnerabilities denial of service DoS update issued**

DHS IAIP Daily; http://secunia.com/advisories/13489/

December 17, Secunia — Symantec Brightmail denial of service vulnerabilities.

Two vulnerabilities have been reported in Symantec Brightmail, which can be exploited by malicious people to cause a DoS (Denial of Service). The Sieve module fails to recognize malformed RFC 822 MIME attachment boundaries and Spamhunter fails to convert certain valid character encoding sets to UTF. Apply patch 134: ftp://ftp.symantec.com/public/english_us_canada/products/sba/sba_60x/updates/Patch134.zip

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-12-21 **US CERT phpBB PHP bulletin board highlight parameter vulnerability Website hacking update issued**

DHS IAIP Daily; http://www.us−cert.gov/cas/techalerts/TA04−356A.html

December 21, US-CERT — Technical Cyber Security Alert TA04-356A: Exploitation of phpBB highlight parameter vulnerability.

The software phpBB, an open-source bulletin board application, contains an input validation problem in how it processes a parameter contained in URLs. An intruder can deface a phpBB Website, execute arbitrary commands, or gain administrative privileges on a compromised bulletin board. According to reports, this vulnerability is being actively exploited by the Santy.A worm. The worm appears to propagate by searching for the keyword "viewtopic.php" in order to find vulnerable sites. The worm writes itself to a file named "m1ho2of" and then overwrites files ending with .htm, .php, .asp. shtm, .jsp, and .phtm replacing them with HTML content that defaces the Web page. Upgrade to phpBB version 2.0.11: http://www.phpbb.com/downloads.php

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-12-30 **colleges recruiting technology admissions tool colleges universities Internet videos Web page Vmags**

EDUPAGE;
http://www.nytimes.com/2004/12/30/technology/circuits/30coll.html

COLLEGES EXPAND RECRUITING TECHNOLOGY

As the effectiveness of e-mail as an admissions tool declines, colleges and universities are beginning to explore alternative recruitment Internet strategies. At the top of the list for many institutions are streaming videos of campus, either on the school's Web page or in the form of video magazines, or Vmags. Saint Mary's College in Notre Dame began testing a Vmag two years ago, sending it to students who had been accepted but had not yet decided to enroll. Saint Mary's Vmag includes four videos, each between one and two minutes, showing various activities on campus. Users who have downloaded the Vmag are prompted when new versions are available. Many believe video is able to persuade in ways that fixed images are not. Westminster College in Salt Lake City has added 136 video clips to its Web site in an effort to appeal to prospective students. Joel Bauman, vice president for enrollment at Westminster, said the videos are fairly inexpensive to produce. Karen Giannino, senior associate dean of admission at Colgate University in Hamilton, N.Y., said the videos added to her institution's Web site help "tell our story in a compelling way" and "differentiate Colgate" from similar schools.

Category 23.6 *Web-site infrastructure, general Web security issues*

2004-12-30 **Mozilla Internet Web browser buffer overflow vulnerability code execution attack update issued**

DHS IAIP Daily; http://securitytracker.com/alerts/2004/Dec/1012726.html

December 30, SecurityTracker — Mozilla buffer overflow in processing NNTP URLs lets remote users execute arbitrary code.

A heap overflow vulnerability was reported in Mozilla in the processing of NNTP URLs. A remote user can create a specially crafted 'news://' URL that, when loaded by the target user, will trigger a buffer overflow and execute arbitrary code on the target user's system. The code will run with the privileges of the target user. The vendor has issued a fixed version (1.7.5), available at: http://www.mozilla.org/products/mozilla1.x/

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-01-03 **Microsoft Internet Explorer IE vulnerability download directory traversal attack FTP file transfer protocol Windows XP SP2 not vulnerable**

DHS IAIP Daily; http://secunia.com/advisories/13704/

INTERNET EXPLORER FTP DOWNLOAD DIRECTORY TRAVERSAL

It has been reported that a vulnerability exists in Internet Explorer, which can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to an input validation error in the handling of FTP file transfers. This can be exploited by a malicious FTP server to create files in arbitrary locations via directory traversal attacks by tricking a user into downloading malicious files (e.g. by dragging or copying a file or folder). The vulnerability does not affect systems running Windows XP with SP2 installed.

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-01-11 **Squid NTLM memory leak vulnerability segmentation fault update issued**

DHS IAIP Daily; http://securitytracker.com/alerts/2005/Jan/1012818.html

SQUID NTLM FAKEAUTH_AUTH HELPER

A vulnerability known as a memory leak has been reported in Squid in the NTLM fakeauth_auth helper. A remote user can trigger a segmentation fault. Under high load or when running for a long period of time, the application may run out of memory. In addition, a remote user can send a specially crafted NTLM type 3 message to cause a segmentation fault and can cause denial of service conditions. As a solution, apply the following patch: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.ST ABLE7-fakeauth_auth.patch

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-01-11 **Microsoft Internet Explorer IE vulnerabilities cross site scripting attack Windows XP SP2 vulnerable no update issued**

DHS IAIP Daily; http://secunia.com/advisories/12889/

MICROSOFT INTERNET EXPLORER MULTIPLE VULNERABILITIES

Some vulnerabilities have been discovered in Internet Explorer, which can be exploited by malicious people to compromise a user's system, conduct cross-site/zone scripting and bypass a security feature in Microsoft Windows XP SP2. They do not require user interaction. The vulnerability was originally discussed as the Drag'n'Drop vulnerability back in October 2004. The new development only utilizes flaws in the HTML Help control. This has been confirmed on a fully patched system with Internet Explorer 6.0 and Microsoft Windows XP SP2. There is no solution at this time.

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-01-13 **PHP-Nuke SQL injection vulnerability code execution source code edit**

DHS IAIP Daily; http://secunia.com/advisories/13824/

PHP-NUKE SGALLERY MODULE FILE INCLUSION AND SQL INJECTION

Two vulnerabilities in the Sgallery module for PHP-Nuke can be exploited by malicious people to compromise a vulnerable system and conduct SQL injection attacks. 1) Input passed to the "DOCUMENT_ROOT" parameter in "imageview.php" isn't properly verified, before it is used to include files. This can be exploited to include arbitrary files from external and local resources. 2) Input passed to the "idalbum" and "idimage" parameters in "imageview.php" isn't properly sanitized before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code. The vulnerability has been reported in version 1.01. Other versions may also be affected. Users should edit the source code to ensure that input is properly sanitized.

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-01-14 **ForumKIT input validation vulnerability remote user cross site scripting attack no update issued**

DHS IAIP Daily; http://securitytracker.com/alerts/2005/Jan/1012895.html

FORUMKIT INPUT VALIDATION HOLE LETS REMOTE USERS CONDUCT CROSS-SITE SCRIPTING ATTACKS

A vulnerability has been reported in forumKIT causing the 'f.aspx' script to improperly validate user-supplied input in the 'members' parameter. A remote user can create a specially crafted URL that, when loaded by a target user, will cause arbitrary scripting code to be executed by the target user's browser. The code will originate from the site running the forumKIT software. As a result, the code will be able to access the target user's cookies (including authentication cookies) associated with the site, access data recently submitted by the target user via web form, or take actions on the site acting as the target user. No solution is available at this time.

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-01-20 **JSBoard PHP Web software input validation flaw vulnerability information disclosure update issued**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2005/Jan/1012949.html

JSBOARD 'SESSION.PHP' INPUT VALIDATION FLAW DISCLOSES FILES TO REMOTE USERS

A remote user can view files on the target system with the privileges of the target web service. The 'session.php' script does not properly validate the user-supplied 'table' variable. If magic_quotes_gpc is set to 'off' in the 'php.ini' configuration file, then a remote user can supply a specially crafted URL to view files on the target system with the privileges of the target web service. The vendor has issued a fixed version (2.0.10), available at: http://kldp.net/frs/download.php/1729/jsboard-2.0.10.tar.gz

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-02-07 **KDE Konqueror Internet Web browser International Domain Names IDN spoofing security vulnerability no update issued**

DHS IAIP Daily; http://securitytracker.com/alerts/2005/Feb/1013098.html

KDE KONQUEROR WEB BROWSER IDN SPOOFING SECURITY ISSUE

A vulnerability was reported in the processing of International Domain Names (IDNs). A remote user can spoof Websites, including secure Websites. The remote user can create a specially crafted URL that, when loaded by the target user, will cause the browser to display a spoofed URL in the status bar but load a Web page from a different Website with an IDN. If the destination site is running SSL and has a valid digital certificate, the browser will authenticate the site but display the spoofed URL as the authenticated URL. No solution is currently available.

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-02-11 **Microsoft Internet Explorer IE multiple vulnerabilities code execution attack**

DHS IAIP Daily; http://www.securityfocus.com/bid/12530/discussion/

MICROSOFT INTERNET EXPLORER MULTIPLE VULNERABILITIES

Microsoft Internet Explorer is reported prone to multiple vulnerabilities. These issues may allow remote attackers to execute arbitrary script code, disclose sensitive information and execute files from the local system. These issues are reported to be addressed by MS05-014: http://www.microsoft.com/technet/security/bulletin/MS05-014. mspx

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-02-18 **design flaw automatic redirection denial of service DoS hotel Internet high-speed connection**

RISKS 23 73

RSS READER REDIRECT RISKS

Monty Solomon discovered that RSS feeds are automatically rerouted to an active proxy server if there is a redirection of HTTP requests while the RSS reader is trying to locate its feeds. Unfortunately, this design feature meant that when he logged on in a hotel where there was a _temporary_ redirection to a registration page for the high-speed Internet connection, many of his RSS feeds were permanently redirected to the registration page with no provision for shifting them back. Turns out the switch occurred while the RSS reader was running on the laptop while it was connected to the network but before the user was able to register for normal usage.

Monty's recommendation: "At a minimum, the RSS reader should validate the feed at the redirected URI before blindly switching to it."

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-02-18 **WebCalendar SQL injection vulnerability input validation error cookie**

DHS IAIP Daily; http://www.k−otik.com/english/advisories/2005/0184

WEBCALENDAR "WEBCALENDAR_SESSION" SQL INJECTION VULNERABILITY

An SQL injection vulnerability was reported in WebCalendar, which may be exploited by attackers to execute arbitrary SQL commands. This flaw exists due to an input validation error in "login" when used in cookies. Update to WebCalendar version 0.9.5: http://www.k5n.us/webcalendar.php?topic=Download

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-02-24 **Mozilla Firefox domain spoofing vulnerability Internationalized Domain Names IDN patch issued**

DHS IAIP Daily; http://news.com.com/Firefox+fix+plugs+security+holes/2100−
10 02_3−5589693.html

MOZILLA FIREFOX VULNERABILITIES PATCHED.

The Mozilla Foundation released on Thursday, February 24, an update to the Firefox Web browser to fix several vulnerabilities, including one that would allow domain spoofing. The open-source project released Firefox 1.0.1 to fix, among other bugs, a vulnerability in the Internationalized Domain Names (IDN), a standard for handling special character sets in domain names that lets companies register domain names that appear to be the same in different languages. The IDN vulnerability allowed an attacker to create a fake Website on a non-Microsoft browser in order to pull off a phishing scam. The update is available for Windows, Mac OS X and Linux at http://www.mozilla.org.

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-03-11 **man-in-the-middle attack SSL encryption decryption misrepresentation confidentiality data theft risk banking proxy servers vulnerability insider fraud**

RISKS; http://www.shellnofcu.com/site/scams.html 23 79

MAN IN THE MIDDLE ATTACK ON SSL?

Russell Page had an interesting analysis of a technique potentially vulnerable to insider fraud:

Marketscore (www.marketscore.com) offer a free proxy service web users. They offer accelerated downloads and e-mail virus scanning. To use their service users download and install software onto their PCs. Marketscore are quite explicit that they collect a wide range of information about their subscribers, and make information available to web site owners on usage patterns - a sort of "Neilson" for the net.

Unfortunately, they also impersonate SSL sites. If a subscriber attempts to set up an SSL connection to say, her bank, the Marketscore proxy sends back it's certificate, and then establishes an SSL connection to the destination. Clearly for this to work, the servers have to decrypt then re-encrypt all of the traffic. Equally clearly, large numbers of credit card numbers, account names, passwords etc are passing through the Marketscore systems in the clear.

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-03-15 **Apache Tomcat JSP Web server vulnerability remote denial of service DoS attack**

DHS IAIP Daily; http://www.k−otik.com/english/advisories/2005/0262

APACHE TOMCAT "AJP12" REMOTE DENIAL OF SERVICE VULNERABILITY

A new vulnerability was identified in Apache Tomcat, which may be exploited by attackers to conduct Denial of Service attacks. The flaw resides in the implementation of the AJP12 protocol and may allow a remote attacker who sends a specially crafted request, to cause Tomcat to stop processing requests. Update to Apache Tomcat 5.5.8: http://jakarta.apache.org/site/downloads/downloads_tomcat-5. cgi

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-03-23 **Mozilla Suite Firefox Thunderbird vulnerabilities code execution update issued**

DHS IAIP Daily; http://www.k−otik.com/english/advisories/2005/0296

MOZILLA SUITE/FIREFOX/THUNDERBIRD CODE EXECUTION VULNERABILITIES

Several vulnerabilities were identified in Mozilla Suite, Firefox and Thunderbird, which may be exploited by attackers to execute arbitrary commands or bypass certain security features. These vulnerabilities are due to a heap overrun error, an error in bookmarking a specially crafted page as a Firefox sidebar panel, and an error when handling specially crafted XUL files. Update to the most current version of the product: http://www.mozilla.org

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-03-30 **E−Store Kit−2 PayPal Edition XSS and PHP file inclusion vulnerability file disclosure cross site scripting attack no update issued**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/0298

E-STORE KIT-2 PAYPAL EDITION XSS AND PHP FILE INCLUSION VULNERABILITY.

Two vulnerabilities were identified in E-Store Kit-2 PayPal Edition, which may be exploited by attackers to include arbitrary files or conduct Cross Site Scripting attacks. The first flaw resides in the "catalog.php" file, when handling specially crafted "main" and "menu" parameters, which may be exploited by a remote attacker to include arbitrary PHP files and execute commands with the privileges of the web server. The second vulnerability is due to an input validation error in the "downloadform.php" script when handling a specially crafted "txn_id" parameter, which may be exploited by attackers to cause arbitrary scripting code to be executed by the user's browser. There is no solution at this time.

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-04-04 **Mozilla Firefox Suite information disclosure vulnerability JavaScript engine flaw no update issued**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/0312

MOZILLA FIREFOX/SUITE INFORMATION DISCLOSURE VULNERABILITY

A new vulnerability was identified in Mozilla Firefox/Suite, which may be exploited by attackers to disclose sensitive information. The browser's javascript implementation does not properly parse lamba list regular expressions. This flaw is due to an error in the JavaScript engine, which may be exploited by attackers to disclose arbitrary heap memory regions. There is no solution at this time.

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-04-18 **Mozilla Firefox multiple vulnerabilities cross site scripting system compromise attack update issued**

DHS IAIP Daily; http://secunia.com/advisories/14938/

MOZILLA FIREFOX MULTIPLE VULNERABILITIES

Multiple vulnerabilities have been reported in Firefox, which can be exploited by malicious people to conduct cross-site scripting attacks, bypass certain security restrictions, and compromise a user's system. Update to version 1.0.3: http://www.mozilla.org/products/firefox/

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-04-19 **Microsoft Windows Explorer preview pane vulnerability script injection attack unauthorized access no update issued**

DHS IAIP Daily; http://www.securityfocus.com/bid/13248/info/

MICROSOFT WINDOWS EXPLORER PREVIEW PANE SCRIPT INJECTION VULNERABILITY

Microsoft Windows Explorer is prone to a script injection vulnerability. This occurs when the Windows Explorer preview pane is enabled on Windows 2000 computers. If a file with malicious attributes is selected using Explorer, script code contained in the attribute fields may be executed with the privilege level of the user that invoked Explorer. This could be exploited to gain unauthorized access to the vulnerable computer. No vendor solution is currently available.

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-04-20 **phpBB PHP bulletin board two vulnerabilities SQL injection path disclosure attacks no update issued**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/0372

PHPBB-AUCTION SQL INJECTION AND PATH DISCLOSURE VULNERABILITIES

Two vulnerabilities were reported in phpBB-Auction, which may be exploited by attackers to execute arbitrary SQL commands or disclose the full web path. 1. The flaw is due to an SQL injection error in the "auction_rating.php" and "auction_offer.php" scripts when handling specially crafted "u" and "ar" parameters. 2. The vulnerability is due to an input validation error in the "auction_myauctions.php" script when handling a specially crafted "mode" parameter, which may be exploited to display the installation path. There is no solution at this time.

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-04-22 **Opera Secure Sockets Layer SSL certificate security feature design error vulnerability no update issued**

DHS IAIP Daily; http://www.securityfocus.com/bid/13176/discussion/

OPERA SSL SECURITY FEATURE DESIGN ERROR VULNERABILITY

Opera browser is prone to a design error that can result in a false sense of security. The source of the vulnerability is that the Organization Name of an SSL certificate is not intended to be unique. Since this field is not unique, it is not sufficient to use as a basis for the user to trust the authenticity of a Website. There is no solution at this time.

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-05-02 **GlobalScape file transfer protocol FTP server remove buffer overflow vulnerability command execution attack**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/0441

GLOBALSCAPE SECURE FTP SERVER REMOTE BUFFER OVERFLOW VULNERABILITY

A buffer overflow vulnerability was identified in GlobalScape Secure FTP Server, which could be exploited by remote attackers to execute arbitrary commands. The flaw occurs when handling specially crafted FTP commands, which could be exploited by a remote and authenticated attacker to compromise a vulnerable server. Upgrade to the latest version: http://www.cuteftp.com/support/srv.asp

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-05-06 **Rivest Shamir Adleman RSA Security encryption Authentication Agent heap buffer overflow vulnerability code execution attack**

DHS IAIP Daily; http://www.securityfocus.com/bid/13524/discussion/

RSA AUTHENTICATION AGENT FOR WEB REMOTE HEAP BUFFER OVERFLOW VULNERABILITY.

A remote heap-based buffer overflow vulnerability exists in RSA Authentication Agent for Web. This issue is due to a failure of the application to properly bounds check user-supplied input data prior to copying it into a fixed-sized heap buffer memory region. This vulnerability allows remote attackers to execute arbitrary machine code in the context of the vulnerable server application. This reportedly occurs with 'LocalSystem' privileges, allowing the attacker to gain complete control of the targeted computer. Versions 5.0, 5.2, and 5.3 of RSA Authentication Agent for Web are vulnerable to this issue. Users of affected packages are urged to contact the vendor for further information. Users with valid support contracts with the vendor may be able to locate fixes at: https://knowledge.rsasecurity.com There are currently no vendor-supplied patches for this issue.

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-05-09 **PHP Web scripting programming Advanced Transfer Manager**

DHS IAIP Daily; http://secunia.com/advisories/15279/

PHP ADVANCED TRANSFER MANAGER FILE UPLOAD VULNERABILITY

A vulnerability has been reported in PHP Advanced Transfer Manager, which potentially can be exploited by malicious people to compromise a vulnerable system. A remote user can authenticate to the system, upload a PHP file with the '.ns' extension, and then have the Web server execute the file. The PHP code, including operating system commands, will run with the privileges of the target Web service. There is no solution at this time.

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-05-10 **Microsoft Security Bulletin Internet Explorer Web View vulnerability Windows operating systems**

DHS IAIP Daily; http://www.microsoft.com/technet/security/Bulletin/MS05−
024. mspx

VULNERABILITY IN WEB VIEW COULD ALLOW REMOTE CODE EXECUTION

A remote code execution vulnerability exists in the way that Web View in Windows Explorer handles certain HTML characters in preview fields. By persuading a user to preview a malicious file, an attacker could execute arbitrary code in the context of the logged on user. This vulnerability affects Microsoft Windows 2000, Windows 98, Windows 98 SE, and Windows ME. Updates available through Source link below.

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-05-16 **Apache HTDigest command line buffer overflow vulnerability**

DHS IAIP Daily; http://www.securityfocus.com/bid/13537/info/

APACHE HTDIGEST REALM COMMAND LINE ARGUMENT BUFFER OVERFLOW VULNERABILITY

A buffer overflow vulnerability exists in the htdigest utility included with Apache. The vulnerability is due to improper bounds checking when copying user-supplied realm data into local buffers. By supplying an overly long realm value to the command line options of htdigest, it is possible to trigger an overflow condition. This may cause memory to be corrupted with attacker-specified values. This issue could be exploited by a remote attacker; potentially resulting in the execution of arbitrary system commands within the context of the web server process. See Source link for any vendor supplied solutions.

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-05-17 **Pserv command execution information disclosure vulnerabilities no update issued**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/0555

PSERV COMMAND EXECUTION AND INFORMATION DISCLOSURE VULNERABILITIES

Multiple vulnerabilities were identified in PServ, which may be exploited by attackers to execute arbitrary commands or disclose sensitive information. The first issue is due to an input validation error when handling specially crafted HTTP requests containing directory traversal sequences, which may be exploited by a remote attacker to disclose the source code of cgi scripts or read arbitrary files outside of the webroot directory. The second flaw is due to a buffer overflow error when processing a specially crafted "completedPath" variable, which may be exploited by attackers to execute arbitrary commands with the privileges of the web server. There is no solution at this time.

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-06-12 **efficiency denial of service performance Web site servers insecure old systems vehicle registration vulnerabilities criminal hackers**

Duluth News Tribune (URL dead)

MINNESOTA STATE WEB SITE BOGGED DOWN
ASSOCIATED PRESS

ST. PAUL - The delivery of thousands of driver's licenses and state identification cards was delayed recently and the state's vehicle registration Web site was suspended because of insecure Web pages and the limitations of an old computer system.

As the Department of Public Safety works to bring its vehicle registration site back online, the Star Tribune of Minneapolis learned that other state agency Web sites may be vulnerable to computer hackers, including the Department of Transportation, the Board of Accountancy and the Health Professionals Services Program…

[Extract contributed by Stephen Cobb]

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-07-19 **IDG fake cards Internet SurfControl PLC phishing personal**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/holes/story/0,10801,103326,00.html

ATTACKERS TURNING TO FAKE ONLINE GREETING CARDS

According to Internet security vendor SurfControl PLC, attackers are increasingly using fake e-mail greeting cards as a way of getting malicious software installed on computers. In fact, the amount of malicious e-mail being disguised as e-mail greeting cards is up about 90% from last year and now makes up more than half of all malicious e-mail being sent, according to Paris Trudeau, a product marketing manager at SurfControl. The number of "phishing" attacks, in which users are tricked into entering personal information on fake Websites, is also on the rise. But increasingly, attackers are looking for ways to trick users into downloading software that can be used to take over a computer, turning it into a so-called zombie machine, she said. Often this can be done by sending an e-mail greeting that entices users to visit a maliciously encoded Web page, Trudeau said. Another trick is to mask an e-mail message so it appears to originate from the user's IT department.

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-08-23 **safety-critical system architecture software design engineering recommendations article overview**

RISKS; http://www.embedded.com//showArticle.jhtml?articleID=169600396 24 05

ARCHITECTURE OF SAFETY-CRITICAL SYSTEMS

David Kalinsky published an excellent overview of the principles of designing and implementing safety-critical systems for the online journal _Embedded.com_. Here are some highlights:

"Safety-critical systems are embedded systems that could cause injury or loss of human life if they fail or encounter errors. Flight-control systems, automotive drive-by-wire, nuclear reactor management, or operating room heart/lung bypass machines naturally come to mind. But devices as common as the power windows in your car are also safety-critical, once you imagine a small child reaching out of the car window at a fast food drive-through to get another packet of ketchup and accidentally leaning on the control switch making the window shut on the child's arm, or worse.

Small system defects or situations can cascade into life-threatening failures very quickly…."

Key points discussed in the article:

* Safety vs. High availability: Some readers may be thinking "Hey, this is starting to sound an awful lot like high availability." But while there are a number of points of contact between safety-critical system design and high-availability system design, the objectives of the two are quite different and many of the design architectures they use are quite different.

* Step-by-step approach: As with any embedded system, design is preceded by a system requirements definition, covering physical and functional specification. For safety-critical systems, a thorough hazard analysis and risk analysis must also be done. Only then can architectural design get started.

* Detecting sensor errors: Correct sensor data are so crucial to safe operation that many systems use redundancy in their sensor data acquisition. Redundancy doesn't always mean sensor replication as shown in Figure 5 with two identical sensors. It could also mean functional redundancy, or the measurement of the same real-world value in two different ways. For example, patient respiration rate can be measured both by the expansion and contraction of the rib cage, and by measurement of expiratory CO2 concentration.

* Shutdown systems: If a safety-critical system has an immediate safe state, as illustrated on the left side of Figure 2, a shutdown system can be used to terminate a hazardous situation as soon it detects it.

* Single channel with actuation monitoring: The idea of a shutdown system can also be applied on a smaller scale within a primary system itself, as shown in Figure 8. The ellipses represent major system activities, which could be implemented as software tasks or processes, either on separate processors or sharing a single processor, depending on the scale of the system. A basic primary system is structured by the simple design pattern of Input-Process-Output, shown here across the top of the figure as the sequence labeled "Data Acquisition," "Processing/Transformations," "Output/Control." To lower costs, the primary system and the sensor data integrity checking "shutdown" monitoring activity (at the lower left) are shown here as sharing the same input sensor(s).

* Dual-channel architectures: For safety-critical systems without an immediate safe state, dual-channel architectures can be used to allow a system to continue operation even when one of its channels has "fail stopped."

* Monitor-actuator architecture: Many safety-critical systems do not have an immediate safe state, but can't incur the high costs of a full dual-channel or multiple-channel architecture.

* Keeping people safe: The selection of a safety-critical system architecture is driven by a rigorous hazard analysis followed by risk analysis, in addition to conventional system requirements definition. System design may include combinations of redundant sensor configurations, shutdown systems, actuation monitoring, multiple channel architectures, and/or monitor-actuator structuring. These embedded systems architectures are much more valuable than can be measured in dollars and cents. Their true value is in protecting and saving human lives.

[Extracts selected by MK; all text by the author]

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-09-25 **online scam fraud phishing protection tool GeoTrust TrustWatch Toolbar Website safety SSL**

EDUPAGE; http://news.com.com/2100-1029_3-5879068.html

NEW TOOLS RATE SAFETY OF WEB SITES

Two new tools from GeoTrust offer Internet users another layer of protection against a range of online scams. The TrustWatch Search site and TrustWatch Toolbar both provide indications about the probable reliability of sites users are visiting, in an effort to help consumers avoid being victimized by phishing scams or by other forms of fraudulent Web sites. The tools evaluate sites for security practices such as certain forms of authentication or use of a Secure Sockets Layer certificate. Sites are also screened against a black list of known fraud sites and checked for patterns that would indicate potentially malicious intent. Users are shown a green signal to indicate a verified site, a yellow signal for suspect sites, and a red signal for sites that cannot be verified. The toolbar provides users with a real-time screen for sites they visit; the search site returns search results--powered by Ask Jeeves--with one of the three indicators for each site returned. CNET, 25 September 2005

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-10-09 **proprietary source code government programs Windows operating system download Java security safety confidentiality Trojans vulnerability risk management**

RISKS 24 07

GREEK TAX DEPARTMENT OFFERS PROPRIETARY, WINDOWS-ONLY EXECUTABLES FOR DOWNLOAD TO CITIZENS

Vassilis Prevalakis noted that the Greek tax department offered taxpayers free software for download from their Web site to help fill in tax forms.

The original programs were

* proprietary (secret) code;
* ran only under Windows.

Eventually, the ministry said it planned "to provide Java-based programs that should run on non-Microsoft platforms and may make the source code available to academic institutions or non-governmental organizations for auditing purposes."

Prevelakis noted, "Still the whole experience shows how easy it is for state agencies to reach out in the homes of their citizens."

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-12-08 **data corruption WHOIS Internet database Government Accountability Office GAO ICANN FTC Web infrastructure**

EDUPAGE; http://www.internetnews.com/ent-news/article.php/3569521

GAO WARNS OF BAD DATA IN WHOIS

A new report from the U.S. Government Accountability Office (GAO) indicates that as many as 2.3 million Web addresses are owned by individuals or organizations that cannot be identified due to bad data in the WHOIS database for .com, .net, and .org domains. The report said that 5 percent of all addresses have incomplete or inaccurate information about the owner, in effect creating a safe haven for operators of Web-based scams, such as phishing attacks or the distribution of spam and viruses. When authorities try to track down those responsible for such malicious activities, they rely on the WHOIS database to find out who operates suspect domains. When the information in WHOIS is wrong, authorities hit a dead end. The Federal Trade Commission has been urging a clean-up of the database for a long time, but progress has been slow. Data are typically entered into the database through domain registrars, which bear some responsibility for ensuring the integrity of the information, along with the Internet Corporation for Assigned Names and Numbers (ICANN). Despite an ICANN policy requiring registrars to remind domain owners to update their information regularly, a system that tracks reports of complaints, however, indicates that only about 60 percent of problems are resolved. Internet News, 8 December 2005

Category 23.6 *Web-site infrastructure, general Web security issues*

2005-12-27 **Microsoft Internet Explorer HTML parsing denial of service vulnerabilities attacker malicious site Security Focus patchers**

DHS IAIP Daily; http://www.securityfocus.com/bid/16070/discuss

Microsoft Internet Explorer HTML parsing denial of service vulnerabilities.

Microsoft Internet Explorer is affected by multiple denial of service vulnerabilities. An attacker may exploit these issues by enticing a user to visit a malicious site resulting in a denial of service condition in the application. Security Focus is not aware of any vendor-supplied patches for this issue.

Category 23.6 *Web-site infrastructure, general Web security issues*

2006-01-13 **US GSA Webs site shut down security flaw consultant eOffer corporate espionage information theft risk**

EDUPAGE; http://www.nytimes.com/2006/01/13/technology/13secure.html 23

GOVERNMENT CLOSES WEB SITE DUE TO SECURITY FLAW

A government Web site for contractors has been shut down due to a security flaw that allowed users of the site to see and change data submitted by other vendors. The General Services Administration (GSA) closed eOffer after a consultant reported the problem. Three weeks passed, however, between the reporting of the flaw and the shuttering of the site. The Web site was launched in 2004 as a means for vendors to bid electronically on government contracts for IT products and services. The flaw allowed site users to access and change corporate and financial information, potentially compromising the entire bidding process, according to security experts. The problem could also allow corporate espionage. The GSA said there was no evidence that the site had been abused by either authorized or unauthorized users. The agency said the delay in shutting down the site was caused by the time that was required to process the report. New York Times, 13 January 2006 (registration req'd)

Category 23.6 *Web-site infrastructure, general Web security issues*

2006-02-01 **Winamp music player software buffer overflow vulnerability US-CERT Cyber Security Alert solution update**

DHS IAIP Daily; http://www.uscert.gov/cas/techalerts/TA06−032A.html 23

US-CERT TECHNICAL CYBER SECURITY ALERT TA06-032A: WINAMP PLAYLIST BUFFER OVERFLOW.

Systems affected: Microsoft Windows systems with Winamp 5.12 or earlier. Overview: America Online has released Winamp 5.13 to correct a buffer overflow vulnerability. Exploitation of this vulnerability could allow a remote attacker to execute arbitrary code with the privileges of the user. Impact: By convincing a user to open a specially crafted playlist file, a remote unauthenticated attacker may be able to execute arbitrary code with the privileges of the user. Winamp may open a playlist file without any user interaction as the result of viewing a Webpage or other HTML document. Solution: Upgrade to Winamp 5.13: http://www.winamp.com/player/

Category 23.6 *Web-site infrastructure, general Web security issues*

2006-02-15 **Winamp music player software multiple buffer overflow vulnerabilities no solution**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2006/0613 23

NULLSOFT WINAMP PLAYLIST HANDLING MULTIPLE BUFFER OVERFLOW VULNERABILITIES

Multiple vulnerabilities have been identified in Winamp, which could be exploited by remote attackers to take complete control of the affected system. Analysis: The buffer overflow error when processing a specially crafted playlist containing an overly long media filename, which could be exploited by remote attackers to compromise a vulnerable system via a specially crafted playlist. The second issue is due to a buffer overflow error when processing a playlist (.m3u) with an overly long filename, which could be exploited by remote attackers to execute arbitrary commands and take complete control of an affected system via a specially crafted Webpage. Affected products: Nullsoft Winamp version 5.13 and prior. Solution: FrSIRT is not aware of any official supplied patch for this issue.

Category 23.6 *Web-site infrastructure, general Web security issues*

2006-02-20 **Indiana University professor active cookie new technology fight defeat online scams**

EDUPAGE; http://www.pcworld.idg.com.au/index.php/id;215389687;fp;2;fpid;1 23

IU PROFESSOR INTRODUCES ACTIVE COOKIE

A researcher at Indiana University has developed technology he calls "active cookies" that he says will help defeat online scams. Markus Jacobsson, associate professor of informatics and associate director of the Indiana University Center for Applied Cybersecurity Research, has teamed up with Ari Juels, manager and principal research scientist at RSA Laboratories, to form a company called RavenWhite to market the technology. Standard cookies are intended only to identify users to a Web host. According to RavenWhite, active cookies also authenticate users. Pharming scams and other similar malicious activities redirect users from intended Web sites to bogus ones without the user's knowing. Active cookies would reportedly alert users to the redirect and foil the scam. The company said it is working on technology that would extend the protections offered by active cookies to users who use multiple computers or who change browser settings that affect how cookies are handled.

Category 23.6 *Web-site infrastructure, general Web security issues*

2006-02-23 **Macromedia Shockwave Player installer buffer overflow vulnerability**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2006/0716 23

MACROMEDIA SHOCKWAVE PLAYER INSTALLER BUFFER OVERFLOW VULNERABILITY.

A vulnerability has been identified in Macromedia Shockwave Player, which could be exploited by remote attackers to take complete control of an affected system. Analysis: This issue is due to a stack overflow error in the ActiveX installer that does not properly handle overly large values passed to certain parameters, which could be exploited by attackers to execute arbitrary commands by tricking a user into visiting a malicious Website with Shockwave content that prompts the user to install the player. Affected products: Macromedia Shockwave Player version 10.1.0.11 and prior. Solution: The vendor has fixed the issue in the Shockwave Player ActiveX installer. Note: Since the vulnerability occurs in the installer, no action needs to be taken by users.

Category 23.6 *Web-site infrastructure, general Web security issues*

2006-03-01 **vulnerability update Apache Web server Sun Solaris 8 9 execute arbitrary code workaround**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2006/0789 23

SUN SECURITY UPDATE FIXES MULTIPLE APACHE WEB SERVER VULNERABILITIES.

A vulnerability in the Apache 1.3 Web server bundled with Solaris 8 and 9 may allow a local user who is able to create e SSI documents which are served by Apache to execute arbitrary code with the privileges of the Apache 1.3 process. The Apache HTTP process normally runs as the unprivileged user "nobody" (uid 60001). Analysis: This vulnerability affects the Apache 1.3 Web server bundled with Solaris 10 which may prevent certain configured security features from being applied to specific HTTP transactions when Apache is configured to use SSL. The second vulnerability in the Apache 1.3 Web server may allow local or remote unprivileged users to bypass security protections associated with some network transactions, corrupt information stored in a Web cache, or perform cross site scripting activities when the Apache Web server is configured to run as a proxy. Affected products: Sun Solaris 8, Sun Solaris 9, and Sun Solaris 10. Solution: Until patches are available, upgrade to the latest versions of Apache and mod_ssl as an interim workaround.

Category 23.6 *Web-site infrastructure, general Web security issues*

2006-03-01 **IBM WebSphere Application Service source code disclosure vulnerability**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2006/0788 23

IBM WEBSPHERE APPLICATION SERVER SOURCE CODE DISCLOSURE VULNERABILITY.

A vulnerability has been identified in IBM M WebSphere Application Server, which can be exploited by remote attackers to gain knowledge of sensitive information. Analysis: The flaw is due to an input validation error when processing malformed HTTP requests containing a specially crafted filename extension, which could be exploited by remote attackers to display the source code of arbitrary JavaServer pages (JSP) instead of an expected HTML response. Affected products: IBM WebSphere Application Server version 5.1.1.4 through 5.1.1.9; IBM WebSphere Application Server version 5.0.2.10 through 5.0.2.15. Solution: Upgrade to version 5.0.2.16 or 5.1.1.10 (when available) or apply Interim fixes: http://www-1.ibm.com/support/docview.wss?rs=180&uid=swg27004980

Category 23.6 *Web-site infrastructure, general Web security issues*

2006-03-04 **Microsoft IIS Web server authentication method disclosure vulnerability no patch solution**

DHS IAIP Daily; http://www.securityfocus.com/bid/4235/references 23

MICROSOFT IIS AUTHENTICATION METHOD DISCLOSURE VULNERABILITY.

Microsoft IIS supports Basic and NTLM authentication. Reportedly, the authentication methods supported by a given IIS server can be revealed to an attacker through the inspection of returned error messages, even when anonymous access is also granted. Analysis: When a valid authentication request is submitted for either message with an invalid username and password, an error message will be returned. This happens even if anonymous access to the requested resource is allowed. An attacker may be able to use this information to launch further intelligent attacks against the server, or to launch a brute-force password attack against a known username. For a complete list of vulnerable products: http://www.securityfocus.com/bid/4235/info. Solution: Currently the Security Focus staff is not aware of any vendor-supplied patches for this issue.

Category 23.6 *Web-site infrastructure, general Web security issues*

2006-03-11 **Apple QuickTime iTunes integer heap overflow vulnerabilities Mac OS X Microsoft Windows releases affected no solution**

DHS IAIP Daily; http://www.securityfocus.com/bid/17074 23

APPLE QUICKTIME/ITUNES INTEGER AND HEAP OVERFLOW VULNERABILITIES.

An integer overflow and heap-based buffer overflow vulnerability have been reported in Apple QuickTime and iTunes. These issues affect both Mac OS X and Microsoft Windows releases of the software. Analysis: A successful exploit will result in execution of arbitrary code in the context of the currently logged in user. Vulnerable: Apple QuickTime Player 7.0.4; Apple QuickTime Player 7.0.3; Apple iTunes 6.0.2; Apple iTunes 6.0.1. Solution: Security Focus is currently not aware of any vendor-supplied patches for this issue.

Category 23.6 *Web-site infrastructure, general Web security issues*

2006-03-15 **Adobe Graphics Server interactive login configuration remote arbitrary code execution attack**

DHS IAIP Daily; http://securitytracker.com/alerts/2006/Mar/1015769.html 23

ADOBE GRAPHICS SERVER INTERACTIVE LOGIN CONFIGURATION LETS REMOTE USERS EXECUTE ARBITRARY CODE.

A vulnerability was reported in Adobe Graphics Server. A remote user can cause arbitrary code to be executed on the target system. Analysis: When configured according to vendor recommendations, a remote user may be able to cause arbitrary code to be executed on the target system. The remote user can load arbitrary code onto the server such that it will be executed the next time an interactive user login occurs. The code will run with the privileges of the Adobe Server service account. On some systems, this may be system level privileges. Only Windows based systems are affected. Vulnerable versions: Version(s): 2.0, 2.1. Solution: The vendor recommends following a manual hardening process as well as restricting interactive logins to the service account for the server (adbeserv) by using local security policies. The vendor's advisory describes the service account restriction steps and is available at: http://www.adobe.com/support/techdocs/332989.html

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2006-03-15 **IBM Tivoli Lightweight Client Framework information disclosure vulnerability solution configuration change**

DHS IAIP Daily; http://www.securityfocus.com/bid/17085/references 23

IBM TIVOLI LIGHTWEIGHT CLIENT FRAMEWORK INFORMATION DISCLOSURE VULNERABILITY.

Tivoli Lightweight Client Framework (LCF) is prone to an information disclosure vulnerability. Analysis: The HTTP interface of Tivoli LCF allows an authenticated user to have read access to files with root authority by manipulating the configuration of log files. Vulnerable: IBM Tivoli Lightweight Client Framework 3.7.1. Solution: The vendor has released an advisory along with configuration parameters to resolve this issue. For further detail: http://www-1.ibm.com/support/docview.wss?rs=0&q1=vulnerability+OR+vulnerabilities&uid=swg21082896&loc=en_US&cs=utf-8&cc=us&lang=en

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2006-03-15 **Flash Player browser plugin arbitrary code execution vulnerabilities solution update**

DHS IAIP Daily; http://secunia.com/advisories/19218/ 23

FLASH PLAYER UNSPECIFIED CODE EXECUTION VULNERABILITIES.

Some vulnerabilities have been reported in Flash Player, which can be exploited by to compromise a user's system. Analysis: The vulnerabilities are caused due to unspecified errors and can be exploited to execute arbitrary code on a user's system when a malicious SWF file is loaded. Affected software: Macromedia Breeze 4.x; Macromedia Breeze 5.x; Macromedia Breeze Meeting Add-In; Macromedia Flash 8.x; Macromedia Flash MX 2004; Macromedia Flash MX Professional 2004; Macromedia Flash Player 7.x; Macromedia Flash Player 8.x; Macromedia Flex 1.x; Shockwave Player 10.x. Solution: Install updated versions. Flash Player 8.0.22.0 and earlier: Update to version 8.0.24.0 or 7.0.63.0. http://www.macromedia.com/go/getflash Flash Player 8.0.22.0 and earlier -- network distribution: Update to version 8.0.24.0 or 7.0.63.0.
http://www.macromedia.com/licensing/distribution Flash Professional 8, Flash Basic: Update to version 8.0.24.0.
http://www.macromedia.com/support/flash/downloads.html Flash MX 2004: Update to version 7.0.63.0.
http://www.macromedia.com/support/flash/downloads.html Flex 1.5: Update to version 8.0.24.0.
http://www.macromedia.com/go/3d2855d6 Breeze Meeting Add-In: Update to version 7.0.55.331 (Win) or 7.0.55.118 (Mac).
http://adobe.breezecentral.com/common/help/en/support/downlo ads.htm Shockwave Player: Update to version 10.1.1.
http://www.macromedia.com/shockwave/download/

Category 23.6 *Web-site infrastructure, general Web security issues*

2006-03-27 **Symantec Veritas NetBackup multiple daemons remote buffer overflow vulnerabilities solution update**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2006/1124 23

SYMANTEC VERITAS NETBACKUP MULTIPLE DAEMONS REMOTE BUFFER OVERFLOW VULNERABILITIES.

Multiple vulnerabilities have been identified in Veritas NetBackup Master, Media Servers and clients, which could be exploited by remote attackers to take complete control of an affected system. Analysis: The first issue is due to a buffer overflow error in the volume manager daemon (vmd.exe) that does not properly handle malformed data sent to port 13701/TCP, which could be exploited by remote attackers to execute arbitrary commands. The second flaw is due to a buffer overflow error in the NetBackup Database Manager service (bpdbm.exe) that does not properly handle malformed data sent to port 13721/TCP, which could be exploited by remote attackers to compromise a vulnerable system. The third vulnerability is due to a buffer overflow error in the VERITAS Network Daemon (vnetd) that does not properly handle specially crafted messages sent to port 13724/TCP, which could be exploited by attackers to execute arbitrary commands. See source advisory for a complete list of vulnerable products. Solution: Apply security updates: http://seer.support.veritas.com/docs/281521.htm

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2006-04-13 **Apache mod_ssl CRL handling off by one buffer overflow vulnerability memory corruption solution update**

DHS IAIP Daily; http://www.securityfocus.com/bid/14366/discuss 23

APACHE MOD_SSL CRL HANDLING OFF BY ONE BUFFER OVERFLOW VULNERABILITY.

Apache's mod_ssl is prone to an off by one buffer overflow condition. The vulnerability arising in the mod_ssl CRL verification callback allows for potential memory corruption when a malicious CRL is handled. Analysis: Several vulnerabilities in the Apache 2.0 Web server prior to version 2.0.55 may allow a local or remote unprivileged user to cause a denial-of-service to the Apache 2 HTTP process, or may allow a local user who is able to write to directories served by the Web server to execute arbitrary code with the privileges of the Apache 2 process. The Apache 2 HTTP process normally runs as the unprivileged user "webservd" (uid 80). For a complete list of vulnerable products: http://www.securityfocus.com/bid/14366/info Solution: The vendor has addressed this issue in version 2.0.55 of the 2.0 branch. Users are advised to obtain the available update. Please see the referenced vendor advisories for further information: http://www.securityfocus.com/bid/14366/references

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2006-04-13 **Adobe Document Server multiple remote vulnerabilities solution update**

DHS IAIP Daily; http://www.securityfocus.com/bid/17500/discuss 23

ADOBE DOCUMENT SERVER FOR READER EXTENSIONS MULTIPLE REMOTE VULNERABILITIES.

Adobe Document Server for Reader Extensions, included with Graphics Server and Document Server, is prone to multiple vulnerabilities. Analysis: When using Adobe Document Server for Reader Extensions 6.0, a user's session ID is included in the URL ("jsessionid" parameter) and is exposed to other Websites in the "Referer:" header. It is possible that a malicious person might monitor a company's Internet traffic to steal the sessionid directly from the URL. That session ID could be used by the malicious person to gain a copy of the PDF file that a legitimate user is processing with Reader Extensions. Vulnerable products: Adobe Graphics Server 2.1 and Adobe Document Server 6.0. Solution: Adobe has released advisories and updated software to address these issues. Please see the referenced advisories for further information: http://www.securityfocus.com/bid/17500/references

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2006-04-13 **Apache HTTP request smuggling vulnerability solution update**

DHS IAIP Daily; http://www.securityfocus.com/bid/14106/discuss 23

APACHE HTTP REQUEST SMUGGLING VULNERABILITY.

Apache is prone to an HTTP request smuggling attack. Analysis: A specially crafted request with a "Transfer Encoding: chunked" header and a "Content Length" header can cause the server to forward a reassembled request with the original "Content Length" header. As a result, the malicious request may piggyback on the valid HTTP request. This attack may result in cache poisoning, cross site scripting, session hijacking, and other attacks. If the described issues have been exploited to cause a denial-of-service condition, the Apache Web Server may be slow to respond to requests or may not respond at all. There are no predictable symptoms that would indicate any of the described issues have been exploited to gain unauthorized access to a host or its data. For a complete list of vulnerable products: http://www.securityfocus.com/bid/14106/info Solution: The vendor has released Apache 2.1.6 to address this issue in the 2.1.x branch. The vendor addressed this issue for earlier versions as well: version 2.0.55 of the 2.0 branch and version 1.3.34 of the 1.3 branch. Please see the referenced vendor advisories for further information: http://www.securityfocus.com/bid/14106/references

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2006-05-08 **IBM WebSphere Application Server welcome page security restriction bypass vulnerability solution update**

DHS IAIP Daily; http://www.securityfocus.com/bid/17900/discuss 23

IBM WEBSPHERE APPLICATION SERVER WELCOME PAGE SECURITY RESTRICTION BYPASS VULNERABILITY.

IBM WebSphere Application Server is prone to a security restriction bypass vulnerability. Analysis: This issue is due to a failure of the application to properly enforce security restrictions and users who try to access the welcome page of their application by giving the default context root in the browser. Vulnerable: IBM Websphere Application Server 6.0.2. Solution: IBM has released fixes and an advisory to address this issue. For information on obtaining fixes: http://www.securityfocus.com/bid/17900/references

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2006-05-09 **Cisco Websense Enterprise Web filtering bypass vulnerability**

DHS IAIP Daily; http://www.securiteam.com/securitynews/5MP042KIKC.html 23

WEBSENSE ENTERPRISE WEB FILTERING BYPASS.

A Websense Enterprise vulnerability exists primarily due to the manner in which Cisco PIX and other Cisco filtering devices handle split packets in conjunction with Websense Enterprise integration. For each HTTP request the Cisco PIX or other Cisco device forwards individual packets to Websense to determine whether or not the request should be permitted. Vulnerable systems: Cisco PIX software version 6.3; Cisco PIX ASA version 7; Cisco FWSM software version 2.3; Cisco FWSM software version 3.1. Proof of concept: http://www.vsecurity.com/tools/WebsenseBypassProxy.java

---

Category 23.6 *Web-site infrastructure, general Web security issues*

2006-05-10 **Microsoft Flash patch glitch user report workaround**

DHS IAIP Daily; http://www.informationweek.com/news/showArticle.jhtml?articleID=187202029&subSection=Breaking+News 23

USERS REPORT GLITCHES WITH MICROSOFT'S FLASH PATCH.

If, as an analyst suggested Tuesday, May 9, Microsoft plans to begin patching more than its own software, its first effort got off to a rocky start. By Wednesday, May 10, Windows users were complaining of glitches in updating Adobe's Flash Player through the Windows Update service. Microsoft took the unusual step Tuesday of feeding an updated edition of Flash Player to Windows XP, Windows 98, and Windows Millennium users. It was the first time the Redmond, WA, developer took an active role in pushing a third-party product update to users. Microsoft is aware of the problem, which it dubbed a "known issue" in a support document posted Wednesday. The document offers a workaround that requires users to delete a pair of Flash-related files, then manually download and install the Player update.

Category 23.6 *Web-site infrastructure, general Web security issues*

2006-05-11 **Apple QuickTime remote buffer integer overflow vulnerabilities solution upgrade**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2006/1778 23

APPLE QUICKTIME MULTIPLE REMOTE BUFFER AND INTEGER OVERFLOW VULNERABILITIES.

Multiple vulnerabilities were identified within Apple QuickTime, which could be exploited by remote attackers to take complete control of an affected system. Analysis: Integers overflow error when processing malformed JPEG images could be exploited by remote attackers to execute arbitrary commands via a malicious Webpage. Remote attackers could successfully execute arbitrary commands that may initiate integer overflow errors from malformed QuickTime movies obtained from a malicious Website. Affected products: Apple QuickTime versions prior to 7.1 (Mac OS X and Windows). Solution: Upgrade to Apple QuickTime version 7.1: http://www.apple.com/support/downloads/quicktime71.html

---

23.7 VoIP

Category 23.7 *VoIP*

2003-02-24 **Session Initiation Protocol SIP new vulnerabilities exploit software CERT CC advisory**

NIPC/DHS

February 21, CERT/CC — CERT Advisory CA-2003-06: Multiple vulnerabilities in implementations of the Session Initiation Protocol (SIP).

The Session Initiation Protocol (SIP) is a developing and newly deployed text-based protocol that is commonly used in Voice over IP (VoIP), Internet telephony, instant messaging, and various other applications. Numerous vulnerabilities have been reported in multiple vendors' implementations of the SIP. These vulnerabilities may allow an attacker to gain unauthorized privileged access, cause denial-of-service attacks, or cause unstable system behavior. SIP-enabled products from a wide variety of vendors are affected. Other systems making use of SIP may also be vulnerable but were not specifically tested. Not all SIP implementations are affected. Detailed instructions for resolving this issue may be found in this advisory on the CERT/CC Website. To determine if your product is vulnerable please refer to CERT/CC Vulnerability Note VU#528719 at http://www.kb.cert.org/vuls/id/528719

Category 23.7 *VoIP*

2004-01-14 **VoIP voice over IP flaw weakness hole exploit text messaging Microsoft Cisco crash denial of service DoS**

RISKS; http://news.com.com/2100-1002_3-5140284.html?tag=nefd_lede 23 21

FLAWS THREATEN VoIP NETWORKS

Peter G. Neumann produced this abstract of an article by Robert Lemos in CNET News:

A technical review conducted by the British government has found several security flaws in products that use VoIP and text messaging, including those from Microsoft and Cisco Systems. The flaws affect software and hardware that support the real-time multimedia communications and processing standard, known as the International Telecommunications Union (ITU) H.323 standard.

The security problems can cause a product that supports H.323 to crash. For example, in Cisco telecommunications products running its IOS operating system, the vulnerability could be used to cause the devices to freeze or reboot. However, on Microsoft's Internet Security and Acceleration Server 2000, which is included with Small Business Server 2000 and 2003 editions, the vulnerability could allow an attacker to take control of the system.

Category 23.7 *VoIP*

2004-01-15 **CERT CC advisorty message vulnerability flaw patch fix**

NIPC/DHS; http://www.cert.org/advisories/CA−2004−01.html

January 13, CERT/CC, NISCC — CERT Advisory CA-2004-01 Multiple H.323 Message Vulnerabilities.

The U.K. National Infrastructure Security Co-ordination Centre has reported multiple vulnerabilities in different vendor implementations of the multimedia telephony protocol H.323. H.323 is an international standard protocol, published by the International Telecommunications Union, used to facilitate communication among telephony and multimedia systems. Examples of such systems include VoIP, video-conferencing equipment, and network devices that manage H.323 traffic. Exploitation of these vulnerabilities may result in the execution of arbitrary code or cause a denial of service, which in some cases may require a system reboot. Systems administrators should apply a patch or upgrade and filter network traffic. Sites should apply network packet filters to block access to the H.323 services at network borders, including 1720/TCP and 1720/UDP. If access cannot be filtered at the network perimeter, the CERT/CC recommends limiting access to only those external hosts that require H.323 for normal operation. Some firewalls process H.323 packets and may themselves be vulnerable to attack. Certain sites may actually want to disable application layer inspection of H.323 network packets. Additional information is available on the Microsoft Website:
http://www.microsoft.com/technet/treeview/default.asp?url=/t echnet/security/bulletin/ms04-001.asp

---

Category 23.7 *VoIP*

2004-01-15 **CERT/CC advisory message vulnerability flaw patch fix VoIP multimedia messaging telephony protocols TCP UDP**

DHS/IAIP Update

CERT ADVISORY CA-2004-01 MULTIPLE H.323 MESSAGE VULNERABILITIES.

The U.K. National Infrastructure Security Coordination Centre has reported multiple vulnerabilities in different vendor implementations of the multimedia telephony protocol H.323. H.323 is an international standard protocol, published by the International Telecommunications Union, used to facilitate communication among telephony and multimedia systems. Examples of such systems include VoIP, video-conferencing equipment, and network devices that manage H.323 traffic. Exploitation of these vulnerabilities may result in the execution of arbitrary code or cause a denial of service, which in some cases may require a system reboot. Systems administrators should apply a patch or upgrade and filter network traffic. Sites should apply network packet filters to block access to the H.323 services at network borders, including 1720/TCP and 1720/UDP. If access cannot be filtered at the network perimeter, the CERT/CC® recommends limiting access to only those external hosts that require H.323 for normal operation. Some firewalls process H.323 packets and may themselves be vulnerable to attack. Certain sites may actually want to disable application layer inspection of H.323 network packets. Additional information is available on the Microsoft Website:
http://www.microsoft.com/technet/treeview/default.asp?url=/t echnet/security/bulletin/ms04-001.asp

---

Category 23.7 *VoIP*

2004-01-23 **Cisco voice product security flaw vulnerability patch fix**

NIPC/DHS; http://www.cisco.com/warp/public/707/cisco-sa-20040121-voice.shtml

January 22, earthweb.com — Cisco warns of voice product security flaws.

Cisco on Thursday, January 22, warned of a default installation vulnerability in multiple voice products running on the IBM platform that leaves TCP and UDP ports open to malicious attack. Cisco said the security flaw could be exploited to cause denial-of-service attacks and administrative takeover. According to the Cisco advisory, the vulnerable voice products running on IBM servers install the Director Agent insecurely by leaving the service on port 14247 (both TCP and UDP) accessible without requiring user authentication. In addition to leaving the products susceptible to administrative takeover, a malicious attacker could make the IBM Director Agent process consume a server's entire CPU resources by scanning it with a network scanner. This advisory underscores the risks that come with the growing dependence on IP-based networks, especially in the enterprise. Specific information on this advisory can be found at:
http://www.cisco.com/warp/public/707/cisco-sa-20040121-voice.shtml

---

Category 23.7 *VoIP*

2004-05-18 **VoIP voice over IP Internet telephony**

http://www.nytimes.com/2004/05/18/technology/18voice.html?th=&pagewanted=print&position=

IBM and Cisco announced their intention to expand their VoIP (Voice over IP) Internet telephony services. VoIP offers increased functionality such as video-conferencing.

[MK notes: expect a whole new realm of hacking / phreaking to arise as VoIP spreads. Shall we call it phacking? As in, "Stop phacking around with my phone calls?"]

Category 23.7 *VoIP*

2004-05-24 **VoIP Voice over IP Internet telephony Juniper Research study**

DHS IAIP Daily; http://www.theregister.co.uk/2004/05/24/voip_market_boom/

May 24, The Register (UK) — VoIP to transform telecoms market.

Internet telephony will make up 12 percent of all telephony revenues in five years time, according to a study by analysts Juniper Research published Friday, May 21. Juniper claims the VoIP (Voice over Internet Protocol) market will contribute $32 billion, out of a total telephony market worth approximately $260 billion, by 2009. Service providers face the challenge of balancing new VoIP revenues against declines in their traditional fixed-line revenues, as flat-rate IP-based voice tariffs replace time and distance related charges. These changes will benefit more nimble service providers. According to Juniper, initial residential use of VoIP will be via a 'PSTN-bypass' through a PSTN interconnect -- this excludes free PC-to-PC or peer-to-peer services that do not offer PSTN interconnect. However in the longer term voice will be offered as part of a service bundle that includes email, Internet access and video telephony. In the enterprise, calls from IP-VPNs (virtual private networks) will also grow quickly as companies take advantage of network convergence to reduce costs. The study is available online: http://www.juniperresearch.com

---

Category 23.7 *VoIP*

2004-06-10 **British Telecom circuit-switched network voice over IP VoIP**

NewsScan

BT TO SHUT DOWN 'CIRCUIT-SWITCHED' NETWORK IN FAVOR OF VOIP

U.K. giant British Telecom will gradually shut down its traditional circuit-switched network and migrate over to technologies that route phone calls over the Internet. The change "will deliver our vision of a converged, multimedia world where our customers can access any communications service from any device, anywhere -- at broadband speed," says BT Wholesale CEO Paul Reynolds. The new system will enable each subscriber to have a single phone number for both mobile and fixed-line services, and will make possible such add-on features as family conference calls, video streaming and voice-activated phones. BT estimates that by the 2008-09 fiscal year, the new network could save it about £1 billion annually. (AP 10 June 2004)

Category 23.7 *VoIP*

2004-06-28 **voice over IP VoIP US consumer use research**

NewsScan

VOIP CATCHING ON

More than 25% of Internet users in the U.S. are aware of VoIP (voice over Internet Protocol) telephony, and 13% of those have considered switching over to Internet telephony for their residential phone service. The new figures from a study conducted by the Pew Internet & American Life
Project and the New Millennium Research Council also show that 11% of Internet users (14 million Americans) have actually made some kind of VoIP phone call. "Anecdotal evidence suggests that the 'pioneering consumer' often faces new technology 'glitches,' but then reaps the benefits and
enjoys being the first on the block with a new gadget," says Pew senior research specialist John Horrigan. The findings suggest that it's not too soon for legislators to begin thinking about the implications of this new technology, says Allen Hepner, NMRC advisory board member: "This
'disruptive technology' is coming to all Americans; it is not a question of 'if,' but 'when.' VoIP also disrupts existing laws and regulations in the telecom arena. Legislators and regulators would be wise to reexamine existing policy sooner rather than later, so as to minimize regulatory uncertainties for business and consumers." (Pew Internet & American Life Project News Release 28 Jun 2004)

Category 23.7 VoIP

2004-07-06 **voice-over-IP VoIP adoption obstacles AT&T**

NewsScan

OBSTACLES TO NET PHONE SERVICE

AT&T says it expects to have 1 million customers for its voice-over-Internet-protocol (VoIP) phone service by the end of next year, and cable-TV company Comcast expects to offer VoIP all its customers by the end of 2006; however, Mark Main of the British consulting firm Ovum warns
that -- although everyone will be using VoIP 10 or 15 years from now -- the road to that point "will be quite varied, quite torturous and not at all clean." Some obstacles in the way: only 27% of U.S. online users have even heard of it; a VoIP subscriber needs a broadband connection, and phone service will be only as good as that broadband connection; prices may go up in the future due to increased regulation and taxes; and VoIP service, which depends on the regular power grid, will fail if grid should fail. (AP/San Jose Mercury News 6 Jul 2004)

Category 23.7 VoIP

2004-08-02 **hackers phone phreaking voice-over-IP VoIP corporate network attack**

DHS IAIP Daily; http://www.nytimes.com/2004/08/02/technology/02virus.html

August 02, New York Times — Hackers are discovering a new frontier:

Internet telephone service. Internet phones break voice conversations into data packets and route them over the Internet, a cheap and more flexible alternative to traditional phone calls that travel over copper wires. But Internet phones and the routers and servers that steer and store the digitized calls are susceptible to bugs, viruses and worms. Already, a few malicious attacks have shut down corporate Internet phone networks, disrupting business at a cost of millions of dollars. With Internet phones, hackers or disgruntled employees with access to a company's phone server can eavesdrop on conversations by surreptitiously installing software that can track voice packets. In theory, hackers can listen in on anyone's conversation, including those of ordinary consumers using a commercial Internet phone service. Hackers, though, are more likely to focus on a business's Internet phone lines to glean information that can be used for profit. Anecdotal evidence and the history of trouble with data networks suggest that it is only a matter time before the number and seriousness of the attacks increases as more companies start digital phone systems and merge them with their data networks.

Category 23.7 VoIP

2004-08-02 **voice-over-IP VoIP hacking phreaking stealing theft service tapping eavesdropping voyeurism**

NewsScan

VOIP -- VOYEURISM OVER INTERNET PROTOCOL?

With businesses and individuals flocking to Internet telephony as a cheap alternative to pricey landline phones, hackers are discovering new opportunities for eavesdropping and making mischief. Tapping phones by hacking into servers and hard drives is much easier than conventional wiretapping and analysts say even though very few incidents have been reported to date, it's just a matter of time. "Once you are running an Internet phone network, all those threats you worry about in the data world will be transferred to the voice world," says one security consultant. "Voice over Internet phones are not in the spotlight of hackers yet, but in this voyeuristic world, if someone can listen in on people's conversations and get a thrill, they will." In addition, voice packets offer new opportunities for disguising and distributing malignant code. "You can spoof a packet and insert myself into a communications flow," says a systems engineer for Mirage Networks. "This kind of threat has been around for a while for data, but now it will move into voice. As you see a broader
acceptance of voice over Internet, you'll see more spoofs." (New York Times 2 Aug 2004)

Category 23.7 VoIP

2004-08-02 **voice-over-IP VoIP outage Vonage**

DHS IAIP Daily; http://zdnet.com.com/2100−1105_2−5293439.html

August 02, CNET News.com — VoIP provider Vonage suffers outage.

Net phone service provider Vonage confirmed that it suffered its first outage in 18 months on Monday, August 2, due to problems at partner Global Crossing. Customers could still receive calls, but a small percentage of Vonage's 200,000 total subscribers couldn't make outbound calls from around 7 a.m. to 8 a.m. PDT, at which time the problem was fixed. Vonage's Website was knocked off the Internet during that time as well, because Global Crossing also hosts the site, according to a Vonage representative. VoIP requires a broadband connection; calls don't dial directly to 911; and if power to a home or office is lost, so is phone service.

Category 23.7 *VoIP*

2004-08-24 **Cisco Internet phone service voice-over-IP VoIP networking**

NewsScan

CISCO SERIOUS ABOUT INTERNET PHONE SERVICE

Computer-networking giant Cisco Systems is acquiring P-Cube, a privately held maker of software for monitoring Internet-protocol network activity, to help Cisco offer service-providers additional products to manage such IP services as voice-over-Internet protocol (VoIP), interactive
gaming, and video-on-demand. (AP/USA Today 24 Aug 2004)

Category 23.7 *VoIP*

2004-10-07 **Skype VoIP voice over IP**

NewsScan; http://www.latimes.com/technology/la-fi-skype7oct07

SKYPE GOES CALLING ON BUSINESSES

Internet telephony service Skype Technologies is turning its attention to small- and medium-size businesses, hoping to duplicate its tremendous success with individual users. "We've been targeting Skype to the individual, not to the residential or business markets. But what we found in a recent survey is that 48% of our customers are people using it for business," says Skype co-founder Niklas Zennstrom. Skype uses filesharing technology to form its network on the fly -- similar to the way that Kazaa filesharing software works. That's no coincidence -- Skype co-founders Zennstrom and Janus Friis are also the original creators of Kazaa. Skype currently counts 12 million users worldwide and last month's introduction of Skype Out -- a service that enables users to make calls to recipients with regular phone service for a minuscule charge -- resulted in an additional 200,000 paying customers. And while up until now, Skype has been offered free, the company's new focus signals a change. "[Zennstrom] is migrating from free services. He's got a revenue plan," says one industry advocate.

Category 23.7 *VoIP*

2004-11-08 **VoIP voice over IP regulation oversight FCC Federal Communications Commission regulation federal jurisdiction**

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/10128196.htm

FCC TO STATES: LEAVE INTERNET PHONE OVERSIGHT TO US

The Federal Communications Commission is planning to declare Internet phone service off-limits to state regulators. Bruce P. Mehlman of the trade group Internet Innovation Alliance says: "The decision before the FCC is critical, and very serious. The question for regulators is: Do we treat it like telecommunications, taxing it and regulating it heavily, or like information technology, keeping our hands off and letting market-based innovation benefit everyone?" But Mark Cooper of the Consumer Federation of America disagrees, saying: "If you let these people avoid their public responsibilities and not pay their fair share for using the network, the people left behind are going to be harmed by rising prices and declining quality." (San Jose Mercury News 8 Nov 2004)

Category 23.7 *VoIP*

2004-11-22 **Kazaa Skype VoIP voice over IP**

NewsScan;
http://news.com.com/Kazaa+offers+unlimited+free+Internet+phone+calls/2110-7352_3-5463440.html

KAZAA OFFERS FREE VOIP CALLS

The latest version of Kazaa software, distributed by Sharman Networks, incorporates Internet telephony software from Skype Technologies, which is also owned by Kazaa founders Niklas Zennstrom and Janus Friis. That means while people are downloading their music they can also make free online calls anywhere in the world. (Reuters/CNet. com 22 Nov 2004)

Category 23.7 *VoIP*

2005-01-06 **National Institute of Standards and Technology NIST concern Voice over IP VoIP security vulnerabilities firewalls encryption report**

DHS IAIP Daily; http://www.fcw.com/fcw/articles/2005/0103/web−voip−01−06−05. asp

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) RAISES CONCERNS ABOUT VOICE OVER INTERNET PROTOCOL (VOIP).

Government administrators may not understand the complexity of installing security systems for Internet telephony, a new government study suggests. Officials at the National Institute of Standards and Technology (NIST) released a January 5 report that examines security vulnerabilities in Internet-based telephone systems and raises concerns about an emerging technology that otherwise appears to offer many advantages over traditional telephone networks. Security concerns described in the report suggest that the cost and complexity of installing such systems is greater than people realize. The report's authors say that security measures such as firewalls and encryption used in traditional data networks are incompatible with current Internet-based telephone systems and can cause serious deterioration in the voice quality possible on such systems. To compensate for the current security vulnerabilities of Voice over Internet Protocol (VoIP) technology, NIST officials made several recommendations in the report. Report: http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-f inal.pdf

---

Category 23.7 *VoIP*

2005-02-07 **VoIP security threats companies VoIPSA TippingPoint networks lists white papers research**

EDUPAGE; http://www.internetnews.com/security/article.php/3469251

VOIP PROVIDERS TACKLE SECURITY THREATS UP FRONT

More than 20 companies involved in voice over Internet protocol (VoIP) tools and technology have formed the VoIP Security Alliance (VOIPSA) to try to stay ahead of security threats to the emerging VoIP market. "The same threats on a data network are also inherent in a VoIP deployment," said Laura Craddick, a spokesperson for TippingPoint, one of the founding members of VOIPSA. "Then there are additional risks in VoIP protocols," she added. With VoIP taking hold in some corporate sectors, and with household adoption of VoIP technology expected to rise from 400,000 to 12 million over the next five years, analysts warn of the need to anticipate threats to VoIP networks and prepare for them. VOIPSA will operate discussion lists, publish white papers, and sponsor research. Aside from TippingPoint, VOIPSA members currently include Alcatel, Avaya, Columbia University, and Symantec. Notably absent are Cisco and Nortel, which the group is actively trying to recruit.

Category 23.7 *VoIP*

2005-02-07 **voice over Internet protocol VoIP security alliance formed VOIPSA Siemens Qwest SANS NIST**

DHS IAIP Daily; http://www.wired.com/news/technology/0,1282,66512,00.html

VOIP SECURITY ALLIANCE FORMED

A new industry group has formed to look at the security threats inherent in voice over Internet protocol (VoIP). The VoIP Security Alliance, or VOIPSA, launched on Monday, February 7. So far, 22 entities, including security experts, researchers, operators and equipment vendors, have signed up. They range from equipment vendor Siemens and phone company Qwest to research organization The SANS Institute. They aim to counteract a range of potential security risks in the practice of sending voice as data packets, as well as educate users as they buy and use VoIP equipment. An e-mail mailing list and working groups will enable discussion and collaboration on VoIP testing tools. Over the past year, experts have repeatedly warned that VoIP abuse is inevitable. The National Institute of Standards and Technology (NIST) put out a report last month urging federal agencies and businesses to consider the complex security issues often overlooked when considering a move to VoIP. NIST is a member of VOIPSA.

Category 23.7 *VoIP*

2005-02-09 **VoIP voice over IP security alliance**

NewsScan; http://online.wsj.com/article/0

COMPANIES BAND TOGETHER TO PROMOTE VoIP SECURITY

A group of more than 20 companies, including 3Com, Alcatel, Avaya, Siemens, Symantec and Ernst & Young, have formed a VoIP Security Alliance to tackle voiceover- IP security problems and strive toward making VoIP as reliable as traditional telephony. Alliance chairman David Endler warns that as businesses embrace VoIP as a cheap alternative to their current phone system, many network operators are unaware that they need to alter their security strategies when they add the service. For instance, traditional firewalls cannot police VoIP traffic, he notes. "VoIP networks really inherit the same cyber-security threats that data networks are today prone to, but those threats take greater severity in some cases," says Endler. (Wall Street Journal 9 Feb 2005)

Category 23.7 *VoIP*

2005-03-20 **VoIP technology hackers phreaking FTC spoofing personal information theft**

EDUPAGE; http://www.wired.com/news/privacy/0,1848,66954,00.html

APPLYING OLD SCAMS TO NEW TECHNOLOGIES

The emergence of voice over Internet protocol (VoIP) phone service has opened a new door for hackers and others to fool users. Using the Internet to transmit phone calls allows callers to spoof Caller ID systems, something that isn't possible with traditional phone service. Although telemarketers are required by the Federal Communications Commission to properly identify themselves, Caller ID spoofing is otherwise not prohibited. As a result, someone can, for example, call Western Union, which requires customers to call from their home phones to initiate money transfers, using a faked source number, and make a fraudulent transfer. In other instances, debt collectors and private investigators use Caller ID spoofing to trick people into answering their phones and possibly divulging information they otherwise would not. Scams similar to e-mail phishing rackets also take advantage of Caller ID spoofing, deceiving people into believing that a caller is at a bank or a financial institution and helping persuade them to reveal personal information to the caller. Wired News, 20 March 2005

Category 23.7 *VoIP*

2005-04-11 **voice over Internet Protocol VoIP security threats warning emergency services targets fire police**

DHS IAIP Daily; http://www.networkingpipeline.com/showArticle.jhtml?articleID=160700231

VoIP SECURITY CHIEF WARNS OF INCREASED SECURITY THREATS

VoIP Security Alliance Chairman, David Endler, says that threats to VoIP are increasing; and emergency services, fire, and police may be targeted. The Voice Over IP Security Alliance (VOIPSA) is the first industry-wide organization devoted to promoting VoIP security. “As VoIP increases in popularity and number of deployments, so will its attractiveness to potential attackers,” Endler observes. “VoIP networks inherit most of the same security threats that traditional data networks have today,” he notes. "However, by adding new VoIP components to an existing data infrastructure, new security requirements are also added: quality of service, reliability, and privacy. We can expect to see over the next year or two VoIP specific attacks emerge that go beyond today's more prevalent data network vulnerabilities." Our reliance on voice communications for basic needs raises the stakes even higher, when you look at emergency services call centers like 911, police and fire departments, Endler says. One of the problems, he says is that “the threats have not been well identified and laid out yet in a coherent manner. That's one of the things VOIPSA is trying to change with one of our first short-term projects, the VoIP Security Threat Taxonomy.” VOIPSA Website: http://www.voipsa.org/

Category 23.7 VoIP

2005-05-27 **VoIP emergency E911 technology FTC providers NTIA**

EDUPAGE; http://chronicle.com/prm/daily/2005/05/2005052701t.htm

UNIVERSITIES UNVEIL 911 VOIP TECHNOLOGY

A group of three universities has announced a project that would allow voice over Internet protocol (VoIP) phone systems to work with 911 calls. Traditional phone networks are connected to 911 networks and, in the event of a 911 call, provide the physical location of the caller. Because VoIP calls are routed over the Internet, which is not connected to 911 networks, making 911 technology work with VoIP has been problematic. The Federal Communications Commission, however, recently issued a ruling that will require VoIP providers to offer 911 service to all customers. The system being developed by Columbia University, Texas A&M University at College Station, and the University of Virginia will provide 911 operators with the caller's location and in some cases would also provide a video image of the caller. Internet2, Cisco Systems, and Nortel are also involved in the project, which is not expected to be complete for another year and a half. Part of the funding for the project came from the National Telecommunications and Information Administration, which is part of the Department of Commerce. Chronicle of Higher Education, 27 May 2005 (sub. req'd)

Category 23.7 VoIP

2005-07-11 **VoIP voice over IP fraud international telephone call sell operations**

RISKS; http://www.usenet.org.uk/uk.telecom.voip.html 23 94

VoIP FRAUD COSTING STARTUPS $MILLIONS IN LOSSES

It's one of the best kept secrets in the Voice over IP industry. The biggest problem facing VoIP providers isn't the specter of costly E911 requirements, overzealous regulators, or even competition from a myriad of sources. The biggest issue is fraud, perpetrated by scammers who take advantage of lax international communications standards and regulations, and make thousands of minutes of calls through carriers - many of them fly-by-night operators - in places such as Afghanistan and Lichtenstein, who charge exorbitant rates for call termination, leaving the originating service provider with sky high bills and no one to charge for them.

VoIP scams have already caused start-ups in the fledgling industry millions of dollars in losses and are blamed, in part, for the recent demise of one service provider. "It is the single largest problem facing providers," says Ravi Sakaria, VoicePulse CEO, "because the development cost associated with addressing the issue is significant enough that it could be prohibitive for the smaller players."

[Carolyn Schuk, writing for VOXILLA.COM]

Category 23.7 VoIP

2005-07-14 **TechWeb eavesdrop VoIP service alerts Secutity ISS X-Force bugs crash CallManager calls**

DHS IAIP Daily; http://www.techweb.com/wire/security/165702369

ATTACKERS COULD EAVESDROP ON CISCO-ROUTED VOIP CALLS

Flaws in Cisco's Voice-over-Internet Protocol (VoIP) software could allow an attacker to bring down the alternative-to-traditional-telephone service, or access the server that initiates and routes Web-based calls, an Atlanta-based security firm said. According to alerts posted online by Internet Security Systems' (ISS) X-Force research team, Cisco's CallManager sports a pair of bugs that could be "reliably exploited" by hackers. The potential result: at best a denial-of-service style crash, at worst, a situation where the attacker could redirect calls at will or even eavesdrop on conversations. By sending specially crafted packets to Cisco CallManager, an attacker could create a heap overflow and crash the system or gain access. ISS said that an exploit wouldn't need any help from a user, pushing the threat into a more dangerous category. Cisco's own advisory includes details on patched editions of CallManager that are ready to download and install.

Category 23.7 *VoIP*

2005-08-09 **George Mason University NSF federal support VoIP tracking defeating eavesdropping technology development**

EDUPAGE; http://news.com.com/2100-7348_3-5825932.htm

UNIV. RECEIVES FEDERAL SUPPORT FOR VOIP TRACKING TECHNOLOGY

The National Science Foundation has given researchers at George Mason University a grant of more than $300,000 to develop a technology that would allow limited eavesdropping on voice over Internet protocol (VoIP) phone calls. Xinyuan Wang, assistant professor of software engineering at the university and principal investigator, has shown that his method can successfully trace VoIP users without their knowledge. As VoIP service has become more common, law enforcement officials have pointed out that they have no way of tapping such phone calls, potentially resulting in a "haven for criminals, terrorists, and spies," according to the Federal Communications Commission. The technology that Wang and his colleagues are working on does not decrypt conversations. It tracks packets as they move from one user to another, allowing authorities to see who is talking to whom, but not to see what they are saying. Wang conceded that "from a privacy advocate's point of view, this is an attack on privacy," but he also noted that "from a police point of view, this is a way to trace things." CNET, 9 August 2005

Category 23.7 *VoIP*

2005-08-25 **denial-of-service DoS Internet phone VoIP FCC emergency 911 compliance**

DHS IAIP Daily; http://www.networkingpipeline.com/showArticle.jhtml?articleId=170100161

INTERNET PHONE PROVIDERS MAY CUT OFF CUSTOMERS

Providers of Internet-based phone services may be forced next week to cut off tens of thousands of customers who haven't formally acknowledged that they understand the problems they may encounter dialing 911 in an emergency. The Federal Communications Commission (FCC) had set the Monday, August 29, deadline as an interim safeguard while providers of Internet calling, also known as "VoIP" for Voice over Internet Protocol, rush to comply with an FCC order requiring full emergency 911 capabilities by late November. The FCC issued its order in May after a series of highly publicized incidents in which VoIP users were unable to connect with a live emergency dispatch operator when calling 911. Vonage, AT&T, and other carriers have indicated that they plan to comply with the FCC deadline to disconnect customers. But Time Warner Cable, the biggest VoIP provider in the cable TV industry with more than 600,000 users, said in its FCC filing that all customers have already been adequately informed about the risk of losing 911 service in a power outage--the primary issue for cable-based VoIP services--and that all have already acknowledged that risk.

Category 23.7 *VoIP*

2005-09-09 **New York City E911 emergency VoIP service nomadic**

DHS IAIP Daily; http://www.govtech.net/magazine/channel_story.php/96576

NEW YORK CITY HAS AN E911 SOLUTION FOR NOMADIC VOIP TELEPHONE SUBSCRIBERS

New York City is now offering an E911 solution for Voice over IP (VoIP) telephone subscribers. This solution addresses a major emergency dialing problem associated with "nomadic" VoIP services. Nomadic services allow subscribers to move their VoIP phones from one location to another with access to a high-speed Internet connection. DoITT Commissioner Gino Menchini stated "The VoIP/911 solution exemplifies what can be accomplished when government and industry work collaboratively." He went on to say that "The VoIP/911 solution exemplifies what can be accomplished when government and industry work collaboratively," said DoITT Commissioner Gino Menchini. "The City of New York recognizes that VoIP offers great potential for new competitive communications services and we encourage its continued growth. At the same time, however, 911 is at the very heart of government's public safety responsibility. I believe this implementation both strengthens the VoIP industry and upholds government's responsibility to protect human life and property."

Category 23.7 VoIP

2005-09-12 **proprietary encryption algorithms VoIP voice over IP vulnerability**

RISKS; http://tinyurl.com/a5kgg; http://tinyurl.com/c58wa (free reg'n req'd) 24 04

PUBLIC CALL FOR SKYPE TO RELEASE SPECIFICATIONS

Andrew Ross Sorkin and Vikas Bajaj wrote in the New York Times, "Skype allows users who download its software and register for its service to talk to one another for free over the Internet. For a company that is a little over two years old, it has already amassed a large global following -- the company says its telephony software has been downloaded 162 million times and it has 53 million registered users, with as many as three million using its service at any given time."

Lauren Weinstein wrote in RISKS,

>eBay's acquisition of Skype (now official) leads to new concerns over the proprietary nature of Skype's security and encryption systems, which will now be under the control of an extremely large and powerful corporate entity. For eBay and Skype to have a chance of maintaining the goodwill and trust of Skype users, I call on Skype to forthwith release the specifications and implementation details of Skype's encryption and related technologies.

This disclosure should ideally be made to the public, but at a minimum to an independent panel of respected security, privacy, and encryption experts, who can rigorously vet the Skype technology and make a public report regarding its security, reliability, and associated issues.<

Category 23.7 VoIP

2005-09-19 **hacker Internet telephony call systems VoIP threat attack vector**

DHS IAIP Daily; http://news.bbc.co.uk/2/hi/technology/4259554.stm

HACKERS TARGET NET CALL SYSTEMS

The biannual Symantec Threat Report is reporting that hackers are starting to turn their attention to the technology behind net phone calls. The Voice over IP (Voip) systems as a technology starting to interest hi-tech criminals and the report predicted that within 18 months, Voip will start to be used as a "significant" attack vector. Voip could resurrect some old hacking techniques as well as using old hacking techniques.

Category 23.7 VoIP

2005-09-19 **VoIP threats report Symantec voice phishing audio spam call hijacking caller-ID spoofing war dialing combing**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4259554.stm

REPORT WARNS OF VOIP THREATS

A new report from security firm Symantec identifies voice over Internet protocol (VoIP) technology as potentially fertile ground for a wave of cybercrime, including a new variation on an old scam. Within the next 18 months, Symantec expects VoIP to become a "significant" channel for electronic mischief including audio spam, voice phishing, call hijacking, and caller-ID spoofing. Ollie Whitehouse, technical manager at Symantec's research labs, said that although few VoIP attacks have been reported so far, the company "believes it's only a matter of time before attackers target it more intensely." A technique called war-dialing, in which computers call many thousands of phone numbers looking for those that respond with data tones, could also see a reemergence with VoIP. Hackers could comb VoIP phone numbers and locate unprotected or poorly protected servers that could then be compromised. BBC, 19 September 2005

Category 23.7 VoIP

2005-09-27 **wiretapping interception VoIP FCC rules considered**

DHS IAIP Daily;
http://management.silicon.com/government/0,39024677,39152744 ,00.htm

VOIP WIRETAPPING RULES TO BE CONSIDERED

The Federal Communications Commission's (FCC) has developed a 59-page decision for Broadband providers and Internet phone services. They now have until spring 2007 to follow a new and complex set of rules designed to make it easier for police to seek wiretaps. This includes that any voice over IP, or VoIP, provider linking with the public telephone network must be wiretap-ready.

Category 23.7 VoIP

2005-09-27 **FCC VoIP emergency services E911 provider deadline**

EDUPAGE;
http://www.siliconvalley.com/mld/siliconvalley/business/technology/12755614.htm

FCC DELAYS 911 VOIP CUSTOMER DISCONNECT AGAIN

The Federal Communications Commission again delayed enforcing a deadline for Internet phone service providers to disconnect customers who have not yet verified that they understand they might not be able to reach an emergency dispatcher when they dial 911 on their cellular phones. The FCC noted that status reports from the VoIP service providers indicated that nearly all subscribers have responded to the prompts. Those providers who have received confirmations from 90 percent or more of their subscribers do not need to meet the disconnect requirement, but must continue to seek complete compliance. Other service providers have until October 31 to reach the 90 percent threshold to avoid disconnecting users. Up to 10,000 subscribers faced disconnection under the original ruling. San Jose Mercury News, 27 September 2005

Category 23.7 VoIP

2005-10-24 **Security VoIP VoIPSA Threat Taxonomy telephony Internet**

DHS IAIP Daily; http://www.networkingpipeline.com/showArticle.jhtml?articleID=172303368

SECURITY GROUP TAKES FIRST MAJOR STEP AGAINST VOIP DANGERS

The Voice over IP Security Alliance (VoIPSA) has announced its VoIP Security Threat Taxonomy, which is a classification and description of the types of security threats that affect IP telephony. Alliance secretary and taxonomy project head Jonathan Zar says that the taxonomy is the first step in dealing with VoIP security. By defining the kinds and nature of threats, VoIPSA hopes to give the Internet voice industry a common reference point to deal systematically with VoIP security issues. The VoIP Security Threat Taxonomy is organized into four broad categories. Two - denial of service and unlawful signal or traffic modification - deal with the integrity of the network signal and infrastructure. Signal interception and bypass of refused consent categorize threats specific to VoIP and deal specifically with privacy. VoIPSA Website: http://www.voipsa.org/

Category 23.7 VoIP

2005-11-07 **FCC Internet phone customer no cutoff VoIP emergency E911**

DHS IAIP Daily;
http://www.boston.com/business/technology/articles/2005/11/08/us_fcc_says_no_cutoff_for_internet_phone_customers/

FEDERAL COMMUNICATIONS COMMISSION SAYS NO CUTOFF FOR INTERNET PHONE CUSTOMERS

According to guidance from the Federal Communications Commission (FCC) released on Monday, November 7, Internet telephone providers will not have to cut off service to U.S. subscribers even if they are not able to receive enhanced 911 (E911) emergency service. Internet telephone providers had worried that the FCC's rules adopted in May would required them to suspend by November 28 service for subscribers who cannot receive E911 service. According to the recently released guidance, existing customers do not have to be disconnected, but Internet telephone providers will have to cease marketing and accepting new customers in areas where they are not connecting 911 calls with the person's location and phone number. The voice-over-Internet-protocol (VOIP) rules adopted in May required 911 calls to be routed to live dispatchers and the caller's location and number be identified. The move followed instances in which customers had trouble reaching help when they dialed 911. The Voice On the Net Coalition, which represents many VOIP providers, said that roughly 750,000 customers could be affected if they had to suspend service to those who did not have enhanced 911 service available. FCC guidance: http://www.fcc.gov/headlines.html

---

Category 23.7 VoIP

2005-11-15 **FCC VoIP emergency E911 Website launch**

DHS IAIP Daily; http://www.govtech.net/news/news.php?id=97263

FEDERAL COMMUNICATIONS COMMISSION LAUNCHES VOIP 911 WEBSITE

The Joint Federal Communications Commission (FCC) and National Association of Regulatory Utility Commissioners (NARUC) Task Force on VoIP 911 Enforcement has launched a new Website to provide consumers, industry, and state and local governments information about the rules that require certain providers of Voice over Internet Protocol (VoIP) services to supply 911 emergency calling capabilities to their customers. FCC Chairman Kevin J. Martin said, "Anyone who dials 911 has a reasonable expectation that he or she will be connected to an emergency operator; this expectation exists whether that person is dialing 911 from a traditional wireline phone, a wireless phone, or a VoIP phone. This new Website will provide an easy way for consumers, industry, and other government agencies to get the most current information on this important issue." FCC/NARUC Task Force website: http://www.voip911.gov

---

Category 23.7 VoIP

2006-01-23 **Cisco product vulnerabilities alert VoIP security**

DHS IAIP Daily; http://www.informationweek.com/security/showArticle.jhtml?articleID=177102457 23

CISCO SECURITY ALERTS SERVE AS VOIP WAKE-UP CALL.

Cisco Systems' revelation last week of two security alerts and fixes for CallManager, the processing component of its voice-over-IP (VoIP) technology, reminds us that while VoIP offers all sorts of benefits, there's no getting around its vulnerability as a software application. CallManager's vulnerability to denial of service attacks and attacks that would let users increase their access privileges seem mild compared with threats aimed at stealing customer data or blocking Website access. But as more voice communication travels over the Internet, reducing that threat becomes increasingly important. Cisco CallManager extends business telephony functions to IP phones, media-processing devices, VoIP network gateways, and multimedia applications. The denial of service and privilege-escalation vulnerabilities, for which patches are available, affect CallManager 3.2 and earlier, and some versions of CallManager 3.3, 4.0, and 4.1. Like Microsoft in the software market, Cisco is likely to be the main target of VoIP hackers because of its market-share leadership. Another danger lies in IT staff inexperience: VoIP hasn't been much of a target for hackers, and gaining the security know-how to protect those networks may not be top of mind during deployments, says Ofir Arkin, chief technology officer of network-management company Insightix Ltd.

Category 23.7 VoIP

2006-01-25 **Skype Vonage VoIP security warning denial of service DoS**

DHS IAIP Daily; http://news.com.com/Skype+could+provide+botnet+controls/2100 −7349_3−6031306.html?tag=cd.top 23

Skype could provide botnet controls.

Internet phone services such as Skype and Vonage could provide a means for cybercriminals to send spam and launch attacks that cripple Websites, experts have warned. Moreover, because many voice over Internet protocol (VoIP) applications use proprietary technology and encrypted data traffic that can't easily be monitored, the attackers will be able to go undetected. "VoIP applications could provide excellent cover for launching denial of service (DoS) attacks," the Communications Research Network said Wednesday, January 25. The Communications Research Network is a joint venture between Cambridge University and the Massachusetts Institute of Technology. The group urges VoIP providers to publish their routing specifications or switch to open standards. "These measures would…allow legitimate agencies to track criminal misuse of VoIP," Jon Crowcroft, a professor at Cambridge University in the UK, said in a statement. VoIP applications such as eBay's Skype and Vonage could give cybercriminals a better way of controlling their zombies and covering their tracks, the Communications Research Network said. "If the control traffic were to be obfuscated, then catching those responsible for DoS attacks would become much more difficult, perhaps even impossible," the group said in a statement.

Category 23.7 VoIP

2006-03-17 **Skype heap overflow vulnerability abort unpredictable behavior solution update voice over IP VoIP**

DHS IAIP Daily; http://www.securityfocus.com/bid/15192/references 23

SKYPE TECHNOLOGIES SKYPE NETWORKING ROUTINE HEAP OVERFLOW VULNERABILITY.

Skype is prone to a heap overflow vulnerability in its networking routines. Analysis: An attacker who sends a stream of specifically crafted network traffic to a Skype client network can cause the client to overwrite part of the heap, including the heap integrity control data. Since the attacker cannot control the address where the data is written, the most likely effect will be that the Skype will abort execution due to an internal error, although other unpredictable behavior is possible. Such a crash will lead to a loss of availability of the Skype application until it is restarted by the user. A complete list of vulnerable products is available in the source advisory. Solution: A fix for Skype for Pocket PC is not currently available. For further solution details: http://www.securityfocus.com/bid/15192/solution

---

Category 23.7 VoIP

2006-04-26 **voice over IP VoIP denial-of-service DoS target warning CRN**

DHS IAIP Daily; http://www.cio−today.com/news/Is−VoIP−the−Next−Target−/story .xhtml?story_id=130004HC857W 23

VOIP MAY BE A FUTURE DENIAL OF SERVICE TARGET.

Although there has yet to be a recognized instance of a VoIP-coordinated Denial of Service (DoS) attack, the Communications Research Network (CRN) says it is only a matter of time before the technique becomes mainstream. The CRN working group on Internet security has discovered a security loophole in VoIP applications that could give criminals operating on the Internet a better way of covering their tracks. According to CRN, VoIP tools could offer good cover traffic for DoS attacks because VoIP runs continuous media over IP packets. The ability to dial in and out of VoIP overlays allows for control of an application via a voice network, making tracing the source of an attack almost impossible. In addition, proprietary protocols inhibit the ability of ISPs to track DoS activity. CRN's Jon Crowcroft suggests that the loophole could be resolved if VoIP providers were to publish their routing specifications or switch over to open standards.

23.8 SMS

Category 23.8 *SMS*

2004-08-03 **airport airline security short message service SMS check-in passenger**

NewsScan

SINGAPORE AIRLINES INTRODUCES SMS CHECK-IN

Passengers on Singapore Airlines will now be able to check in for flights by sending a text message on their mobile phones. The short message service (SMS) function is the latest use of technology that Singapore Airlines has introduced to make checking in easier and quicker, adding to Internet, mobile phone and fax facilities. After checking in remotely, passengers need to pick up their boarding passes and check in their luggage on the day of departure from a dedicated counter, rather than wait in regular queues. (The Age 3 Aug 2004) rec'd from John Lamp, Deakin U.

23.9 PERL, CGI scripts

Category 23.9 *PERL, CGI scripts*

2000-03-24 **credit-card fraud QA quality assurance CGI programming error vulnerability hole**

RISKS 20 85

Martin Minow, a regular contributor to the RISKS Forum, reported on vulnerabilities in Perl scripts used to accept credit-card information from consumers. Apparently, in many cases, a simple "update account" will reveal the latest versions of these forms as recently filled in by a customer. The vulnerability results from leaving the CGI script world-readable and in a world-readable directory, just as the vendor supplied it by default. [Moral: always check the default values for adequate security and secure your resources according to your own needs.]

Category 23.9 *PERL, CGI scripts*

2003-11-14 **BEA Tuxedo Administration vulnerability fix patch Fortune 500 software denial-of-service**

NIPC/DHS

November 10, Information Security — BEA Tuxedo Administration vulnerability requires fix.

Thousands of customers in Fortune 500 enterprises are urged to patch or upgrade to remedy a security issue in BEA Tuxedo Administration Console. A problem with processing input arguments can allow denial of service, disclosure of file system information or cross-site scripting. BEA Tuxedo provides middleware for building scalable enterprise applications in heterogeneous, distributed environments. The BEA Tuxedo administration console is a CGI application for remote administration of Tuxedo functions. Vulnerable versions include BEA Tuxedo 8.1 and prior. A patch is available for Tuxedo 8.1, and previous versions should be upgraded to 8.1:
http://edocs.bea.com/tuxedo/tux81/install/insadm.htm

Category 23.9 *PERL, CGI scripts*

2005-01-19 **AWStats two vulnerabilities command execution vulnerabilities Perl CGI script**

DHS IAIP Daily; http://secunia.com/advisories/13893/

AWSTATS "CONFIGDIR" PARAMETER ARBITRARY COMMAND EXECUTION

Two vulnerabilities have been reported in AWStats, where one has an unknown impact and the other can be exploited by malicious people to compromise a vulnerable system. Input passed to the "configdir" parameter is not sanitized before being used as an argument to the "open()" Perl routine. This can be exploited to execute arbitrary commands with the privileges of the web server by passing these as input together with certain shell meta-characters. Successful exploitation requires that the application is running as a CGI script. Update to version 6.3: http://awstats.sourceforge.net/#DOWNLOAD

Category 23.9 *PERL, CGI scripts*

2005-02-11 **perl suid wrapper vulnerabilities code execution privilege escalation update issued**

DHS IAIP Daily; http://www.securityfocus.com/archive/1/390215

VULNERABILITIES IN PERL-SUID WRAPPER

Vulnerabilities leading to file overwriting and code execution with elevated privileges have been discovered in the perl-suid wrapper. A local attacker could set the PERLIO_DEBUG environment variable and call existing perl-suid scripts, resulting in file overwriting and potentially the execution of arbitrary code with root privileges. Users should upgrade to the latest version of Perl.

[Note: "cross-site scripting:" Causing a user's Web browser to execute a malicious script. One approach is to hide code in a "click here" hyperlink attached to a URL that points to a non-existent Web page. When the page is not found, the script is returned with the bogus URL, and the user's browser executes it. -- from the Computer Desktop Encyclopedia, v18.2. See < http://www.computerlanguage.com >]

Category 23.9 *PERL, CGI scripts*

2005-07-14 **FrSIRT WPS Web Portal System command arbitrary input validation error filter parameter**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1099

WPS WEB-PORTAL-SYSTEM "WPS_SHOP.CGI" REMOTE COMMAND EXECUTION

A vulnerability was identified in WPS Web-Portal-System, which may be exploited by remote attackers to execute arbitrary commands. This flaw is due to an input validation error in the "wps_shop.cgi" script that does not properly filter a specially crafted "art" parameter, which may be exploited by remote attackers to execute arbitrary commands via the pipe character. WPS Web-Portal-System version 0.7.0 and prior The FrSIRT is not aware of any official supplied patch for this issue.

24 Operating systems, network operating systems,TCP/IP problems (alerts & improvements)

Category 24 *Operating systems, network operating systems,TCP/IP problems (alerts & im*

1997-02-12 **NT**

RISKS 18 82

Christopher Klaus describes three classes of attacks on NT systems:

* NT CPU Port Attacks
* NT DNS Denial Attack
* NT Trojan Password DLL

Category 24 *Operating systems, network operating systems,TCP/IP problems (alerts & im*

1997-04-01 **Windows NT passwords**

EDUPAGE

A superzap utility for Windows NT was announced that allows decryption of encrypted password files.

Category 24 *Operating systems, network operating systems,TCP/IP problems (alerts & im*

1997-06-20 **hack Windows NT Web server URL denial of service**

C|Net http://www.news.com

Hackers informed Microsoft of a major bug in Windows NT 4.0 running Microsoft's Internet Information Server version 3.0 and promptly shut down Microsoft's Web site by typing in a specific URL in any Web browser. Todd Fast (uncertain if this is a real name or a handle), claiming to have discovered the bug, wrote, "This is a hugely embarrassing bug for Microsoft in my opinion, particularly since they've just been lauded for pulling ahead of Netscape in Web server market. Knowing that anyone with a grudge and a twitchy keyboard could shut down any of their customer's Web sites must bear horribly on their collective conscience." Microsoft had a patch available within a day of the discovery.

Category 24 *Operating systems, network operating systems,TCP/IP problems (alerts & im*

1998-04-02 **survey vulnerabilities Windows NT database service holes**

RISKS 19 65

Shake Communications of Melbourne, Australia released a report on the top 104 vulnerabilities in Windows NT that allow criminal hackers to penetrate such networks. The company maintains a vulnerability database available by subscription (see <http://www.shake.net>) and also noted that Microsoft maintains a roster of free patches for known vulnerabilities.

Category 24 *Operating systems, network operating systems,TCP/IP problems (alerts & im*

1998-11-30 **bug vulnerability Windows NT attack Web site hacker**

PC Week http://www.zdnet.com/pcweek/stories/printme/0,4235,374497,00.html

A criminal hacker (or hacker supporter) calling himself Vitali Chkliar put up a Web site that demonstrated the vulnerabilities of Windows NT servers configured without adequate regard for security. The problem was confirmed by PC Week labs. Microsoft officials dismissed the site, saying that there was no bug; the problem was default settings.

Category 24 *Operating systems, network operating systems,TCP/IP problems (alerts & im*

1998-12-01 **Windows NT vulnerability flaw bug weakness hole flaw exploit**

InfoWorld http://www.infoworld.com/cgi-bin/displayStory.pl?98121.wcntbug.htm

In Novermber, after Microsoft released its Service Pack 4 for Windows NT 4.0, another security vulnerability was discovered and patched. The "Named Pipes Over RPC" flaw allowed hackers to provoke a denial-of-service attack on an NT 4.0 system by opening multiple named pipe connections to Remote Procedure Call (RPC) services and sending random data. The result of attack on various system services was consumption of all CPU resources and saturation of RAM — in other words, a denial of service. Fixes appeared in December.

Category 24 *Operating systems, network operating systems,TCP/IP problems (alerts & im*

1998-12-15 **Internet protocols DARPA research development protocols**

PR Newswire

Network Associates Inc. won several multimillion dollar contracts for DARPA (Defense Advanced Research Projects Agency) developments of secure internetworking protocols. These contracts continue the close relationship developed over many years between DARPA and the former Trusted Information Systems (TIS) Advanced Research and Engineering Division; TIS was acquired by NAI in 1998.

Category 24 *Operating systems, network operating systems,TCP/IP problems (alerts & im*

1999-01-12 **bug time calendar operating system Microsoft Windows**

ZDNN http://www.zdnet.com/zdnn/stories/news/0,4586,2186402,00.html

In January 1999, Microsoft admitted that its Windows 95, Windows 98 and Windows NT operating systems contained a bug in the MSVCRT.DLL file that would delay the start of daylight savings time by a week on April 1 2001. The "April Fool's bug" would affect about 95% of all PCs in the world but should be fixed by patches that were posted on the WWW by Microsoft.

Category 24 *Operating systems, network operating systems,TCP/IP problems (alerts & im*

1999-02-23 **criminal hackers white-hat gray-hat Windows NT vulnerability hole**

OTC

What a newspaper writer called "The benevolent hackers of L0pht Heavy Industries" announced another Windows NT vulnerability. They warned Microsoft that editing the system cache would allow substitution of privileged DLLs by hacked versions that could do anything.

Category 24 *Operating systems, network operating systems,TCP/IP problems (alerts & im*

1999-02-23 **threats operating systems utilities vulnerabilities reports alerts**

CERT-CC Summary http://www.cert.org/summaries/CS-99-01.html 99 01

CERT Summary CS-99-01 (February 23, 1999) reported continuing threats from widespread scans, BackOrifice and NetBus, Trojan horse programs and FTP buffer overflows.

Category 24 *Operating systems, network operating systems,TCP/IP problems (alerts & im*

1999-05-25 **threats operating systems utilities vulnerabilities reports alerts**

CERT-CC Summary http://www.cert.org/summaries/CS-99-02.html 99 02

CERT Summary CS-99-02 (May 25, 1999) reported threats from new viruses, a resurgence of SYN flooding attacks, continued widespread automated scans and Web server attacks.

Category 24 *Operating systems, network operating systems,TCP/IP problems (alerts & im*

1999-06-17 **buffer overflow security flaw response publication patch**

LA Times

ECompany.com notified Microsoft of a serious (CERT-CC severity rating 95th percentile) security flaw allowing a buffer overflow to compromise MS Internet Information Server 4.0; vulnerabilities included complete access to all files on a server. The warning was apparently ignored, the tiny company published news of the problem and criticized the giant firm for failing to take security seriously.

Category 24 *Operating systems, network operating systems,TCP/IP problems (alerts & im*

1999-07-26 **buffer overflow UNIX calendar CERT-CC alert**

New York Times

CERT-CC issued an alert on buffer overflow vulnerabilities on several UNIX systems, including Solaris and HP-UX. Using this violation of memory array restrictions, criminal hackers can plant logic bombs and back doors on victimized systems. Manufacturers scrambled to provide patches.

Category 24 *Operating systems, network operating systems,TCP/IP problems (alerts & im*

1999-08-31 **threats operating systems utilities vulnerabilities reports alerts**

CERT-CC Summary http://www.cert.org/summaries/CS-99-03.html 99 03

CERT Summary CS-99-03 (August 31, 1999) reported threats and vulnerabilities from RPC, continued virus and Trojan horse activity, and continued widespread scans. In addition, the Summary provided information about the new CERT PGP key.

Category 24 *Operating systems, network operating systems,TCP/IP problems (alerts & im*

1999-11-23 **threats operating systems utilities vulnerabilities reports alerts**

CERT-CC Summary http://www.cert.org/summaries/CS-99-04.html 99 04

Topics in this regularly scheduled CERT Summary include distributed intruder tools and vulnerabilities related to CDE, BIND, WU-FTP, AMD, and RPC.

Category 24 *Operating systems, network operating systems,TCP/IP problems (alerts & im*

1999-12-17 **threats operating systems utilities vulnerabilities reports alerts**

CERT-CC Summary http://www.cert.org/summaries/CS-99-05.html 99 05

The CERT-CC issued a special edition of the CERT Summary. Topics included the Year 2000 and distributed-system intruder tools. The Summary also notified users of the new Current Activity Web page, "with a regularly updated summary of the most frequent, high-impact types of security incidents and vulnerabilities currently being reported to the CERT/CC. It is available from < http://www.cert.org/current/current_activity.html >.

Category 24 *Operating systems, network operating systems,TCP/IP problems (alerts & im*

2000-03-21 **threats operating systems utilities vulnerabilities reports alerts**

CERT Summary CS-2000-01 http://www.cert.org/summaries/CS-2000-01.html 00 01

The first edition of the CERT-CC Summary for the year 2000 included warnings of Distributed Denial-of-Service Developments, BIND Vulnerabilities, Multiple Vulnerabilities in Vixie Cron, Root Compromises, and Malicious HTML Tags Embedded in Client Web Requests.

Category 24 *Operating systems, network operating systems,TCP/IP problems (alerts & im*

2000-04-09 **software open-source**

NewsScan, San Jose Mercury News
http://www.sjmercury.com/svtech/news/breaking/reuters/docs/408434l.htm

Intel plans to use the Web to give away advanced security software based on industry-standard security functions known as the Common Data Security Architecture. A report in the Wall Street Journal says Intel will begin making the software available by mid-May. (Reuters/San Jose Mercury News 9 Apr 2000)

Category 24 *Operating systems, network operating systems,TCP/IP problems (alerts & im*

2002-01-19 **operating system push-pop stack buffer overflows design**

RISKS 21 87

Earl Boebert wrote a succinct summary of how easy it would be to prevent buffer overflows if any of several possible well-known designs were used in today's operating systems:
>In my view, attempts to close the buffer overflow vulnerability through software or compiler tricks are doomed to one degree of failure or another because you're trying to program around a stupid processor design. Certain contemporary processors actually host a Pantheon of stupidities, consisting of a Greater Stupidity and two handmaiden Lesser Stupidities.

Greater Stupidity: Read access implying execute access. Any piece of data that the processor can be tricked into loading into the command register immediately becomes code. This is a stupidity of such breadth and depth that it comes with an event horizon.

Lesser Stupidity I: Segmented addressing that isn't. Let's say you have an addressing scheme consisting of segment number plus offset. This raises the question of what to do when, in executing code, block moves, etc., the offset gets counted up to maximum length plus one. Smart answer: take a fault. Dumb answer: set offset to zero and count up one in segment number.

Lesser Stupidity II: Brain-dead stack design. If you enumerate the design space of dynamic storage management, you may realize that one actually has to *work* to produce a stack design so dumb that overflow attacks are possible. Here are four classes of designs that are immune to the vulnerability:

1. Descriptor stacks. The only thing that goes in the stack are addresses, preferably with a bounds value attached. Overflow a buffer and at worst you clobber the heap. Penalty: one level of indirection, which (The Horror! The Horror!) may cause your dancing pigs to dance slower than the other guy's. Possibility: can be fitted transparently to existing processor designs, assuming anybody cared.

2. Stack per protection domain. This assumes you can find the perimeters of your protection domains. Also slows down dancing pig displays because of copying parameters from stack to stack.

3. Separate control and data stacks. CALL/RETURN works the control stack, PUSH/POP works the data stack. Doh.

4. Error-checking stacks. A whole raft of options, including "shadow stacks" with checksums, return addresses protected with trap bits, etc. etc.

So, if it's all so straightforward and well known, why hasn't some vendor or other fixed it? Answer: the dancing pigs have won.<

24.1 Windows 9x/Me

Category 24.1 *Windows 9x/Me*

2000-07-19 **Trojan horse buffer overflow e-mail**

RISKS, Securityfocus http://www.securityfocus.com/news/62 20 97

MS-Outlook and Outlook Express were shown to be susceptible to a buffer overflow through the date field of incoming e-mail. The bug was fixed using the IE SP1 or IE v5.5 on Windows 9x and NT. A service pack was made available for Windows 2000. The buffer overflow would allow execution of arbitrary code upon receipt of e-mail, not through execution of mobile code.

Category 24.1 *Windows 9x/Me*

2001-11-15 **Windows XP vulnerability administrator account root privilege default cost benefit analysis 80/20 rule Pareto principle**

RISKS 21 76

By default, all user accounts created under Windows XP have administrator (root) capability and have no passwords. Mark Wilkins offered an interesting explanation of what might be behind such a decision. Writing in RISKS, he described how he had worked on the design for a TV security system which originally kept all channel lock settings in place, allowing parents to selectively "allow or deny TV viewing according to those settings as they liked." However, the TV manufacturer reversed this policy so that "unlocking the TV caused ALL of the information about which channels or times were or were not permissible to be erased, requiring that they be re-entered next time." Mr Wilkins continued, ". . . . support telephone calls on the issue of parental lock . . . nearly always asked 'My kids have locked me out of the television. What do I do?' Since those calls cost money to support a product for which the company had already been paid, they were to be minimized. The product had to be easy to unlock and hard to lock." He concluded, "I suspect this behavior in Windows XP is a similar matter."

Category 24.1 *Windows 9x/Me*

2002-08-07 **proprietary code open source Windows antitrust settlement court order intellectual property patents**

NewsScan

WINDOWS CODE RELEASED TO DEVELOPERS
Complying with provisions of the proposed antitrust settlement with the Justice Department, Microsoft has begun giving independent software developers technical information about the Windows operating system, which will be used to create alternative Web browsers and other software products to rival ones offered by Microsoft. But the company's critics remain unappeased and vocal. Mike Pettit of ProComp, a trade group backed by Microsoft's competitors, says he has found "several examples where if you unclick a choice indicating you don't want to use Microsoft middleware, it shows up anyway... I find astonishing at this stage of the game that these kinds of things would happen. Either the Justice Department didn't do a very good job of protecting consumers or Microsoft has not done a very good job of compliance." (Los Angeles Times 6 Aug 2002)

Category 24.1 *Windows 9x/Me*

2003-02-27 **Microsoft security bulletin Millenium Edition ME vulnerability**

NIPC/DHS

February 26, Microsoft — Microsoft Security Bulletin MS03-006: Flaw in Windows Me Help and Support Center could enable code execution .

A security vulnerability is present in the Windows Me version of Microsoft's Help and Support Center. Users and programs can execute URL links to Help and Support Center by using the "hcp://" prefix in a URL link instead of "http://". The vulnerability results because the URL Handler for the "hcp://" prefix contains an unchecked buffer. An attacker who successfully exploited this vulnerability could cause code of his or her choice to be executed as though it originated on the local machine. Such code could provide the attacker with the ability to take any desired action on the machine, including adding, deleting or modifying data on the system or running any code of the attacker's choice. Microsoft assigned a risk rating of "Critical" to this vulnerability. A patch is available at the Microsoft website.

24.2 Windows NT/2K/XP

Category 24.2 *Windows NT/2K/XP*

2000-02-20 **QA quality assurance operating system bugs**

RISKS 20 80

Jim Allchin, Group Vice President, Platforms Group, Microsoft Corporation, wrote an open letter to MS customers about claims that Windows 2000 had over 63,000 defects. He listed a number of threads of evidence showing that Windows 2000 was the most highly tested and stable products the company had released.

Category 24.2 *Windows NT/2K/XP*

2000-02-21 **QA quality assurance availability operating system**

RISKS 20 81

According to users of a new Windows 2000 system in the Tula County Court Clerk's Office, the new operating system was causing serious downtime: "The new system has been down completely for at least a day twice in the last two weeks and regularly has system errors that hinder access to records for hours at a time."

Category 24.2 *Windows NT/2K/XP*

2000-09-08 **access control vulnerability operating system lock screen saver communications port vulnerability**

RISKS 21 04

Avi Rubin noted in RISKS that despite the "lock" function in Windows 2000 and Windows NT, communications through ports still works. He illustrated the risks by sketching scenarios in which the synchronization function of the Palm Pilot could be used to obtain or damage information on a supposedly locked system. [Readers should note that under Windows 9x, screen savers, even secure ones, do not generally prevent access via the communications ports if appropriate software is running. LapLink, for example, functions perfectly well even if a target computer is in screen-saver mode.]

Category 24.2 *Windows NT/2K/XP*

2001-05-29 **risk management insurance rates operating system stability hacking penetration vulnerabilities**

RISKS 21 44

According to an article in _InternetWeek_, hacking insurance will cost more for clients using Windows NT. Oleg Broytmann contributed this summary:
>"We saw that our NT-based clients were having more downtime" due to hacking, says John Wurzler, founder and CEO of the Michigan company, which has been selling hacker insurance since 1998. Wurzler said the decision to charge higher premiums was not mandated by the syndicates affiliated with Lloyd's of London that underwrite the insurance he sells. Instead, the move was based on findings from 400 security assessments that his firm has done on small and midsize businesses over the past three years. Wurzler found that system administrators working on open-source systems tend to be better trained and stay with their employers longer than those at firms using Windows software, where turnover can exceed 33 percent per year.<
http://www.zdnet.com/intweek/stories/news/0,4164,2766045,00.html

---

Category 24.2 *Windows NT/2K/XP*

2001-10-08 **wireless network security product management chip**

NewsScan

IBM TO OFFER SECURITY SOFTWARE AND SERVICES FOR WIRELESS DEVICES
IBM is launching new security software and services for wireless devices, including the ability for a corporation to manage those devices the same way it uses firewalls and servers to manage other security exposures. The company has also begun to sell ThinkPad notebooks and NetVista desktop computers that include a security chip designed to protect against vandals trying to hack into them through a wireless network. (Reuters/San Jose Mercury News 8 Oct 2001)
http://www.siliconvalley.com/docs/news/svfront/020703.htm

Category 24.2 *Windows NT/2K/XP*

2002-07-17 **standards vulnerability assessment defaults parameters operating system**

NewsScan

SETTING STANDARDS TO PROTECT THE INTERNET
In support of the nation's homeland security, the nonprofit Center for Internet Security (CIS) has forged a technical consensus among a large group of government agencies and private businesses. The focus of the plan is largely on the widely used (though not the latest) Microsoft Windows 2000 operating system, and uses a software "scoring" system to ensure that specific technical security settings are properly in place. Government agencies participating in the security review included the Pentagon, NSA and NIST, and corporations included Allstate, First Union, Visa and Pacific Gas & Electric. (Washington Post 17 Jul 2002)

Category 24.2 *Windows NT/2K/XP*

2002-12-13 **critical flaws Windows operating systems alert Java virtual machine HTML**

NewsScan

MICROSOFT WARNS OF 'CRITICAL' SECURITY FLAWS IN WINDOWS
Microsoft revealed "critical" flaws in its Windows operating system that conceivably could allow hackers to alter data stored in computers, load and run malicious programs, or reformat hard drives. Microsoft is urging Windows users to download a new version of Microsoft Virtual Machine, which is the part of Windows that runs Java applications. "An attacker could, in the most serious of these vulnerabilities, gain complete control of a user's system and take any action" he or she chooses, said John Montgomery, head of Microsoft's developer platform and evangelism group. Security features in Outlook Express 6 and Outlook 2002 are safe from the HTML-mail-based attacks by default and Outlook 98 and 2000 users are also protected if users have installed the Microsoft security updates for them. The good news is, a hacker would have to be quite sophisticated to carry out an attack of the kind described, says Gary Bahadur, CIO at Foundstone. "This is not an easy attack at all. You've got to be pretty slick, pretty creative." (Wall Street Journal 13 Dec 2002)

Category 24.2 *Windows NT/2K/XP*

2003-02-06 **Microsoft security bulletin unchecked buffer vulnerability**

NIPC/DHS

February 05, Microsoft — Microsoft Security Bulletin MS03-005: Unchecked buffer in Windows Redirector could allow privilege elevation.

A security vulnerability exists in the implementation of the Windows Redirector on Windows XP because an unchecked buffer is used to receive parameter information. By providing malformed data to the Windows Redirector, an attacker who successfully exploited this vulnerability could cause the system to fail, or could cause code of the attacker's choice to be executed with system privileges. Code running with system privileges could provide the attacker with the ability to take any desired action on the machine, such as adding, deleting, or modifying data on the system, and creating or deleting user accounts. This vulnerability cannot be exploited remotely. Windows XP systems that are not shared between users would not be at risk. The vulnerability could only be exploited by an attacker who had valid credentials to interactively log onto the computer. Microsoft has assigned a severity rating of "Important" to this vulnerability. A patch is available at the Microsoft website.

Category 24.2 *Windows NT/2K/XP*

2003-03-12 **CERT CC advisory Windows Shares Serve Message Block 2000 XP target**

NIPC/DHS

March 11, CERT/CC — CERT Advisory CA-2003-08: Increased Activity Targeting Windows Shares.

Over the past few weeks, the CERT/CC has received an increasing number of reports of intruder activity involving the exploitation of Null (i.e., non-existent) or weak Administrator passwords on Server Message Block file shares used on systems running Windows 2000 or Windows XP. This activity has resulted in the successful compromise of thousands of systems, with home broadband users' systems being a prime target. Recent examples of such activity are the attack tools known as W32/Deloder, GT-bot, sdbot, and W32/Slackor. The presence of any of these tools on a system indicates that the Administrator password has likely been compromised, and the entire system is therefore suspect. With this level of access, intruders may exercise remote control expose confidential data; install other malicious software; change files; delete files; or launch attacks against other sites. Information on how to guard against these attacks may be found on the CERT/CC website.

Category 24.2 *Windows NT/2K/XP*

2003-03-20 **new vulnerability Microsoft security bulletin Windows Script Engine**

NIPC/DHS

March 19, Microsoft — Microsoft Security Bulletin MS03-008: Flaw in Windows Script Engine Could Allow Code Execution.

The Windows Script Engine provides Windows operating systems with the ability to execute script code. A flaw exists in the way by which the Windows Script Engine for JScript processes information. An attacker could exploit the vulnerability by constructing a web page that, when visited by the user, would execute code of the attacker's choice with the user's privileges. The web page could be hosted on a web site, or sent directly to the user in email. Exploiting the vulnerability would allow the attacker only the same privileges as the user. Computers configured to disable active scripting in Internet Explorer are not susceptible to this issue. Users whose accounts are configured to have few privileges on the system would be at less risk than ones who operate with administrative privileges. Automatic exploitation of the vulnerability by an HTML email would be blocked by Outlook Express 6.0 and Outlook 2002 in their default configurations, and by Outlook 98 and 2000 if used in conjunction with the Outlook Email Security Update. Microsoft has assigned a risk rating of "Critical" to this vulnerability. A patch is available at the Microsoft Website. Microsoft has also provided information about preventive measures customers can use to help block the exploitation of this vulnerability while they are assessing the impact and compatibility of the patch.

Category 24.2 *Windows NT/2K/XP*

2003-03-27 **new vulnerability Remote Procedure Call RPC Microsoft denial-of-service advisory**

NIPC/DHS

March 26, Microsoft — Microsoft Security Bulletin MS03-010: Flaw in RPC Endpoint Mapper Could Allow Denial of Service Attacks.

There is a vulnerability in the part of Remote Procedure Call (RPC) that deals with message exchange over TCP/IP due to incorrect handling of malformed messages. This vulnerabilty affects the RPC Endpoint Mapper process, which listens on TCP/IP port 135. To exploit this vulnerability, an attacker would need to establish a TCP/IP connection to the Endpoint Mapper process on a remote machine. Once the connection was established, the attacker would begin the RPC connection negotiation before transmitting a malformed message. At this point, the process on the remote machine would fail. The RPC Endpoint Mapper process is responsible for maintaining the connection information for all of the processes on that machine using RPC. Because the Endpoint Mapper runs within the RPC service itself, exploiting this vulnerability would cause the RPC service to fail, with the attendant loss of any RPC-based services the server offers, as well as potential loss of some COM functions. A patch is available at the Microsoft website for Windows 2000 and Windows XP. However, Microsoft is unable to provide a patch for this vulnerability for Windows NT 4.0 and users are encouraged to employ the workaround posted on the Microsoft website, which is to protect the NT 4.0 system with a firewall that blocks Port 135.

Category 24.2 *Windows NT/2K/XP*

2003-04-10 **new vulnerability Microsoft security bulletin virtual machine flaw patch exploit fix**

NIPC/DHS

April 09, Microsoft — Microsoft Security Bulletin MS03-011: Flaw in Microsoft VM Could Enable System Compromise.

The Microsoft VM is a virtual machine for the Win32 operating environment. The Microsoft VM is shipped in most versions of Windows, as well as in most versions of Internet Explorer. A new security vulnerability affects the ByteCode Verifier component of the Microsoft VM, and results because the ByteCode verifier does not correctly check for the presence of certain malicious code when a Java applet is being loaded. The attack vector for this new security issue would likely involve an attacker creating a malicious Java applet and inserting it into a web page that when opened, would exploit the vulnerability. An attacker could then host this malicious web page on a web site, or could send it to a user in e-mail. Corporate IT administrators could limit the risk posed to their users by using application filters at the firewall to inspect and block mobile code. Microsoft has assigned a risk rating of "Critical" to this vulnerability. A patch is available at the Microsoft website.

Category 24.2 *Windows NT/2K/XP*

2003-04-17 **new vulnerability Microsoft security bulletin buffer overflow kernel message handling**

NIPC/DHS

April 16, Microsoft — Microsoft Security Bulletin MS03-013: Buffer Overrun in Windows Kernel Message Handling could Lead to Elevated Privileges.

The Windows kernel is the core of the operating system. It provides system level services such as device and memory management, allocates processor time to processes and manages error handling. There is a flaw in the way the kernel passes error messages to a debugger. A vulnerability results because an attacker could write a program to exploit this flaw and run code of their choice. An attacker could exploit this vulnerability to take any action on the system including deleting data, adding accounts with administrative access, or reconfiguring the system. For an attack to be successful, an attacker would need to be able to logon interactively to the system, either at the console or through a terminal session. Also, a successful attack would require the introduction of code in order to exploit this vulnerability. Because best practices recommends restricting the ability to logon interactively on servers, this issue most directly affects client systems and terminal servers. Microsoft has assigned a risk rating of "Important" to this vulnerability. A patch is available at the Microsoft website.

Category 24.2 *Windows NT/2K/XP*

2003-04-28 **Cisco Systems Secure Access Control Server Windows vulnerability patch fix**

NIPC/DHS

April 24, CNET News.com — Cisco flaw exposes Windows servers.

A potentially critical vulnerability has been found in Cisco Systems' Secure Access Control Server for Windows servers, which is used to control devices such as routers in large networks. The buffer overflow glitch may allow an attacker to seize control of the Cisco service when it's running on Windows, according to Cisco. The Unix variant is not affected. Exploitation of the flaw could result in a malicious hacker gaining full control of a target company's security infrastructure, leaving it completely exposed. An exploit for the vulnerability is not known to be circulating, and ACS servers are usually deployed on network segments with limited physical access. Administrators of ACS systems block TCP port 2002 until they can deploy Cisco's fix. A patch is available at the Cisco Website:
http://www.cisco.com/warp/public/707/cisco-sa-20030423-ACS.s html.

Category 24.2 *Windows NT/2K/XP*

2003-05-01 **windows flaw patch security microsoft multi-processor machine crash 2000 XP**

NIPC/DHS

May 01, eWEEK — Microsoft updates patch for Windows flaw.

Microsoft Corp. has released an updated patch for a security vulnerability discovered in Windows NT 4.0 in December. The new update fixes a flaw in the original patch that installed the wrong binaries on multi-processor machines, causing them to crash in some situations. The original vulnerability that the patch was meant to fix affected Windows 2000 and XP as well. But the problem that prompted the release of the new patch only occurs in machines running Windows NT 4.0 Terminal Services Edition. The revised bulletin and patch for this flaw are available on the Microsoft Website:
http://www.microsoft.com/technet/treeview/default.asp?url=/t echnet/security/bulletin/MS02-071.asp.

Category 24.2 *Windows NT/2K/XP*

2003-05-07 **MS03-017 Microsoft Windows Media Player 7.1 XP malicious executable HTML e-mail outlook update code execution**

NIPC/DHS

May 07, Microsoft — Microsoft Security Bulletin MS03-017: Flaw in Windows Media Player Skins Downloading could allow Code Execution.

A flaw exists in the way Microsoft's Windows Media Player 7.1 and Windows Media Player for Windows XP handle the download of skin files. An attacker could force a file masquerading as a skin file into a user's machine. This could allow an attacker to place a malicious executable on the system. In order to exploit this flaw, an attacker would have to host a malicious web site and then persuade a user to visit that site. An attacker could also embed the link in an HTML e-mail and send it to the user. If the user was not using Outlook Express 6.0 or Outlook 2002 in their default configurations, or Outlook 98 or 2000 in conjunction with the Outlook Email Security Update, the attacker could cause an attack that could both place, then launch the malicious executable without the user having to click on a URL contained in an e-mail. Microsoft has assigned a risk rating of "Critical" to this vulnerability, and a patch is available at the Microsoft website.

Category 24.2 *Windows NT/2K/XP*

2003-05-28 **MS03-019 microsoft security bulletin ISAPI Extension Windows Media Service Denial Service NT4.0 Server IIS exploit**

NIPC/DHS

May 28, Microsoft — Microsoft Security Bulletin MS03-019: Flaw in ISAPI Extension for Windows Media Services Could Cause Denial of Service.

When Windows Media Services are installed in Windows NT 4.0 Server or added through add/remove programs to Windows 2000, nsiislog.dll is installed to the Internet Information Services (IIS) Scripts directory on the server. A flaw in the way in which nsiislog.dll processes incoming requests could allow and attacker could send specially formed communications to the server that could cause IIS to stop responding to Internet requests. An attacker attempting to exploit this vulnerability would have to be aware which computers on the network had Windows Media Services installed on it and send a specific request to that server. Microsoft has assigned a risk rating of "Moderate" to this vulnerability and a patch is available at the Microsoft website.

Category 24.2 *Windows NT/2K/XP*

2003-07-03 **Windows 2000 ShellExecute API hole buffer overflow vulnerability SecureNet Service MUA**

NIPC/DHS

July 03, eSecurity Planet — Windows 2000 ShellExecute API hole patched.

Microsoft has issued a fix for a buffer overflow vulnerability in the Windows 2000 ShellExecute API after a security researcher warned the flaw could trigger denial-of-service attacks. According to research firm SecureNet Service (SNS), which reported the hole, Microsoft included a fix in Windows 2000 Service Pack 4. It affects Microsoft Windows 2000 Datacenter Server, Windows 2000 Advanced Server, Windows 2000 Server and Windows 2000 Professional. SNS said the problem was triggered when the pointer to an unusually long string was set to the 3rd argument of the Windows 2000 API Shell Execute() API function. SNS said that several applications containing Web browser, MUA and text editor were vulnerable to security hole.

Category 24.2 *Windows NT/2K/XP*

2003-07-09 **MS03-025 windows message handling utility privilege elevation interactive processes**

NIPC/DHS

July 09, Microsoft — Microsoft Security Bulletin MS03-025: Flaw in Windows Message Handling through Utility Manager Could Enable Privilege Elevation.

Microsoft Windows messages provide a way for interactive processes to react to user events and communicate with other interactive processes. A flaw in the way that the Microsoft Accessibility Utility Manager handles Windows messages results in a vulnerability because the control that provides the list of accessibility options to the user does not properly validate Windows messages sent to it. It's possible for one process in the interactive desktop to use a specific Windows message to cause the Utility Manager process to execute a callback function at the address of its choice. Because the Utility Manager process runs at higher privileges than the first process, this would provide the first process with a way of exercising those higher privileges. By default, the Utility Manager contains controls that run in the interactive desktop with Local System privileges. An attacker who had the ability to log on to a system interactively could run a program that could send a Windows message upon the Utility Manager process, causing it to take any action the attacker specified. This would give the attacker complete control over the system. Microsoft has assigned a risk rating of "Important" to this issue and recommends that system administrators install the patch immediately.

Category 24.2 *Windows NT/2K/XP*

2003-07-09 **MS03-024 buffer overrun data corruption Server Message Block SMB port 139 445**

NIPC/DHS

July 09, Microsoft — Microsoft Security Bulletin MS03-024: Buffer Overrun in Windows Could Lead to Data Corruption.

When a client system sends an Server Message Block (SMB) packet to the server system, it includes specific parameters that provide the server with a set of "instructions." The server is not properly validating the buffer length established by the packet. If the client specifies a buffer length that is less than what is needed, it can cause the buffer to be overrun. By sending a specially crafted SMB packet request, an attacker could cause a buffer overrun to occur. If exploited, this could lead to data corruption, system failure, or it could allow an attacker to run the code of their choice. An attacker would need a valid user account and would need to be authenticated by the server to exploit this flaw. By default, it is not possible to exploit this flaw anonymously. The attacker would have to be authenticated by the server prior to attempting to send a SMB packet to it. Blocking port 139/445 at the firewall will prevent the possibility of an attack from the Internet. Microsoft has assigned a risk rating of "Important" to this issue and recommends that system administrators consider installing the patch.

Category 24.2 *Windows NT/2K/XP*

2003-07-16 **MS03-027 buffer windows shell system compromise attacker service pack 1 XP important**

NIPC/DHS

July 16, Microsoft — Microsoft Security Bulletin MS03-027: Unchecked Buffer in Windows Shell Could Enable System Compromise.

An unchecked buffer exists in one of the functions used by the Windows shell to extract custom attribute information from certain folders. An attacker could seek to exploit this vulnerability by creating a Desktop.ini file that contains a corrupt custom attribute, and then host it on a network share. If a user were to browse the shared folder where the file was stored, the vulnerability could then be exploited. A successful attack could have the effect of either causing the Windows shell to fail, or causing an attacker's code to run on the user's computer in the security context of the user. This vulnerability only affects Windows XP Service Pack 1. Microsoft has assigned a risk rating of "Important" to this issue and recommends that system administrators install the patch at the earliest opportunity.

Category 24.2 *Windows NT/2K/XP*

2003-07-17 **flaw Windows Microsoft Server 2003 vulnerability**

NewsScan

MICROSOFT FLAW: A NEW STAGE OF DELIRIUM
Microsoft has acknowledged a critical vulnerability in most versions of its Windows operating system software, including its latest Windows Server 2003 software. The vulnerability (first pointed out by researchers in Poland known as the "Last Stage of Delirium Research Group") could be used by network vandals to seize control of a victim's Windows computer over the Internet, stealing data, deleting files or eavesdropping on e-mail messages. The Server 2003 software was sold under the highly promoted "Trustworthy Computing" initiative launched last year by Microsoft founder Bill Gates. The company urged customers to immediately apply a free software patch available from Microsoft's Web site. Internet Security Systems, an Atlanta-based computer firm, characterized the Windows flaw as "an enormous threat." (AP/San Jose Mercury News 17 Jul 2003)

Category 24.2 *Windows NT/2K/XP*

2003-07-23 **MS03-029 denial service windows nt 4.0 server file management function**

NIPC/DHS

July 23, Microsoft — Microsoft Security Bulletin MS03-029: Flaw in Windows Function Could Allow Denial of Service.

A flaw exists in a Windows NT 4.0 Server file management function that can cause a denial of service vulnerability. The flaw results because the affected function can cause memory that it does not own to be freed when a specially crafted request is passed to it. If the application making the request to the function does not carry out any user input validation and allows the specially crafted request to be passed to the function, the function may free memory that it does not own. As a result, the application passing the request could fail. By default, the affected function is not accessible remotely, however applications installed on the operating system that are available remotely may make use of the affected function. Microsoft has assigned a risk rating of "Moderate" to this issue and recommends that system administrators consider applying the security patch

---

Category 24.2 *Windows NT/2K/XP*

2003-09-10 **Internet Operations Microsoft Operating Systems Remote procedure Call Server Service RPCSS NCSD DHS IAP DCOM RPC ports exploit vulnerabilities worm virus**

NIPC/DHS

September 10, U.S. Department of Homeland Security — Potential For Significant Impact On Internet Operations Due To Vulnerability In Microsoft Operating Systems' Remote Procedure Call Server Service (RPCSS).

The National Cyber Security Division (NCSD) of the Department of Homeland Security (DHS) / Information Analysis and Infrastructure Protection (IAIP) Directorate is issuing this advisory in consultation with the Microsoft. There are three vulnerabilities in the part of Remote Procedure Call (RPC) that deals with RPC messages for the Distributed Component Object Model (DCOM) activation—two that would allow arbitrary code execution, and one that would result in a denial of service. These particular vulnerabilities affect the DCOM interface within the RPCSS, which listens on RPC enabled ports. An attacker who successfully exploited these vulnerabilities could be able to run code with local system privileges on an affected system, or cause the RPCSS to fail. The attacker could be able to take any action on the system. DHS is concerned that a properly written exploit could rapidly spread on the Internet as a worm or virus in a fashion similar to the Blaster Worm. DHS and Microsoft recommend that system administrators install the patch immediately. Additional information is available on the Microsoft Website:
http://www.microsoft.com/security/security_bulletins/ms03-03 9.asp

---

Category 24.2 *Windows NT/2K/XP*

2003-09-17 **iDefense internet attack blaster like tool hacker access victims computer infection**

NewsScan

VANDAL WATCH
Security firm iDefense Inc. of Reston, Va., has found new Internet attack software being distributed via a Chinese Web site, and says they expect widespread attacks similar to the Blaster infection within days. Microsoft confirmed it was studying the new attack tool, which gives hackers access to victims' computers by creating a new account with the name "e" with a preset password. The tool includes options to attack two Windows 2000 versions that are commonly used inside corporations. (AP/San Jose Mercury News 17 Sep 2003)

Category 24.2 *Windows NT/2K/XP*

2003-09-19 **ATM Windows NT security issues hackers IBM OS/2 open technology hardware support cut-down version**

NewsScan

ATMs TO SWITCH OVER TO WINDOWS
Sixty-five percent of the automated teller machines in the U.S. will be running on a stripped down version of Windows NT within three years, according to a study by market researcher Celent. Currently most ATMs use IBM's OS/2 operating system, but banking industry officials say they now prefer Windows, which is more compatible with their internal corporate networks. "Because we are seeing so many mergers and acquisitions in the last few years, you have large banks running a fleet of ATM hardware," says Celent analyst Gwenn Bezard. "With open technologies [like Windows] it is easier to run different types of hardware on the same software." Banking officials generally dismiss worries over hackers disabling or corrupting ATMs across the country, but some security specialists continue to have doubts: "What Microsoft actually sells to the banks for ATM use is a cut-down version of Windows that doesn't contain things like Web servers. They have tried to cut out the unnecessary rubbish that clutters up the typical PC. How good a job they've done, I just don't know… So we definitely can't rule out the possibility that someone in the future writes a Slammer-style worm that causes thousands of ATMs to start spewing out cash," says British security expert Ross Anderson. (Wired.com 19 Sep 2003)

Category 24.2 *Windows NT/2K/XP*

2003-11-13 **new critical vulnerability Microsoft security bulletin buffer overrun overflow workstation patch fix exploit**

NIPC/DHS

November 11, Microsoft — Microsoft Security Bulletin MS03-049: Buffer Overrun in the Workstation Service Could Allow Code Execution.

A security vulnerability exists in the Workstation service that could allow remote code execution on an affected system. This vulnerability results because of an unchecked buffer in the Workstation service. If exploited, an attacker could gain System privileges on an affected system, or could cause the Workstation service to fail. An attacker could take any action on the system, including installing programs, viewing data, changing data, or deleting data, or creating new accounts with full privileges. If users have blocked inbound UDP ports 138, 139, 445 and TCP ports 138, 139, 445 by using a firewall an attacker would be prevented from sending messages to the Workstation service. Most firewalls, including Internet Connection Firewall in Windows XP, block these ports by default. Disabling the Workstation service will prevent the possibility of attack. Only Windows 2000 and Window XP are vulnerable to this attack. Microsoft has assigned a risk rating of "Critical" to this issue and recommends that system administrators install the patch immediately.

Category 24.2 *Windows NT/2K/XP*

2003-11-17 **Microsoft Windows exploit patch fix release**

NIPC/DHS

November 13, eWEEK — Windows exploits released.

Microsoft Corp. released its monthly passel of patches on Tuesday, November 11, including one for a flaw in the Workstation service in Windows 2000 and XP. A successful exploitation would give the attacker complete control of the compromised PC, Microsoft said. Less than 24 hours after Microsoft issued the fix, two members of the BugTraq security mailing list posted exploit code for the vulnerability. The author of one of the exploits said the code had been tested only on a Windows 2000 machine with Service Pack 4 installed and the FAT32 file system running. The other exploit is designed for machines running Windows XP. However, experts said it would take little effort to adapt the code for other Windows machines. And, more importantly, the Workstation vulnerability appears to be a prime candidate for a worm.

Category 24.2 *Windows NT/2K/XP*

2003-12-11 **security expert warning Microsoft Windows critical vulnerability TCP UDP**

NIPC/DHS

December 10, eWEEK — Security experts warn of new way to attack Windows.

Security experts have found a new way to exploit a critical vulnerability in Windows that evades a workaround. Microsoft Corp. issued a patch for the vulnerability in November, but the security bulletin also listed several workarounds for the flaw, including disabling the Workstation Service and using a firewall to block specific UDP and TCP ports. Researchers at security company Core Security Technologies discovered a new attack vector that uses a different UDP port. This attack still allows the malicious packets to reach the vulnerable Workstation Service. An attacker who successfully exploits the weakness could run any code of choice on the vulnerable machine. An attacker doesn't have to individually address computers on the network, but can broadcast an attack. Such a tactic could actually create a worm that spreads faster than the SQL Slammer worm did last year. Microsoft urged customers to apply the patch. "Applying the patch does correct the problem," said Iain Mulholland, a security program manager for Microsoft.

Category 24.2 *Windows NT/2K/XP*

2004-02-16 **exploit vulnerability Microsoft ASN.1 operating systems Windows NT XP 2000 Trojan Horse**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/24946−1.html

February 16, Government Computer News — Exploit code for Microsoft vulnerability circulating.

Security researchers say code designed to exploit a recently announced critical vulnerability in Microsoft operating systems now is widespread on the Internet. The code crashes targeted computers by exploiting a flaw in Microsoft's Abstract Syntax Notation 1 Library in Windows NT, 2000 and XP. The exploit code was discovered Saturday, February 14, four days after the vulnerability and a patch to correct it was announced by Microsoft. The code is available on several discussion groups and Web sites. Ken Dunham of iDefense Inc. said there have been reports of denial-of-service attacks against specific targets using this exploit, but the attacks are not yet widespread. "It may be a few days before we see anything beyond a DOD attack," he said. " Several attackers are actively working on an ASN.1 exploit to spread Trojans and 'bots. One attacker has expressed an interest in creating a worm that will 'take down the Internet.'" Dunham said the malicious actors are capable of "weaponizing" the exploit, but have so far had little success in their tests. In other malicious-code news, Symantec Corporation has raised the security level for the new Welchia worm because of increasing numbers of infections. Welchia, also known as Nachi, first appeared last August in the wake of the MSBlaster worm. It automatically patched against the vulnerability exploited by Blaster. The new version, Welchia.b, appears to remove the MyDoom a and b worms from infected machines. Once installed on a machine, it tries successively to exploit three vulnerabilities against a random IP address.

Category 24.2 *Windows NT/2K/XP*

2004-03-10 **Microsoft security bulletin vulnerability hole flaw patch fix Windows Media denial-of-service**

DHS IAIP Daily; http://www.microsoft.com/technet/security/bulletin/ms04−
009. mspx

March 09, Microsoft — Microsoft Security Bulletin MS04-008: Vulnerability in Windows Media Services Could Allow a Denial of Service.

A vulnerability exists because of the way that Windows Media Station Service and Windows Media Monitor Service, components of Windows Media Services, handle TCP/IP connections. If a remote user were to send a specially-crafted sequence of TCP/IP packets to the listening port of either of these services, the service could stop responding to requests and no additional connections could be made. The service must be restarted to regain its functionality. Windows Media Unicast Service may also be affected by a successful attack against Windows Media Station Service if Windows Media Unicast Service is sourcing a playlist from Windows Media Station Service. In this case, Windows Media Unicast Service could stop functioning when it encounters the next item in the playlist. Microsoft has assigned a risk rating of "Moderate" to this issue and recommends that system administrators consider installing the security update.

Category 24.2 *Windows NT/2K/XP*

2004-04-13 **Micrsoft security bulletin update Windows critical**

DHS IAIP Daily; http://www.microsoft.com/technet/security/bulletin/ms04−
011. mspx

April 13, Microsoft — Microsoft Security Bulletin MS04-011: Security Update for Microsoft Windows.

This update resolves several newly-discovered vulnerabilities which are detailed on the Microsoft Website. An attacker who successfully exploited the most severe of these vulnerabilities could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges. Microsoft has assigned a risk rating of "Critical" to these issues and recommends that customers apply the update immediately.

Category 24.2 *Windows NT/2K/XP*

2004-04-13 **Micrsoft security bulletin update Windows critical Jet Database Engine buffer overflow**

DHS IAIP Daily; http://www.microsoft.com/technet/security/bulletin/ms04−
014. mspx

April 13, Microsoft — Microsoft Security Bulletin MS04-014 Vulnerability in the Microsoft Jet Database Engine Could Allow Code Execution.

A buffer overrun vulnerability exists in the Microsoft Jet Database Engine (Jet) that could allow remote code execution. An attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges. Microsoft recommends that customers install the update at the earliest opportunity.

Category 24.2 *Windows NT/2K/XP*

2004-04-13 **Micrsoft security bulletin update Windows critical RPC DCOM**

DHS IAIP Daily; http://www.microsoft.com/technet/security/bulletin/ms04−
012. mspx

April 13, Microsoft — Microsoft Security Bulletin MS04-012 Cumulative Update for Microsoft RPC/DCOM.

This update resolves several newly-discovered vulnerabilities in RPC/DCOM. Each vulnerability is documented on the Microsoft Website. An attacker who successfully exploited the most severe of these vulnerabilities could take complete control of the affected system. An attacker could then take any action on the affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges. Microsoft has assigned a risk rating of "Critical" to this issue and recommends customers apply the update immediately.

Category 24.2 *Windows NT/2K/XP*

2004-04-22 **Microsoft flaw hole vulnerability exploit**

DHS IAIP Daily; http://www.us−cert.gov/current/current_activity.html#pct

April 22, US-CERT — Exploit for Microsoft PCT vulnerability released.

Exploit code has been publicly released that takes advantage of a buffer overflow vulnerability in the Microsoft Private Communication Technology (PCT) protocol. The vulnerability allows a remote attacker to execute arbitrary code with SYSTEM privileges. US-CERT is aware of network activity that is consistent with scanning and/or exploit attempts against this vulnerability. Reports indicate increased network traffic to ports 443/tcp and 31337/tcp. The PCT protocol runs over SSL (443/tcp) and the known exploit code connects a command shell on 31337/tcp. Note that the exploit code could be modified to use a different port or to execute different code. This vulnerability is remedied by the patches described in Microsoft Security Bulletin MS04-011:
http://www.microsoft.com/technet/security/bulletin/MS04-011. mspx

---

Category 24.2 *Windows NT/2K/XP*

2004-04-26 **Microsoft Windows vulnerability flaw hole exploit worm**

DHS IAIP Daily; http://informationweek.securitypipeline.com/news/19201802;js
essionid=LUENRK1IB4PBYQSNDBGCKHQ

April 26, InformationWeek — Windows vulnerability exploited, worm may be next.

Security experts are monitoring widespread use of exploit code that takes advantage of a recently-disclosed vulnerability in Windows, but a worm, although anticipated, hasn't yet been spotted. The vulnerability stems from a flaw in Windows Protected Communications Technology (PCT) v. 1.0, a packet protocol within Microsoft's SSL library. An April bulletin from Microsoft warned that an attacker could create a buffer overflow condition on vulnerable Windows servers, then follow that by inserting their own code into the system to take control. Windows XP and Windows Server 2003 systems are also vulnerable. The first form of the exploit code was discovered within days of the disclosure of the SSL vulnerability, added Ken Dunham of iDefense. Last week, that code was updated to include a "phone home" feature that allowed hackers using it to be notified when they'd compromised a server. Additional information is available in Microsoft Knowledge Base Article 187498:
http://support.microsoft.com/default.aspx?scid=
http://suppor t.microsoft.com:80/support/kb/articles/q187/4/98.asp&NoWebCo ntent=1

Category 24.2 *Windows NT/2K/XP*

2004-04-26 **attack exploit source code Microsoft MS LSASS buffer overflow**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/story/0,10801,92696,00.html

April 26, IDG News Service — Attack code surfaces for recent MS security hole.

Computer code that claims to exploit a recently disclosed hole in Microsoft products has surfaced on a French-language Website. The code can be used by a remote attacker to trigger a buffer overrun vulnerability in the Local Security Authority Subsystem (LSASS). The code was released on Saturday, April 24, according to the Website. It was unclear whether the exploit code works, but notes attached by its author say some modifications may be necessary before the code can be used by a remote attacker to compromise Windows machines. An attacker who could exploit the LSASS vulnerability could remotely attack and take total control of Windows 2000 and Windows XP systems, according to Microsoft. Unlike e-mail worms and viruses, no user interaction would be necessary to trigger the LSASS buffer overflow, according to Johannes Ullrich of the SANS Institute's Internet Storm Center. Microsoft released a patch for the LSASS vulnerability in Microsoft Security Bulletin MS04-011: http://www.microsoft.com/technet/security/bulletin/MS04-011. mspx

---

Category 24.2 *Windows NT/2K/XP*

2004-04-26 **Windows critical hijack flaw vulnerability**

DHS IAIP Daily; http://www.esecurityplanet.com/alerts/article.php/3345351

April 26, eSecurity Planet — 'Critical' Windows hijack flaw reported.

Security researchers have discovered a serious boundary error vulnerability in multiple versions of Microsoft's Windows platform and warned that attackers could hijack systems via Windows Explorer and Internet Explorer. Rodrigo Gutierrez, a researcher with Trustix AS, notified Microsoft of the flaw with a warning that it could be exploited by malicious attackers to cause a buffer overflow and lead to system takeover. Microsoft confirmed Gutierrez's findings and recommended users install the latest service packs for Windows XP and Windows 2000. Independent security consultants Secunia said the vulnerability "has been confirmed on fully patched systems running Windows XP and Windows 2000." Secunia urged Windows XP and Windows 2000 users to restrict traffic in border routers and firewalls as a temporary workaround. Users could also disable the "Client for Microsoft Networks" for network cards to impact file sharing functionality. The flaw also reportedly affects Windows 95, 98, and Me. Secunia Advisory SA11482: http://secunia.com/advisories/11482/

Category 24.2 *Windows NT/2K/XP*

2004-04-29 **Microsoft SSL patch bug confirmation Windows 2K 2000**

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1578752,00.asp

April 29, eWEEK — Microsoft confirms bug in SSL patch.

Microsoft Corp. has confirmed in a knowledge base article that its patch for a critical bug can cause some Windows 2000 systems to lock up and fail at boot time. The patch is for a particularly critical vulnerability of which experts have begun to see exploits in the last few days. The knowledge base article goes by the unusually long name: "Your computer stops responding, you cannot log on to Windows, or your CPU usage for the System process approaches 100 percent after you install the security update that is described in Microsoft Security Bulletin MS04-011." The article also gives one specific example, where the Nortel Networks VPN client is installed and the IPSec Policy Agent is set to Manual or Automatic for the startup type. In such cases, the article suggests disabling the IPSec Policy Agent.

Category 24.2 *Windows NT/2K/XP*

2004-05-11 **Microsoft patch vulnerability security bulletin code execution attack**

DHS IAIP Daily; http://www.microsoft.com/security/security_bulletins/200405_windows.asp

May 11, Microsoft — Microsoft Security Bulletin MS04-015: Vulnerability in Help and Support Center Could Allow Remote Code Execution.

A remote code execution vulnerability exists in the Help and Support Center because of the way that it handles HCP URL validation. If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges. Users whose accounts are configured to have fewer privileges on the system would be at less risk than users who operate with administrative privileges. Microsoft recommends that customers install the update at the earliest opportunity.

Category 24.2 *Windows NT/2K/XP*

2004-05-12 **windows microsoft security flaw patch sofware PC XP Server 2003**

NewsScan

NEW MICROSOFT WINDOWS SECURITY FLAW

Microsoft has identified and released a Windows software patch for a new flaw that could allow hackers to take control of a PC by luring users to a malicious Web site and getting them to take certain actions there. The security flaw affects the latest versions of Windows, including Windows XP, and software for networked computers such as Windows Server 2003. A user would be vulnerable to the security flaw only by visiting the attacker's Web site and performing several actions there. (Reuters/USA Today 12 May 2004)

Category 24.2 *Windows NT/2K/XP*

2004-08-19 **network time synchronization protocol NTP Microsoft operating systems Active Directory vulnerability time spoofing attacks**

DHS IAIP Daily; http://www.securityfocus.com/bid/10980

August 19, SecurityFocus — Microsoft NTP time synchronization spoof weakness.

The NTP implementation in Microsoft operating systems is vulnerable to time spoofing attacks. An attacker may be able to alter the time on the domain controller, causing the entire domain to synchronize with the attacker specified time. This weakness may allow a malicious user to deny service to legitimate users, as correct time is required for many operations, including domain authentication and X.509 certificate expiration times. This weakness is reported to exist in all versions of Microsoft operating systems that include Active Directory support. Microsoft has implemented a default failsafe for time synchronization that prevents an attacker from adjusting the time for more than 12 hours. By setting this to a smaller amount, an attacker would have to spend more time altering the clock by significant amounts.

Category 24.2 *Windows NT/2K/XP*

2004-08-19 **Microsoft Windows XP SP2 bugs vulnerability shell folder**

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1637596,00.asp

August 19, eWEEK — Bugs, exploits dog XP SP2.

Microsoft has issued a hotfix for Windows XP Service Pack 2 to solve a problem about which many users have complained: programs that attempt to connect to loopback addresses other than 127.0.0.1 get error messages. However, since it is a hotfix, it is not fully supported. It is expected that Microsoft will issue a more permanent fix in the future. Meanwhile, security researchers are reporting a new vulnerability in SP2 that could allow a malicious Website to deposit an attack program on a user's system. The attack utilizes Internet Explorer's drag-and-drop features and the Windows "shell folders" to copy an executable from a malicious Website to a user's startup folder, from which it would execute the next time the user logged on. Secunia, a security consulting firm, said the attack works on a fully patched Windows XP Service Pack 1 system, and that the drag-and-drop approach could be replaced with a single click. For the attack to succeed, the user would have to visit a Website that hosted it and follow the instructions. Any attack code deposited would be scanned by anti-virus software on the user's computer.

Category 24.2 *Windows NT/2K/XP*

2004-08-30 **Microsoft Windows XP Service Pack 2 SP2 security update**

DHS IAIP Daily; http://www.uscert.gov/cas/alerts/SA04−243A.html

August 30, US-CERT — Cyber Security Alert SA04-243A: Security Improvements in Windows XP Service Pack 2.

Windows XP Service Pack 2 is a major operating system update that contains a number of new security updates and features. Like other Microsoft Service Packs, Windows XP Service Pack 2 also includes previously released security fixes and other operating system updates. To help protect your Windows XP computer from attacks and vulnerabilities, install Service Pack 2 using Windows Update or Automatic Updates. Service Pack 2 makes significant changes to improve the security of Windows XP, and these changes may have negative effects effects on some programs and Windows functionality. Before you install Service Pack 2, back up your important data and consult your computer manufacturer's web site for information about Service Pack 2. Downloads available at: http://www.microsoft.com/windowsxp/sp2/default.mspx

---

Category 24.2 *Windows NT/2K/XP*

2004-09-17 **Microsoft patch fix early warning systems customers**

NewsScan

PATCH DEALS FAVOR BIG BUSINESS

Microsoft has quietly begun giving some of its largest customers early warning of what types of security patches it will be releasing. Under the free program, some customers are receiving three business days' notice as to how many security fixes Microsoft plans to release in its regular monthly bulletins, and which Microsoft products are affected. Customers also can learn how severe a threat the flaws pose several days before the general public gets that information. Microsoft began testing the program last year, and expanded it in April. It has not been widely publicized, and Microsoft has been offering the service to some customers individually through sales representatives. (The Australian 17 Sep 2004) Rec'd from John Lamp, Deakin U.

Category 24.2 *Windows NT/2K/XP*

2004-11-27 **Microsoft WINS packet memory overwrite vulnerability code execution attack**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Nov/1012341.html

November 27, SecurityTracker — Microsoft WINS Memory overwrite lets remote users execute arbitrary code.

It is reported that a remote user can send a specially crafted WINS packet to the target server on TCP port 42 to modify a memory pointer and write arbitrary contents to arbitrary memory locations. This could permit a remote user to execute arbitrary code on the target system. There is no solution at this time.

Category 24.2 *Windows NT/2K/XP*

2004-12-07 **Microsoft Windows 2000 2K XP Resource Kit buffer overflow vulnerability no update issued**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Dec/1012435.html

December 07, SecurityTracker — Microsoft Windows Resource Kit buffer overflow and input validation holes.

Several vulnerabilities were reported in the 'w3who.dll' Microsoft ISAPI extension in the Windows 2000/XP Resource Kit. A remote user can execute arbitrary code on the target system because the software does not properly validate user-supplied input before displaying HTTP headers or error messages. A remote user can create a specially crafted URL that, when loaded by a target user, will cause arbitrary scripting code to be executed by the target user's browser. No solution is available at this time.

Category 24.2 *Windows NT/2K/XP*

2004-12-14 **Microsoft security patches update release December 2004 Wordpad DHCP HyperTerminal Windows Kernel LSASS WINS**

DHS IAIP Daily; http://www.microsoft.com/technet/security/current.aspx

December 14, Microsoft — Microsoft releases December security updates.

Microsoft released five security updates on Tuesday, December 14. Vulnerable products are Wordpad, DCHP, HyperTerminal, Windows Kernel and LSASS, and WINS. Successful exploitation of the vulnerabilities in these products could allow a malicious user to execute remote code, launch a denial of service, or gain elevated privileges. Microsoft has assigned a risk rating of " Important" to these issues and recommends users install updates as soon as possible.

Category 24.2 *Windows NT/2K/XP*

2004-12-22 **EU Microsoft antitrust media player**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A18543-2004Dec22.html

EU COURT RULES AGAINST MICROSOFT

A European Union judge today ruled that Microsoft must immediately submit to sanctions imposed by EC regulators after they found that Microsoft broke antitrust laws by integrating its Windows Media Player into Windows, thus putting rival media software companies at a disadvantage. Microsoft had appealed the initial decision, arguing that pulling Media Player out of Windows would degrade its performance, but in today's ruling, Chief Judge Bo Vesterdorf of the Court of First Instance found that postponing sanctions would give Microsoft time to strengthen its grip on the market for media playing applications. Microsoft must now create two versions of Windows for European distribution -- one that contains Media Player and one without. Microsoft announced it would comply while contemplating its next legal move. (Washington Post 22 Dec 2004)

Category 24.2 *Windows NT/2K/XP*

2004-12-24 **Microsoft Windows unpatched holes warning Symantec heap overflow vulnerability no update issued**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/holes/s
tory/0,10801,98532,00.html

December 24, IDG News Service — Researchers warn of multiple unpatched Windows holes.

The antivirus company Symantec Corp. warned its customers about a number of critical holes in Microsoft Corp.'s Windows operating system that surfaced late Thursday, December 23, that could make Windows systems vulnerable to compromise by remote attackers. Symantec acted after security researchers published the details of the heap overflow vulnerabilities in messages posted to online security news groups, including the Bugtraq mailing list and on xfocus.net. The flaws affect most supported versions of Windows, but Microsoft has not yet issued a patch for the newly disclosed holes. Windows users are vulnerable to Internet based attacks until patches are issued, Symantec said. Symantec recommended that Windows users exercise caution when receiving and opening files from unknown sources.

Category 24.2 *Windows NT/2K/XP*

2004-12-28 **Microsoft Windows kernel file parsing denial of service DoS vulnerability XP SP2 not vulnerable**

DHS IAIP Daily; http://security−
protocols.com/modules.php?name=News&file=art icle&sid=2357

December 28, Security Protocols — Microsoft Windows Kernel ANI file parsing crash and denial of service.

Parsing a specially crafted ANI file causes the Windows kernel to crash or stop to work properly. An attacker can crash or freeze a target system if he sends a specially crafted ANI file within an HTML page or within an e-mail. Two vulnerabilities exist in the Windows kernel when it parses ANI files. These vulnerabilities are due to improper input validation of the frame number set and the rate number set in the ANI file header. Windows XP SP2 is not vulnerable.

Category 24.2 *Windows NT/2K/XP*

2005-01-11 **Microsoft Windows Security Bulletin cursor icon format handling vulnerability code execution full rights attacker critical rating update issued**

DHS IAIP Daily; http://www.microsoft.com/technet/Security/bulletin/ms05−
002. mspx

VULNERABILITY IN CURSOR AND ICON FORMAT HANDLING COULD ALLOW REMOTE CODE EXECUTION

This update resolves several newly-discovered, privately reported and public vulnerabilities. An attacker who successfully exploited the most severe of these vulnerabilities could take complete control of an affected system, install programs; view, change, or delete data; or create new accounts that have full privileges. Microsoft has assigned a risk rating of "Critical" to these issues and recommends that customers apply the update immediately.

Category 24.2 *Windows NT/2K/XP*

2005-01-11 **Microsoft Windows Security Bulletin indexing service format handling vulnerability code execution full rights attacker important rating update issued**

DHS IAIP Daily; http://www.microsoft.com/technet/security/bulletin/MS05−
003. mspx

VULNERABILITY IN THE INDEXING SERVICE COULD ALLOW REMOTE CODE EXECUTION

A remote code execution vulnerability exists in the Indexing Service because of the way that it handles query validation. An attacker could exploit the vulnerability by constructing a malicious query that could potentially allow remote code execution on an affected system. An attacker who successfully exploited this vulnerability could take complete control of an affected system. While remote code execution is possible, an attack would most likely result in a denial of service condition. Microsoft has assigned a risk rating of "Important" to this issue and recommends that system administrators consider applying the security update.

Category 24.2 *Windows NT/2K/XP*

2005-01-11 **Microsoft Windows Security Bulletin HTML Help vulnerability code execution full rights attacker critical rating update issued**

DHS IAIP Daily; http://www.microsoft.com/technet/security/Bulletin/MS05−001. mspx

MS05-001: VULNERABILITY IN HTML HELP COULD ALLOW CODE EXECUTION

A vulnerability exists in the HTML Help ActiveX control in Windows that could allow information disclosure or remote code execution on an affected system. If a user is logged on with administrative privileges, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full privileges. Users whose accounts are configured to have fewer privileges on the system could be less impacted than users who operate with administrative privileges. Microsoft has assigned a risk rating of "Critical" to this issue and recommends that customers install the update immediately.

Category 24.2 *Windows NT/2K/XP*

2005-01-12 **Microsoft Windows multiple vulnerabilities denial of service privilege escalation code execution update issued**

DHS IAIP Daily; http://www.us−cert.gov/cas/techalerts/TA05−012A.html

MULTIPLE VULNERABILITIES IN MICROSOFT WINDOWS ICON AND CURSOR PROCESSING

Microsoft Windows contains multiple vulnerabilities in the way that it handles cursor and icon files. A remote attacker could execute arbitrary code or cause a denial-of-service condition. If a remote attacker can persuade a user to access a specially crafted bitmap image, icon, or cursor file, the attacker may be able to execute arbitrary code on that user's system, with their privileges. Potentially, any operation that displays an image could trigger exploitation, for instance, browsing the file system, reading HTML e-mail, or browsing Websites. A solution is to install the update as described in Microsoft Security Bulletin MS05-002: http://www.microsoft.com/technet/security/bulletin/ms05-002. mspx

---

Category 24.2 *Windows NT/2K/XP*

2005-01-26 **piracy Microsoft Windows XP software updates patches fixes enhancements**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A37035-2005Jan26.html

MICROSOFT: SOFTWARE FIXES AREN'T FOR PIRATES

Microsoft will soon be requiring that Windows XP users verify that their copy of the software is genuine before they'll be able to receive "greater reliability, faster access to updates, and richer user experiences." Although users of pirated copies of Windows will still be able get security patches, they won't be able to get other enhancements to Windows. The company will be expanding a trial authentication program it began last fall, and will make mandatory in mid-2005 for all users seeking to access software updates, downloads and security fixes for Windows. (Reuters/Washington Post 26 Jan 2005)

Category 24.2 *Windows NT/2K/XP*

2005-02-02 **Microsoft software international government threat early warning attack prevention mitigation national security public safety**

DHS IAIP Daily; http://www.nytimes.com/aponline/technology/AP−Microsoft−Secu rity.html

MICROSOFT OFFERING GOVERNMENTS EARLY WARNINGS

Microsoft offered Wednesday, February 2, to begin alerting the world's governments early to cyberthreats and security flaws in its attack-prone software. Microsoft also wants to work with governments to help prevent and mitigate the damage from hacker attacks, said Giorgio Vanzini, the director of Microsoft's government engagement team. Microsoft already provides the U.S. government with early warnings. Vanzini said extending the program aims to protect critical infrastructure given that major Internet attacks can affect national security, economic stability and public safety. The new program intends to complement Microsoft's existing Government Security Program, in which governments and agencies may review Microsoft's proprietary source code for Windows operating systems and Office business software and evaluate for themselves the software's security and ability to withstand attacks. So far three countries, Canada, Chile and Norway, as well as the U.S. state of Delaware, have been engaged in the new project, Vanzini said. Governments currently under a trade embargo with the United States are not eligible to sign up to the program, which is provided free of charge.

Category 24.2 *Windows NT/2K/XP*

2005-02-08 **Microsoft February 2005 security bulletin critical important moderate issues Office Windows Internet Explorer flaws vulnerabilities**

DHS IAIP Daily; http://www.microsoft.com/technet/security/bulletin/ms05−feb.
mspx

MICROSOFT FEBRUARY SECURITY BULLETIN RELEASED

Microsoft's February Security Bulletin contains eight "Critical" issues, three "Important" issues and one "Moderate" issue. Software affected by these issues includes: Office, Project, Visio, Windows, Windows Media Player, Windows Messenger, MSN Messenger, Internet Explorer, the .NET Developer Tools and Platform. Exploitation of these vulnerabilities could result in remote code execution, information disclosure, or elevation of privilege. Updates are available through Microsoft at Source link below.

Category 24.2 *Windows NT/2K/XP*

2005-03-05 **Microsoft Windows Server 2003 XP SP2 LAND vulnerability denial of service DoS attack TCP packet SYN flag firewall enable**

DHS IAIP Daily; http://www.securityfocus.com/archive/1/392354/2005−03−
03/200 5−03−09/0

WINDOWS SERVER 2003 AND XP SP2 LAND ATTACK VULNERABILITY

Windows Server 2003 and XP SP2 (with Windows Firewall turned off) are vulnerable to a Denial of Service through a LAND attack. A LAND attack occurs when a user sends a TCP packet with SYN flag set and source and destination IPs are the same and source and destination ports are the same, using the target system IP address. Enable Windows Firewall as a workaround.

Category 24.2 *Windows NT/2K/XP*

2005-03-14 **Air Force Microsoft agreement security patches beta test versions**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/35271−1.html

AIR FORCE TO GET MICROSOFT SECURITY PATCHES BEFORE OFFICIAL RELEASE

The Air Force now has a jump-start on implementing Microsoft security patches thanks to a plan that allows the department to receive beta test versions of patches. Under the company's Security Update Validation Program, the Air Force will receive beta patches before they are officially released. After the department tests them, the patches will be distributed to other federal agencies. The Air Force is "in discussions" with the Defense Department about ways to bring the security services concept to other branches of the military and federal agencies, according to John Gilligan, Air Force CIO. Under the program, Microsoft will identify vulnerabilities and implement fixes across the enterprise.

Category 24.2 *Windows NT/2K/XP*

2005-03-24 **Microsoft Windows Remote Desktop vulnerability denial of service DoS attack update issued**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2005/Mar/1013552.html

MICROSOFT WINDOWS REMOTE DESKTOP 'TSSHUTDN.EXE' REMOTE DENIAL OF SERVICE VULNERABILITY

A vulnerability was reported in Microsoft Windows Remote Desktop. A remote authenticated user can shutdown the target system. A non-administrative user can remotely shut down a Microsoft Windows XP Service Pack 1 (SP1)-based computer by using the TSShutdn.exe command. This problem occurs because the Remote Desktop does not check the Force shutdown from a remote system user right. A hotfix is available from Microsoft Product Support Services. See the knowledge base article for more information: http://support.microsoft.com/kb/889323/

Category 24.2 *Windows NT/2K/XP*

2005-04-04 **Microsoft Jet Database Engine database buffer overflow vulnerability command execution attack no update issued**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/0306

MICROSOFT JET DATABASE ENGINE DB FILE BUFFER OVERFLOW VULNERABILITY

A new vulnerability was identified in Microsoft Jet, which may be exploited by attackers to execute arbitrary commands. The flaw resides in the "msjet40.dll" library, and occurs when handling a specially crafted "mdb" file, which may be exploited by attackers to compromise a vulnerable system by convincing a user to open a malicious database file with a vulnerable application. No solution is currently available.

Category 24.2 *Windows NT/2K/XP*

2005-04-08 **Microsoft Windows Domain Name resource cache corruption vulnerability NT 2000 2K spoofed DNS response update issued**

DHS IAIP Daily; http://www.securityfocus.com/bid/6791/discussion/

MICROSOFT WINDOWS DNS RESOURCE RECORD CACHE CORRUPTION VULNERABILITY

A vulnerability has been discovered in the DNS server on the Windows NT and Windows 2000 operating systems. The problem occurs in the caching of glue records. It has been reported that glue records received from non-delegated name servers will be cached by default. This may allow for a malicious server to respond to a legitimate DNS query with a spoofed DNS response, designed to contain the necessary glue record characteristics. Solution available at:
http://support.microsoft.com/kb/241352/EN-US/

Category 24.2 *Windows NT/2K/XP*

2005-08-26 **Microsoft Windows 2000 2K XP design flaw hackers hide malicious code anti-virus scanner registry**

DHS IAIP Daily;
http://www.techweb.com/showArticle.jhtml?articleID=170100835

WINDOWS FLAW MAY LET HACKERS HIDE CODE FROM ANTI-VIRUS SCANNERS

A flaw in how Windows handles entries in the all-important registry can be used by hackers to hide evidence of malicious code from a wide swath of commercial anti-virus and anti-spyware scanners, the SANS Internet Storm Center reported Friday, August 26. Extra-long key entries (those greater than 254 characters) are mishandled by the Windows registry editor, and essentially "disappear" from view, as do others added to the key after that because the editor stops at that too-long key, thinking it is the last in the section. Worse, many malicious code scanners have a similar blind spot, and also stop processing the registry for anomalous entries when they come to a too-long key. The technique would let attackers add their malicious software to the "Run" registry key which lists the programs or components that automatically launch at Windows' boot. The weakness, said Secunia, affects Windows 2000 and XP, including fully patched XP SP2 systems.

Category 24.2 *Windows NT/2K/XP*

2005-10-03 **error-handling code systems engineering software design quality assurance QA operating system file system inconsistency**

RISKS 24 06

INCONSISTENT ERROR-HANDLING CODE IN WINDOWS

In the Windows XP command interpreter CMD.EXE (the default command line shell) one can specify multiple arguments to the DEL(ete) command, in order to delete multiple files. If at least one of the files can be deleted, the command will not complain about any nonexistent files specified as arguments. For example:

```
C:\> echo.>foo
C:\> del nonexistent foo
C:\> del nonexistent
Could Not Find C:\nonexistent
```

This behavior is non-orthogonal and risky. If one mistypes the name of one of several files that are to be deleted, that file will silently continue to exist. The same will happen if one of the files has the hidden attribute set: DEL will silently ignore it, rather than issue an error message. Although one should not depend on a delete command to reliably obliterate data, the current behavior can lead to difficult-to-locate bugs, especially in scripts.

Further examination of the command reveals other instances of non-orthogonal behavior. When specifying multiple non-existent files as arguments, DEL will complain only about the first one, but when specifying multiple files with the read-only attribute set, DEL will complain about each one. Also DEL, never sets the ERRORLEVEL environment variable to indicate an error, although other commands, like DIR, set it correctly.

The logic behind a correctly-operating implementation of DEL is trivial.

```
Errorlevel = 0
foreach filename
    if not delete(filename) then
        display_error_message(filename)
        errorlevel = 1
    end if
end foreach
exit(errorlevel)
```

If a central and critical piece of the Windows operating system, such as the command shell, can't get the above logic right, what are the chances of having in the system a secure TCP/IP stack, web browser, or firewall?

[Analysis by Diomidis Spinellis]

Category 24.2 *Windows NT/2K/XP*

2005-10-28 **operating system kernel deficiencies compensation ring authorization run-time limitations malicious software malware virus worm Windows**

http://www.computerworld.com/printthis/2005/0,4814,105776,00.html

AXE RUNTIME SUPPLEMENTS WINDOWS KERNEL

Researchers Amit Singh, Anurag Sharma and Steve Welch of IBM's Almaden Lab announced their "Axe runtime" package -- standing for "Assured Execution Environment" -- at the end of October 2005. The package provides the missing pieces for the Windows kernel: a security ring structure differentiating between authorized and unauthorized software. Only authorized software can run on the system being controlled by Axe and the authors claim that malware authors will find it almost impossible to gain authorization for their malicious code.

Category 24.2 *Windows NT/2K/XP*

2005-12-28 **Microsoft Windows metafile handling buffer overflow vulnerability**

DHS IAIP Daily; http://www.microsoft.com/technet/security/Bulletin/MS05−
053. mspx

TECHNICAL CYBER SECURITY ALERT TA05-362A:
MICROSOFT WINDOWS METAFILE HANDLING BUFFER OVERFLOW.

Microsoft Windows Metafiles are image files 14 that can contain both vector and bitmap-based picture information. Microsoft Windows contains routines for displaying various Windows Metafile formats. However, a lack of input validation in one of these routines may allow a buffer overflow to occur, and in turn may allow remote arbitrary code execution. This new vulnerability may be similar to one Microsoft released patches for in Microsoft Security Bulletin MS05-053. However, publicly available exploit code is known to affect systems updated with the MS05-053 patches. Not all anti-virus software products are currently able to detect all known variants of exploits for this vulnerability. However, US-CERT recommends updating anti-virus signatures as frequently as practical to provide maximum protection as new variants appear. There is no known patch for this issue at this time. Information on potential workarounds is available on the US-CERT Website. Microsoft Security Bulletin MS05-053: http://www.microsoft.com/technet/security/Bulletin/MS05-053. mspx US-CERT Vulnerability Note VU#181038, Microsoft Windows Metafile handler buffer overflow: http://www.kb.cert.org/vuls/id/181038 CVE-2005-4560: http://nvd.nist.gov/nvd.cfm?cvename=CVE-2005-4560

Category 24.2 *Windows NT/2K/XP*

2005-12-28 **Technical Cyber Security Alert Microsoft Windows Metafile Handling Buffer Overflow image files vector bitmap picture information arbitrary updated patches software products detect**

DHS IAIP Daily; http://www.us−cert.gov/cas/techalerts/TA05−362A.html

TECHNICAL CYBER SECURITY ALERT TA05-362A:
MICROSOFT WINDOWS METAFILE HANDLING BUFFER OVERFLOW.

Microsoft Windows Metafiles are image files that can contain both vector and bitmap-based picture information. Microsoft Windows contains routines for displaying various Windows Metafile formats. However, a lack of input validation in one of these routines may allow a buffer overflow to occur, and in turn may allow remote arbitrary code execution. This new vulnerability may be similar to one Microsoft released patches for in Microsoft Security Bulletin MS05-053. However, publicly available exploit code is known to affect systems updated with the MS05-053 patches. Not all anti-virus software products are currently able to detect all known variants of exploits for this vulnerability. However, US-CERT recommends updating anti-virus signatures as frequently as practical to provide maximum protection as new variants appear. There is no known patch for this issue at this time. Information on potential workarounds is available on the US-CERT Website. Microsoft Security Bulletin MS05-053: http://www.microsoft.com/technet/security/Bulletin/MS05-053. mspx US-CERT Vulnerability Note VULNERABILITY#181038, Microsoft Windows Metafile handler buffer overflow: http://www.kb.cert.org/vuls/id/181038 CVE-2005-4560: http://nvd.nist.gov/nvd.cfm?cvename=CVE-2005-4560

Category 24.2 *Windows NT/2K/XP*

2006-01-02 **Microsoft WMF flaw exploit unofficial patch SANS ISC**

DHS IAIP Daily; 23
http://www.techworld.com/security/news/index.cfm?NewsID=5070 &inkc=0

SANS: DON'T WAIT FOR MICROSOFT TO FIX WMF FLAW

Windows users should install an unofficial security patch now, without waiting for Microsoft to make its move, advised security researchers at the SANS Institute's Internet Storm Center (ISC). Their recommendation follows a new wave of attacks on a flaw in the way versions of Windows from 98 through XP handle malicious files in the WMF (Windows Metafile) format. One such attack arrives in an e-mail message entitled "happy new year," bearing a malicious file attachment called "HappyNewYear.jpg" that is really a disguised WMF file, security research companies, including iDefense and F-Secure, said Sunday, January 1. Even though the file is labeled as a JPEG, Windows recognizes the content as a WMF and attempts to execute the code it contains. Staff at the ISC worked over the weekend to validate and improve an unofficial patch developed by Ilfak Guilfanov to fix the WMF problem, according to an entry in the Handler's Diary, a running commentary on major IT security problems on the ISC Website. Updated version of Guilfanov's patch: http://isc.sans.org/diary.php?storyid=999

Category 24.2 *Windows NT/2K/XP*

2006-01-03 **code execution vulnerability Microsoft Windows graphics rendering engine SYSTEM privileges**

DHS IAIP Daily; http://www.securityfocus.com/bid/16074/references 23

MICROSOFT WINDOWS GRAPHICS RENDERING ENGINE WMF SETABORTPROC CODE EXECUTION VULNERABILITY

Microsoft Windows WMF graphics rendering engine is affected by a remote code execution vulnerability. The problem presents itself when a user views a malicious WMF formatted file, triggering the vulnerability when the engine attempts to parse the file. The issue may be exploited remotely or by a local attacker. Any remote code execution that occurs will be with the privileges of the user viewing a malicious image. An attacker may gain SYSTEM privileges if an administrator views the malicious file. Solution: Microsoft has released a security advisory (Microsoft Security Advisory 912840) confirming this issue. The advisory contains information about workarounds. Microsoft plans to release updates to address this issue on Tuesday, January 10. Microsoft Security Advisory 912840: http://www.microsoft.com/technet/security/advisory/912840.mspx

---

Category 24.2 *Windows NT/2K/XP*

2006-01-03 **Microsoft Windows WMF vulnerability third-party patch warning**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1907562,00.asp 23

MICROSOFT: BEWARE OF THIRD-PARTY WMF PATCH

Microsoft Corp. has slapped a "buyer beware" tag on a third-party patch for the zero-day Windows Metafile (WMF) flaw and promised that its own properly tested update will almost certainly ship Tuesday, January 10. The company's latest guidance comes days after an unofficial hotfix from reverse-engineering guru Ilfak Guilfanov got rare blessings from experts at the SANS ISC (Internet Storm Center) and anti-virus vendor F-Secure Corp. Guilfanov, author of the IDA (Interactive Disassembler Pro), released an executable that revokes the "SETABORT" escape sequence that is the crux of the problem. The hotfix was tested and approved for use by many security experts, but Microsoft says it cannot vouch for the quality of the fix. Microsoft said its own patch has already been developed and is going through a rigid round of quality assurance testing. Last-minute glitches in the patch testing process could still delay the update. As a general rule, the company never recommends third-party updates. Ever since attackers started exploiting the bug to push malware on vulnerable Windows systems (XP SP2 included), the company has thrown all its security resources into the investigation and patch-creation process, making it virtually impossible to validate the third-party code.

Category 24.2 *Windows NT/2K/XP*

2006-01-03 **WMF vulnerability zero-day Microsoft Windows patch release plan**

DHS IAIP Daily; 23
http://www.securitypipeline.com/news/175800841;jsessionid=HCQOZBHQGSYK0QSNDBCSKHSCJUMEKJVN

MICROSOFT PLANS TO PATCH ZERO-DAY WINDOWS BUG

Microsoft plans to patch an increasingly-dangerous zero-day vulnerability in Windows next week as part of its monthly security update, the Redmond, WA,-based developer said Tuesday, January 3. "Microsoft has completed development of the security update for the vulnerability," a company spokesperson stated. "The security update is now being localized and tested to ensure quality and application compatibility." The move is just the latest in the week-long story of a new vulnerability uncovered in Windows' rendering of WMF (Windows Metafile) images, and an increasingly long list of both exploits and Websites using these exploits to hack into PCs. As far as some researchers are concerned, Microsoft's promise is overdue.

Category 24.2 *Windows NT/2K/XP*

2006-01-04 **Microsoft Windows WMF vulnerability users await patch**

EDUPAGE; http://news.zdnet.com/2100-1009_22-6016747.html 23

USERS SWEAT BULLETS WAITING FOR WMF PATCH

Security experts are warning about the danger of a currently unpatched vulnerability in all current versions of the Windows operating system, but Microsoft has said the patch won't be released until January 10, its next scheduled patch release date. Sam Curry of Computer Associates International said, "This vulnerability is rising in popularity among hackers, and it is simple to exploit." Others estimate that more than one million computers have already been infected worldwide, noting that attacks have taken the form of malicious Web sites, Trojan horses, and instant messaging worms. The flaw, which affects how Windows handles Windows Meta File (WMF) images, is especially dangerous because users need only view an image designed to take advantage of the vulnerability to have their computers infected. Despite the calls for an immediate patch, Microsoft, which adopted a schedule of monthly patch updates, has said the fix for the current bug will not be released until the next scheduled group of patches. In the meantime, Microsoft is warning users to be careful about what sites they visit. Most Internet users, however, do not have a level of awareness of such security concerns to protect themselves, according to Stacey Quandt, an analyst with the Aberdeen Group.

Category 24.2 *Windows NT/2K/XP*

2006-01-05 **Microsoft Windows WMF vulnerability patch release**

DHS IAIP Daily; 23
http://www.cnn.com/2006/TECH/internet/01/05/wmfflaw/index.html

MICROSOFT RELEASES PATCH FOR WMF FLAW

Microsoft has released a patch for a vulnerability in some Windows graphics files. For more than a week, criminal hackers have been exploiting the flaw in Windows Meta File, or WMF. About 90 percent of computer users worldwide use some form of the Windows operating system. The company became aware of the malicious attacks Tuesday, December 27. What's especially dangerous about the attacks: Your computer could be infected with viruses, spyware or other malicious programs just by viewing a Webpage, an e-mail message, or an Instant Message that contains one of the contaminated images. Computer security experts have been dealing with scores of variations on the attack since it was discovered. "Nobody knew it was coming," security expert Rick Howard of Counterpane Internet Security said. "There was no security intervention or mitigation for it." Unlike infamous computer worms and viruses like Blaster, Code Red or I Love You, the WMF attack is not spreading like wildfire across the Internet. Most of the malicious efforts fit the patterns of recent attacks. They are not designed to earn bragging rights for a brash programmer, but instead are likely tied to theft, fraud and organized crime. US-CERT Technical Cyber Security Alert TA06-005A: Update for Microsoft WMF vulnerability: http://www.uscert.gov/cas/techalerts/TA06-005A.html Microsoft Security Bulletin MS06-001: http://www.microsoft.com/technet/security/Bulletin/MS06-001. mspx

---

Category 24.2 *Windows NT/2K/XP*

2006-01-05 **Microsoft Windows WMF vulnerability patch early release**

EDUPAGE; http://news.zdnet.com/2100-1009_22-6020070.html 23

MICROSOFT RELEASES WMF PATCH EARLY

Responding to concerns that the recently disclosed Windows Meta File (WMF) vulnerability presented serious risk, Microsoft has released a patch ahead of the company's monthly patch release date. Microsoft said that testing of the patch was completed early and that there was "strong customer sentiment that the release should be made available as soon as possible." Some security experts, warning of the threat posed by the flaw, had even encouraged users to install a third-party patch developed by a European programmer. The patch is for Windows 2000, Windows XP, and Windows Server 2003; although Microsoft had earlier said the vulnerability also affected Windows 98 and Windows ME, the company now says those operating systems are not affected by the flaw. With the release, Microsoft acknowledged that the risk to unpatched systems is critical, though it said data indicated that the infection rate from attacks that exploit the weakness was low to moderate so far. Some security experts offered a different characterization of the situation, saying they have identified thousands of Web sites that exploit the flaw.

Category 24.2 *Windows NT/2K/XP*

2006-01-06 **Microsoft Windows WMF vulnerability critical patch release**

DHS IAIP Daily; 23
http://www.techweb.com/showArticle.jhtml?articleID=175802037

MICROSOFT PLANS TWO MORE CRITICAL PATCHES THIS WEEK [6 JAN 2006]

Microsoft may have released the Windows Metafile hot fix, but it has other patches still to come Tuesday, January 10, the Redmond, WA-based developer said late Thursday, January 5. In the monthly pre-patch notification it puts out five days prior to releasing fixes, Microsoft warned users that two security bulletins, both tagged as "Critical," will be issued Tuesday. In Microsoft's terminology, Critical means that a vulnerability can be remotely exploited. One of the two bulletins will involve Windows, and the other will affect Microsoft Office and Microsoft Exchange, the company's business suite and e-mail server software, respectively. Multiple non-security, high-priority updates will also be released Tuesday, as will an updated Windows Malicious Software Removal Tool. Microsoft will host a follow-up Webcast Wednesday, January 11, to answer questions about the fixes. More details can be found in the advance notice posted on Microsoft's Website: http://www.microsoft.com/technet/security/bulletin/advance.mspx

---

Category 24.2 *Windows NT/2K/XP*

2006-01-09 **Microsoft Windows WMF new vulnerability denial of service DoS arbitrary code execution**

DHS IAIP Daily; http://www.securitypipeline.com/news/175802826 23

MORE UNPATCHED BUGS LOOSE IN MICROSOFT WINDOWS METAFILE

Just days after Microsoft rushed out a patch for a bug in Windows Metafile (WMF) image processing, a security company has warned customers that multiple memory corruption vulnerabilities in the same rendering engine could leave users open to attack. "An attacker may leverage these issues to carry out a denial of service attack or execute arbitrary code," Symantec said in a vulnerability alert issued through its DeepSight Management System. The bugs may be associated with the one patched Thursday, January 5, by Microsoft, but they involve different functions of the Windows WMF rendering engine, added Symantec, which highlighted the various values and structures within the engine which could be exploited. "Reports indicate that these issues lead to a denial of service condition, however, it is conjectured that arbitrary code execution is possible as well," the Symantec alert went on. If true, the dangers of these new vulnerabilities are identical to the flaw that Microsoft fixed last week. Like that bug, these newly-discovered vulnerabilities can be exploited with a maliciously-crafted WMF file that's posted on a Website, opened from an e-mail attachment, or launched with Microsoft or third-party image applications.

Category 24.2 *Windows NT/2K/XP*

2006-01-09 **Microsoft scour source code discover vulnerability WMF**

DHS IAIP Daily; 23
http://news.com.com/Microsoft+to+hunt+for+new+species+of+Win
dows+bug/2100−1002_3−6024778.html?tag=cd.lede

MICROSOFT TO HUNT FOR NEW SPECIES OF WINDOWS BUG

Microsoft plans to scour its code to look for flaws similar to a recent serious Windows bug and to update its development practices to prevent similar problems in future products. The critical flaw, in the way Windows Meta File (WMF) images are handled, is different than any security vulnerability the software maker has dealt with in the past, said Kevin Kean and Debby Fry Wilson, directors in Microsoft's Security Response Center. Typical flaws are unforeseen gaps in programs that hackers can take advantage of and run code. By contrast, the WMF problem lies in a software feature being used in an unintended way. In response to the new threat, the software company is pledging to take a look at its programs, old and new, to avoid similar side effects. Microsoft has been working for years to improve its security posture, beginning with its Trustworthy Computing Initiative, launched in early 2002. The WMF problem is not a good advertisement for Microsoft's security efforts, one analyst said, as the legacy issue seemingly went undetected. "This should have been caught and eliminated years ago," said Gartner analyst Neil MacDonald.

Category 24.2 *Windows NT/2K/XP*

2006-01-11 **Microsoft Outlook Exchange vulnerability danger WMF exploit e-mail**

DHS IAIP Daily; 23
http://www.techweb.com/wire/security/175803652;jsessionid=KS
BY2QFNY1BIQQSNDBOCKHSCJUMEKJVN

MICROSOFT'S NEWEST BUG COULD BE SERIOUS, RESEARCHER SAYS

The Outlook and Exchange vulnerability disclosed by Microsoft Tuesday, January 10, has the potential to become a much more virulent problem than the long-hyped Windows Metafile (WMF) bug patched last week, said one of the e-mail flaw's discoverers Wednesday, January 11. The TNEF (Transport Neutral Encapsulation Format) vulnerability, which Microsoft spelled out in the MS06-003 security bulletin, is a flaw in how Microsoft's Outlook client and older versions of its Exchange server software decode the TNEF MIME attachment. TNEF is used by Exchange and Outlook when sending and processing messages formatted as Rich Text Format (RTF), one of the formatting choices available to Outlook users. "All that's required to exploit this is an e-mail message," said Mark Litchfield, director of NGS Software. "If you did it right, you could own every Outlook user in the world within a week," he said.

Category 24.2 *Windows NT/2K/XP*

2006-01-18 **Windows XP patch update delay Vista release Palladium**

DHS IAIP Daily; http://www.securityfocus.com/brief/107 23

WINDOW XP UPDATE DELAYED UNTIL AFTER VISTA

Microsoft will not release Windows XP Service Pack 3 until the second half of 2007, after the company's planned shipment date for its next-generation operating system Vista, the software giant said on Wednesday, January 18. Vista will add some long-overdue security features, including limiting the privileges of the everyday user account similar to Unix-based systems, such as Linux and the Mac OS X. Another security feature that Microsoft touted -- the next-generation secure computing base (NGSCB), formally known as "Palladium" -- will only be partially incorporated in Vista, and it's uncertain whether it will follow the industry-created standard. The last major update for Windows XP, known as Service Pack 2, was released in August 2004 and added a host of new security features and bug fixes to Microsoft's flagship desktop operating system. Vista's focus on security will not eradicate security flaws -- just this week the software giant released an update for the beta version of the operating system to fix the recent vulnerability in the Windows Meta File (WMF) format.

Category 24.2 *Windows NT/2K/XP*

2006-02-02 **Microsoft Windows SSDP UPnP vulnerability privilege escalation no official patch**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2006/0417 23

MICROSOFT WINDOWS SSDP AND UPNP SERVICES PRIVILEGE ESCALATION ISSUE.

A vulnerability has been identified in Microsoft Windows, which could be exploited by malicious users to obtain elevated privileges. This issue is due to an access validation error in the Simple Service Discovery Protocol (SSDP) and the Universal Plug and Play Device Host (UPnP) services that fail to properly validate user permissions, which could be exploited by local unprivileged attackers to bypass security restrictions and execute malicious programs with elevated privileges. Solution: The FrSIRT is not aware of any official supplied patch for this issue.

Category 24.2 *Windows NT/2K/XP*

2006-02-08 **Windows WMF vulnerability IE quality assurance**

DHS IAIP Daily; http://www.vnunet.com/vnunet/news/2149931/windows−hit− 23
yet−wm f−hole

WINDOWS HIT BY YET ANOTHER WMF HOLE.

Microsoft has issued a warning about a new vulnerability in the Windows Meta File (WMF) image format that affects older versions of Internet Explorer (IE). The vulnerability exists in IE 5.5 running on Windows 2000 and IE 5.01 on Windows ME. Users of IE 6 or other Windows versions are not affected by this vulnerability, Microsoft emphasized in a security advisory. Microsoft Security Advisory: http://www.microsoft.com/technet/security/advisory/913333.mspx

---

Category 24.2 *Windows NT/2K/XP*

2006-02-15 **Microsoft security patch February issue TCP/IP vulnerability**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1927250,00.asp 23

MICROSOFT CORRECTS SECURITY PATCH ISSUE.

Microsoft was forced to update one of its February security patches after some users were unable to install the fix that addressed a TCP/IP vulnerability in several versions of Windows. The software giant confirmed on its Website that security patch number MSO6-007 was altered to provide additional installation instructions after it was discovered that some people were having issues downloading the update. The company said the problem did not affect the content of the security patch itself. Microsoft said that shortly after the release of the patch on Tuesday, February 14, the company realized that the fix was not working properly when installed alongside its Inventory Tool for Microsoft Updates using its Automatic Updates, Windows Update, Windows Server Update Services and Systems Management Server 2003 management features.

Category 24.2 *Windows NT/2K/XP*

2006-04-11 **US CERT Technical Cyber Security Alert Microsoft Windows Internet Explorer arbitrary code execution denial-of-service DoS**

DHS IAIP Daily; http://www.uscert.gov/cas/techalerts/TA06−101A.html 23

US-CERT TECHNICAL CYBER SECURITY ALERT TA06-101A: MICROSOFT WINDOWS AND INTERNET EXPLORER VULNERABILITIES.

Microsoft has released updates that address critical vulnerabilities in Microsoft Windows and Internet Explorer. Exploitation of these vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary code or cause a denial-of-service on a vulnerable system. Microsoft Security Bulletin Summary for April 2006 addresses vulnerabilities in Microsoft Windows and Internet Explorer. Further information is available in the US-CERT Vulnerability Notes listed within the source advisory. Systems affected: Microsoft Windows and Microsoft Internet Explorer. Solution: Apply updates using the Security Bulletins site or Microsoft Update site. Microsoft Security Bulletin Summary for April 2006: http://www.microsoft.com/technet/security/bulletin/ms06-apr. mspx Microsoft Update site: https://update.microsoft.com/microsoftupdate/v6/muoptdefault .aspx?ln=en&returnurl=https://update.microsoft.com/microsoft update/v6/default.aspx?ln=en-us

---

Category 24.2 *Windows NT/2K/XP*

2006-04-26 **Microsoft Windows Shell COM object remote code execution vulnerability solution update**

DHS IAIP Daily; http://www.securityfocus.com/bid/17464/solution 23

MICROSOFT WINDOWS SHELL COM OBJECT REMOTE CODE EXECUTION VULNERABILITY.

Microsoft Windows Shell is prone to a remote code execution vulnerability. This issue is due to a flaw in its handling of remote COM objects. Analysis: If a user is logged on with administrative user rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights. For a detailed list of vulnerable products: http://www.securityfocus.com/bid/17464/info Solution: Microsoft has released an advisory along with fixes to address this issue. Microsoft has updated this security bulletin (MS06-015) to release new fixes due to problems with the fixes originally released with this bulletin. Customers who did not experience problems with Windows shell or Windows Explorer after installing the original fixes do not need to update their fixes. Microsoft Security Bulletin MS06-015: http://www.microsoft.com/technet/security/Bulletin/MS06-015. mspx

---

Category 24.2 *Windows NT/2K/XP*

2006-05-10 **Microsoft Windows path conversion weakness security bypass vulnerability no solution**

DHS IAIP Daily; http://www.securityfocus.com/bid/17934/references 23

MICROSOFT WINDOWS PATH CONVERSION WEAKNESS.

Microsoft Windows is susceptible to a path conversion weakness that may allow attackers to bypass security applications. Analysis: This issue is due to the operating system utilizing multiple differing file path resolution algorithms. This allows the exploit by attackers to bypass security software such as anti-virus and anti-spyware software. Other attacks may also be possible. Any software utilizing the affected function, or utilizing APIs and other functions that in turn utilize the affected function may be affected by this issue. Specific information regarding affected software and versions is known to be incomplete and possibly inaccurate. For a complete list of vulnerable products: http://www.securityfocus.com/bid/17934/info Solution: Currently, Security Focus is not aware of any vendor-supplied patches for this issue.

24.3 UNIX flavors

Category 24.3 *UNIX flavors*

1999-02-20 **denial of service saturation operating system table UNIX**

RISKS 20 22

Simson Garfinkel, co-author with Gene Spafford of the classic text _Practical UNIX and Internet Security_, posted a serious warning of an unsolved vulnerability of UNIX (and other) operating systems: saturation of the process table. By launching a large number of TCP/IP connections on a target machine, an attacker can fill up the process table and thereby prevent the creation of any other processes while the table is saturated.

Category 24.3 *UNIX flavors*

2000-01-17 **operating system security**

Federal Computer Week http://www.fcw.com/fcw/articles/web-nsalinux-01-17-00.as

In January, the NSA authorized Secure Computing Corporation to develop a secure version of Linux. Contract terms stipulated robust, highly secure operations.

Category 24.3 *UNIX flavors*

2002-01-20 **vulnerability flaw quality assurance QA penetration weakness operating system OS UNIX TCP/IP malformed packet patches**

Security Wire Digest 4 5

CERT ISSUES NEW WARNING FOR OLD FLAW
Attackers are now actively exploiting a 2-month-old CDE vulnerability in Sun Microsystems' Solaris and other Unix OSes to break into servers on the Internet, say researchers at the Honeynet Project. According to published reports, researchers believe the vulnerability was first exploited in the wild last week. The buffer-overflow flaw, which affects Solaris, IBM's AIX, HP-UX and other Unix OSes, allows a specially crafted packet of Internet data to give an attacker full system access. Details of the vulnerability were published in a November CERT advisory. Security experts recommend administrators install corresponding patches, and limit or disable access to the vulnerable service.

http://www.cert.org/advisories/CA-2002-01.html
http://www.cert.org/advisories/CA-2001-31.html

Category 24.3 *UNIX flavors*

2002-05-05 **operating systems command interpreters standards assumptions differences dialects user interface UNIX LINUX GNU**

RISKS 22 05ff

Theo Markettos provided an interesting warning about assuming anything about command structures in different dialects of UNIX:

***

Both Linux and HPUX provide a 'killall' command. Under Linux 'killall <process name>' is used to kill all processes with the given name -- for example, as root one might kill all instantiations of httpd.

Under HPUX, killall kills _every_ process, except those required for shutdown. It takes an optional signal argument, but ignores this if it doesn't recognise it as a valid signal name. Hence 'killall httpd' kills everything except a handful of processes required for shutdown. If not running as root, it kills all processes owned by the current user.

The RISK? Don't assume something that is safe on one OS is on another, and don't assume that running a command without arguments to get help will do the right thing.

***

Markettos' short comment provoked a flurry of rants and counter-rants in subsequent issues of RISKS; one quibble was that Linux is not UNIX (Richard Stallman once suggested it be spelled "LiGNUx"). Another comment I liked was that a well-designed command interpreter should question the presence of parameters following a command when it doesn't expect them, just as it would question the absence of required parameters.

Category 24.3 *UNIX flavors*

2002-08-16 **open-source Linux Windows activists legislation government**

NewsScan

OPEN-SOURCE ACTIVISTS SAY: GIVE US LIBERTY FROM MICROSOFT
A group of just 30 of the 15,000 Linux World conference attendees in San Francisco staged a rally outside City Hall to urge politicians to adopt the Digital Software Security Act, which would require California state agencies to use open-source software such as Linux as an alternative to Microsoft Windows. A leader of the group proclaimed, "Government and monopolists want to take away our right to write software and use computers as we want to use them. Open source is the true spirit of democracy, and we must preserve it." The Computing Technology Industry Association, a Washington, D.C.-based industry trade group, charged that the proposed Digital Software Security Act -- which is supported by an array of hackers, civil libertarians, and critics of Microsoft -- would stifle innovation in corporate America and have unintended adverse consequences. (AP/New York Times 15 Aug 2002)

Category 24.3 *UNIX flavors*

2002-09-16 **LINUX operating system corporate applications acceptance**

NewsScan

LINUX IN THE CORPORATE WORLD
The Linux operating system, which has already found a secure place in academic and government computing environments, is becoming increasingly attractive to corporate information technology managers seeking less-costly alternatives to the offerings of Microsoft and Sun. IBM is now expanding its foray into the corporate Linux world, by announcing a multi-year alliance with Red Hat, the largest company in the marketplace that sells professional support for Linux, an "open-source" product available free (without support). Alliances such as these will ease the fears of corporate IT managers concerned about the compatibility issues of unsupported software. (New York Times 16 Sep 2002)

Category 24.3 *UNIX flavors*

2002-09-17 **LINUX operating system applications acceptance office software universities digital divide international**

NewsScan

SUN OFFERS SCHOOLS STAROFFICE SOFTWARE FOR FREE
Sun Microsystems took aim at Microsoft's dominant position as a supplier of office software for schools and is sponsoring a giveaway of its rival StarOffice product to ministries of education in Europe and South Africa. Sun hopes its donation, estimated to be worth $650 million, will put StarOffice into schools serving some 26 million elementary, secondary and college students in those areas. The donation comes as something of a departure for Sun, which up until now has focused more on supplying relatively obscure software development tools to universities. The company's goal, says CEO Scott McNealy, is to destabilize Microsoft Office's dominance on the PC desktop and to erode billions of dollars of profit earned from sales of the software. The prevalence of Office in schools means that by the time children graduate, "they're going to be kind of hooked for life," says McNealy, who noted his initiative would also free up funding for other instructional expenses and student/teacher ratio reductions. (Wall Street Journal 17 Sep 2002)

Category 24.3 *UNIX flavors*

2002-09-18 **LINUX operating system applications acceptance management**

NewsScan

SUN TO PLAY LINUX CARD AGAINST MICROSOFT
Sun's strategy for competing against Microsoft has begun to revolve around the Linux operating system and the "open source" software movement, in which programmers around the world are given access to computer code and invited to suggest improvements. Sun executive Jonathan Schwartz thinks Microsoft is vulnerable because of the perceived security issues with some of its products and because Sun has a cost-advantage against Microsoft in providing service to corporate call centers that handle customer service, retail banking, and other such applications. Schwartz claims, "We can support 2,000 users with one system administrator at Sun. It requires in the neighborhood of one administrator for every 50 users in the Windows world." (New York Times 17 Sep 2002

SUN'S LOW-PRICED LINUX SYSTEMS FOR CORPORATE USE
In its continuing battle against Microsoft for the PC desktop marketplace, Sun soon will be offering inexpensive Linux-based machines targeted for call centers other corporate environments that require a limited set of features. A statement from Sun says, "The primary motivator for enterprise customers will be reduction in costs and freedom from Microsoft." The systems (called the "Mad Hatter" at Sun) will cost about $1,000, including monitor, and will be sold in lots of 100 along with a computer server and a services fee. (Reuters/San Jose Mercury News 18 Sep 2002)

Category 24.3 *UNIX flavors*

2002-11-18 **Linux Windows personal computers PCs consumer sales**

NewsScan

WAL-MART SELLS WINDOW-LESS COMPUTERS
Wal-Mart's online shopping site has started selling inexpensive computers, priced in the $299 to $599 range, that feature the Linux-based LindowsOS operating system. Lindows' Web site says "LindowsOS computers come with software to view, print and copy MS Word files, MS PowerPoint files and MS Excel files," but they lack the software necessary to run those programs. Instead, the LindowsOS computers support alternatives such as the free OpenOffice software suite. Wal-Mart said its move comes in response to customers asking for machines loaded with Linux, but it has no plans to sell them in its stores. (AP 16 Jul 2002)
http://apnews.excite.com/article/20020716/D7KQADA80.htm

LINUX, IN DAVID VS. GOLIATH BATTLES, CONTINUES TO MAKE HEADWAY
Little Linux, the home-grown, fast-growing, open-source operating system that invites code-enhancements from programmers all over the world, continues to make headway in the so-called real world: Wall Street, Hollywood, and government. Industry analyst Bill Claybrook of the Aberdeen Group says the operating systems wars will come down to two players, with Sun's Unix offering eventually falling in battle: "The real horse race, long-term, is going to be between Linux and Windows." [Yes, we've mixed some metaphors here. Be quiet.] Microsoft, unsurprisingly, thinks that victory is theirs, but Linux supporters believe that the bigger they are the harder they'll fall. Surprisingly, money may be the ultimate deciding factor, and one information services executive who just opted for Linux in his company explains: "We wanted to run it on Linux because it was quick and easy to launch. Plus, it was a fraction of the cost of a Microsoft license." (USA Today 5 Aug 2002)

SUN'S NEW LINUX STRAGEGY
Sun Microsystems is introducing its first line of computers using the Linux operating system, created and distributed as "open source code" by the Finnish programmer Linus Torvalds, and then further developed by volunteer programmers throughout the world. The pricing of Sun's LX50 server will begin at $2,795, making it very competitive with Dell's system running the red Hat version of Linux and costing about $3,700 for a similarly configured system. Sun seems to be shifting away from its "thin client" strategy, which uses inexpensive terminals that rely on powerful centralized computing, and instead embracing the Linux operating sytems and its low-cost StarOffice software suite for word processing, spreadsheet, and other business applications. Sun is hoping to persuade large corporations to abandon Microsoft software applications: "Our target is the telephone-call center that wants to put software on 10,000 desktops," says Sun executive Jonathan Schwartz. (New York Times 12 Aug 2002)

THE LINUX ASSAULT ON MICROSOFT
Although Linux has proven quite successful in the server market, it has had trouble penetrating the desktop market because Microsoft's Windows software comes bundled with most new PCs. The new hope of Linux enthusiasts is that the release of LindowsOS 2.0 as a $129 standalone product will create new momentum in the war against Microsoft domination. The new Lindows product will support dozens of Linux applications (including ones that mimic Windows applications), will include Sun's StarOffice 6.0 word processing software, and will support more than 800 printers. The software will also be available on an inexpensive tablet computer scheduled for release in early 2003. (ZDNet 18 Nov 2002)

Category 24.3 *UNIX flavors*

2002-12-19 **Linux consumer electronics**

NewsScan

SONY, MATSUSHITA TO DEVELOP LINUX SYSTEM
Sony and Matsushita Electric are teaming up to develop an operating system based on Linux technology that will be incorporated into their digital consumer electronic products, such as televisions, DVDs and microwave ovens. The decision is likely to increase competitive pressure on Microsoft. Computer heavyweight IBM and several other high-tech companies have also embraced open-source software, particularly Linux, in their offerings. Matsushita and Sony say they are considering expanding the use of their jointly developed OS with other interested electronics companies, including Hitachi, IBM, NEC, Philips, Samsung and Sharp. The source code will also be made available free to the public to encourage its broader use throughout industry. (AP 18 Dec 2002)
http://apnews.excite.com/article/20021218/D7O09AEG2.htm

Category 24.3 *UNIX flavors*

2003-01-08 **Linux consumer appliances cellular mobile telephones**

NewsScan

LINUX IN CELL PHONES
The Linux operating system, which is being used in an increasing variety of devices (including handhelds, digital video recorders, and wristwatches) will soon be used in cell phones, vying for market share with operating systems from PalmSource, Microsoft, and Symbian. The NEC corporation is working on the development of Linux-based cell phones with MontaVista Software, and is in talks with other cell phone makers to begin similar projects focused on the global and Japanese markets. NEC executive Scott Hedrick says, "One of our customers wants to move its entire product line to MontaVista Linux." (PC World 8 Jan 2002)
http://www.pcworld.com/news/article/0,aid,108556,00.asp

Category 24.3 *UNIX flavors*

2003-01-10 **Linux home computers appliances consumer electronics**

NewsScan

SONY EXEC: WINDOWS FOR THE OFFICE, LINUX FOR THE HOME
Sony president and chief operating officer Kunitake Ando told an audience at the Consumer Electronics Show in Las Vegas that, although his company has a working partnership with Microsoft, Sony sees the Linux operating system, rather than Microsoft's Windows, as the standard for transferring digital entertainment from device to device in the home. He predicted that the TV set will be reborn as an "always on, interactive device" that will serve as a broadband networking hub for high-speed communications between all electronic systems in the home, from a large-screen digital screen to a handheld device. Sony's plan for doing that features a TV set-top box called Cocoon that is Linux-based, Internet-connected, and complemented by a hard-disk drive. (San Jose Mercury News 9 Jan 2003)

Category 24.3 *UNIX flavors*

2003-01-16 **Linux operating system data centers corporations study prediction open source**

NewsScan

LINUX: THE RISE OF THE PENGUIN
Linux will emerge as the dominant operating system in corporate data centers, according to a new study by Goldman Sachs, which says the ascendance of the open source software will enable IT managers to take advantage of lower-cost, higher-performance Intel-based servers, and to avoid "premium-priced proprietary systems." The report, titled "Fear the Penguin," predicts that eventually, Linux-based systems will displace those running on Unix and RISC processors: "Many observers confine Linux's enterprise opportunity to the market for low-end 'edge' servers such as file, print, Web and e-mail servers. But we are confident that the technical developments and market forces are in place for it also to become the dominant OS on the higher-end servers of the enterprise data center." The winners in this scenario will be "independent PC semiconductor companies (Intel and AMD) and Intel-based server businesses (Dell)." The emergence of Linux is also expected to buoy the fortunes of "open" infrastructure software vendors, such as BEA Systems, BMC Software, Oracle and Veritas. However, with regard to archrival Microsoft, Linux will "hamper the movement of Windows into the enterprise data center, an area that Microsoft has only recently begun to target for growth," by providing an easier migration path from current Unix-based systems. "This shift will limit Windows' market opportunity in the data center for both its OS and its applications that run on that platform," concludes the study. (NewsFactor Network 15 Jan 2003)
http://www.newsfactor.com/perl/story/20471.html

Category 24.3 *UNIX flavors*

2003-01-21 **Linux operating system sales**

NewsScan

LINUX ACCOUNTS FOR $2 BILLION OF HP's SALES
Carly Fiorina, the chief executive of Hewlett-Packard, the world's top seller of personal computers, says that the Linux operating system now accounts for fully $2 billion of HP sales. That $2 billion figure contrasts with virtually no sales at all a mere five years ago. Of course, the increasing importance of Linux goes beyond HP, and market research groups such as IDC say that Linux installations grew 35% last year, in spite of the fact that corporate information technology budgets were in most cases flat or declining. (Reuters/San Jose Mercury News 21 Jan 2003)

Category 24.3 *UNIX flavors*

2003-02-05 **Linux training certification network administration universities colleges**

NewsScan

LINUX CERTIFICATION VS. WINDOWS CERTIFICATION
Red Hat, which sells Linux software, has developed a training course that academic institutions can use to teach Linux and certify their graduates as skilled Linux technicians. Red Hat says that "the costs and legal burden of proprietary [read: Microsoft] software are becoming unsupportable," and so believes that their courses will be very competitive against Microsoft's MSCE training program. The Red Hat instructional program will allow students to gain certified experience in subjects such as system administration, network engineering, C or C++ programming, databases, Web development, PC repair, and forensic computing. (The Inquirer 4 Feb 2003)
http://www.theinquirer.net/?article=7600

Category 24.3 *UNIX flavors*

2003-03-19 **Linux vulnerability open source Samba file server**

NIPC/DHS

March 17, CNET News.com — Linux firms urge users to plug Samba hole.

The open-source community is urging customers to patch their systems to close a hole in a software component that allows Windows programs to store and retrieve files on Linux and Unix servers. Known as Samba, the software can be found on many workstations and servers running any one of the variety of flavors of Linux and Unix, including systems running Apple OS X. The flaw occurs in the code that reassembles data that the software receives from the Internet, according to the advisory. By sending the server a specially crafted data packet, an attacker could overload the memory used by the Samba software and cause the application to run code of the intruder's choice. Members of the Samba team planned to announce the vulnerability on Tuesday, but they released information over the weekend because some believed a Web site break-in in Germany may have been attributed to the software. Several Linux editions—including Debian, Gentoo, and SuSE—released patches for the problem. Apple Computer noted in an advisory that Samba is not enabled by default with Mac OS X and Mac OS X Server, but the company plans to issue a patch for version 10.2.4. Red Hat hasn't yet released a patch but will do so soon, the company said in a statement.

Category 24.3 *UNIX flavors*

2003-04-08 **US military hacking fund open source software DARPA secure**

NIPC/DHS

April 06, The Globe and Mail (Canada) — U.S. Military funds Calgary hacker.

Theo de Raadt, a hacker from Calgary, Canada, has received a $2-million grant from the U.S. Defense Advanced Research Projects Agency (DARPA), the R&D arm of the U.S. military. For this grant, DARPA is interested in testing the security of commercial software systems against the security of open source software projects. de Raadt leads development of OpenBSD, an open-source computer operating system. OpenBSD, a derivative of the Unix operating system, is widely considered by computer experts to be the most resistant to unauthorized use. "We were convinced OpenBSD was the best platform to use as a basis for further securing open source," said Jonathan Smith, a professor of computer and information science at the University of Pennsylvania. Because DARPA does not directly fund projects outside the United States, it is Smith's computer science department that received the grant, although most of the money flows through to de Raadt's project. Although Microsoft Corp., whose Windows products are the world's dominant operating system products, and many other commercial software vendors are paying new attention to the security of their products, that renewed interest has done little to improve their products so far, de Raadt said.

Category 24.3 *UNIX flavors*

2003-04-09 **vulnerability Samba file server Windows Linux Unix patch fix FreeBSD Sun Solaris**

NIPC/DHS

April 07, CNET News.com — Samba flaw threatens Linux file servers.

The Samba Team released a patch on Monday for the second major security flaw found in the past few weeks in the open-source group's widely used program for sharing Windows files between Unix and Linux systems. The security problem could easily let an attacker compromise any Samba server connected to the Internet. The vulnerability is already being used by online attackers to compromise vulnerable servers, the company warned in an advisory. The Samba software that runs on major Linux distributions as well as FreeBSD and Sun Microsystems' Solaris operating system were affected. Security firm Digital Defense found the vulnerability. However, in an added twist to the situation that could make the threat more serious, while Digital Defense noted that some hackers obviously knew of the method by which the vulnerability could be exploited, it also mistakenly posted its own exploit onto its Web site. A patch is available on the Samba Website: http://us1.samba.org/samba/samba.html.

Category 24.3 *UNIX flavors*

2003-04-10 **Linux operating system cheap changing business operation**

NewsScan

RISE OF LINUX IS CHANGING THE LANDSCAPE
The growing appeal of Linux as an alternative to rival operating systems such as Microsoft's Windows and Sun Microsystems' Solaris is changing the dynamics of the computer software business. Although currently relegated to "back-office" operations that handle e-mail, Web pages, file-sharing and printing, Linux is primed to begin making inroads into the higher echelons of business computing, such as telecom billing and airline reservation systems. A recent Garner report says that "businesses are coming to regard Linux as a worthy alternative to Unix and Windows." That trend has proven a boon for IBM, which embraced Linux in 1999 and now offers it across its entire product range, from lowly PCs to mighty mainframes. Also benefiting are Hewlett-Packard and Dell, both of which have been successful selling Linux servers. But the blossoming of Linux could prove toxic to Sun, which has seen some of its high-end Solaris server customers migrate to inexpensive Linux-run machines. Sun has compensated by offering its own cheap boxes running Linux alongside its more powerful Solaris-based ones, but many in the industry predict the dual strategy is "doomed." (The Economist 10 Apr 2003)

Category 24.3 *UNIX flavors*

2003-06-04 **Novell Unix patent copyright operating system SCO SEC**

NewsScan

NOVELL CLAIMS UNIX PATENTS, COPYRIGHTS NEVER TRANSFERRED
Conflicting claims of Unix intellectual property ownership have come to light, with Novell saying it sold SCO Group broad rights to the Unix operating system but retained the copyrights and patents. According to a 1995 contract, Novell sold "all rights and ownership of Unix and UnixWare" to SCO's predecessor, the Santa Cruz Operation. But the asset purchase agreement filed with the SEC specifically excludes "all copyrights" and "all patents" from the purchase. "This agreement is kind of murky. You end up with a lot of questions, to put it mildly," says one intellectual property lawyer. The question of Unix patent and copyright ownership is central to SCO's attempt to force companies using Linux software to pay royalties for Unix software code that SCO says was illegally incorporated into Linux. On May 14, SCO sent letters to 1,500 of the world's largest corporations warning them that using Linux could open them up to legal liability for infringement. SCO CEO Darl McBride acknowledged last week that the contract contained "conflicting statements," but added: "It doesn't make sense. How would you transfer the product but not have the copyright attached? That would be like transferring a book but only getting the cover." Novell CEO Jack Messerman, meanwhile, said his company is basing future operating system products on Linux: "Novell is an ardent supporter of Linux and the open-source development community." (CNet News.com 4 Jun 2003)

Category 24.3 *UNIX flavors*

2003-06-17 **SCO unix IBM AIX operating system lawsuit**

NewsScan

SCO SUES IBM OVER UNIX LICENSE
The SCO Group has revoked IBM's license to use Unix. SCO is claiming in a lawsuit that IBM illegally used Unix in its AIX operating system. IBM seems unruffled by the lawsuit. Its spokesman says: "As we have said all along, our license is irrevocable, perpetual, and can not be terminated." (Reuters/USA Today 17 Jun 2003)

Category 24.3 *UNIX flavors*

2003-11-12 **attack hack Linux kernel operating system Trojan horse development code**

NIPC/DHS

November 06, CNET News.com — Attempted attack on Linux kernel foiled.

An unknown intruder attempted to insert a Trojan horse program into the code of the next version of the Linux kernel, stored at a publicly accessible database. The public database was used only to provide the latest beta, or test version, of the Linux kernel to users of the Concurrent Versions System (CVS), a program designed to manage source code. The changes, which would have introduced a security flaw to the kernel, never became a part of the Linux code and were never a threat, said Larry McVoy, founder of software company BitMover and primary architect of the source code database BitKeeper, Thursday, November 6. An intruder apparently compromised one server earlier, and the attacker used his access to make a small change to one of the source code files, McVoy said. The change created a flaw that could have elevated a person's privileges on any Linux machine that runs a kernel compiled with the modified source code. The recent incident raises questions about the security of open-source development methods, particularly how well a development team can guarantee that any changes are not introducing intentional security flaws. While Microsoft code has had similar problems, closed development is widely considered to be harder to exploit in that way.

Category 24.3 *UNIX flavors*

2003-11-24 **Debian GNU Linux attack hacker cracker open-source operating system backdoor kernel**

NIPC/DHS

November 21, eWEEK — Debian Linux under attack by hackers.

An unknown cracker compromised several machines belonging to the Debian Project, including servers that house the project's bug-tracking system and security components. Officials from the project said last week they are working to restore all of the affected machines. Debian is an open-source operating system that uses the Linux kernel and also includes a number of packages and tools from the GNU Project. This is the second such attack against an open-source project in recent weeks. Someone tried to insert a backdoor into the Linux kernel two weeks ago.

Category 24.3 *UNIX flavors*

2003-12-03 **Linux security new critical vulnerability kernel operating system**

NIPC/DHS

December 01, eWEEK — Researchers find serious vulnerability in Linux kernel.

Security professionals took note of a critical new vulnerability in the Linux kernel that could enable an attacker to gain root access to a vulnerable machine and take complete control of it. An unknown hacker recently used this weakness to compromise several of the Debian Project's servers, which led to the discovery of the new vulnerability. This discovery has broad implications for the Linux community. Because the flaw is in the Linux kernel itself, the problem affects virtually every distribution of the operating system and several vendors have confirmed that their products are vulnerable. The vulnerability is in all releases of the kernel from Version 2.4.0 through 2.5.69, but has been fixed in Releases 2.4.23-pre7 and 2.6.0-test6. RedHat Inc. and the Debian Project have both released advisories warning customers of the issue and providing information on fixes. Products from other vendors, including, MandrakeSoft S.A., SuSE Linux AG and Caldera International Inc., are also vulnerable.

Category 24.3 *UNIX flavors*

2003-12-08 **vulnerability fix flaw patch Gentoo operating system Linux**

NIPC/DHS

December 05, ZDNet UK — Patch fixes flaw behind Gentoo attack.

The team responsible for Rsync, an open-source file-transfer program, has released a fix for a security flaw used in the recent compromise of a Gentoo Linux project server. The attacker used a flaw in Rsync along with a recently-announced bug in the Linux kernel to penetrate the security of the Gentoo machine, which was subsequently taken offline for analysis. The attack and compromise of Gentoo's server came after several machines belonging to the Debian Linux project were breached by attackers last month. Gentoo and Debian are both distributions of the open-source operating system based on the Linux kernel. The flaw in Rsync versions 2.5.6 and earlier cannot be used on its own to remotely gain administrator, or root, access to a Rsync server, but could be used with the kernel flaw for a full remote compromise—as was apparently the case with Gentoo's Rsync server. The exploit does not work unless Rsync is being used as a server. Users are recommended to immediately upgrade to Rsync version 2.5.7, a version of the Linux kernel later than 2.4.23, and turn off the "use chroot = no" option in Rsync. Additional information available here:
http://rsync.samba.org/

Category 24.3 *UNIX flavors*

2004-01-07 **Linux security flaw critical vulnerability warning virtual memory**

NIPC/DHS; http://www.pcworld.com/resource/printable/article/0,aid,114088,00.asp

January 05, PC World — Security group warns of Linux flaw.

There is a critical vulnerability in the code used to manage virtual memory on Linux systems. The vulnerability affects versions of the Linux kernel up to and including version 2.6 and would give low-level Linux users total control over a Linux system. ISEC Security Research said Monday, January 5, that the problem is in kernel code for a component called "mremap," the core of the Linux operating system that provides basic services for all other parts of the operating system such as allocating processor time for the programs running on the computer and managing the system's memory or storage. Attackers could use the vulnerability to create an invalid virtual memory area, which could destabilize the Linux operating system or allow a malicious user to run attack code on the system. Attackers would need local user access to the vulnerable machine, but would not need any special privileges on the Linux system to exploit the hole, ISEC said. ISEC said they have developed test code to exploit the mremap vulnerability. Users should fix vulnerable systems as soon as software patches became available from their vendor. The original advisory is available here:
http://isec.pl/vulnerabilities04.html

Category 24.3 *UNIX flavors*

2004-01-20 **HP Tru64 UNIX operating system vulnerability flaw patch fix**

NIPC/DHS;
http://news.zdnet.co.uk/software/linuxunix/0,39020390,39119149,00.htm

January 16, ZDNet — HP patches critical security holes in Tru64 Unix.

Critical security vulnerabilities in HP's Tru64 Unix operating system were patched on Friday, January 16, after it was discovered that implementations of IPsec and SSH programs, which carry VPN and secure system command traffic, were vulnerable to attackers. The vulnerabilities both were found in vital components of the operating system and both could enable malicious users to either take control of a machine or launch a denial of service attack. SSH, a secure Telnet program, is used to securely send commands to a server, while IPSec is used to create virtual private networks to carry encrypted information over the Internet between two computers. HP has issued patches that will fix any known problems. Only HP's Tru64 UNIX 5.1B is affected and fixes for both the IPsec software and SSH software can be found on HP's Web site:
http://us-support3.external.hp.com/common/bin/doc.pl/sid=485 45bf71719ae72bf

---

Category 24.3 *UNIX flavors*

2004-01-20 **HP Tru64 UNIX operating system vulnerability flaw patch fix**

DHS IAIP Daily; http://news.zdnet.co.uk/software/linuxunix/0,39020390,39119149,00.htm

January 16, ZDNet — HP patches critical security holes in Tru64 Unix.

Critical security vulnerabilities in HP's Tru64 Unix operating system were patched on Friday, January 16, after it was discovered that implementations of Ipsec and SSH programs, which carry VPN and secure system command traffic, were vulnerable to attackers. The vulnerabilities both were found in vital components of the operating system and both could enable malicious users to either take control of a machine or launch a denial of service attack. SSH, a secure Telnet program, is used to securely send commands to a server, while IPSec is used to create virtual private networks to carry encrypted information over the Internet between two computers. HP has issued patches that will fix any known problems. Only HP's Tru64 UNIX 5.1B is affected and fixes for both the Ipsec software and SSH software can be found on HP's Web site: http://us-support3.external.hp.com/common/bin/doc.pl/sid=485 45bf71719ae72bf

---

Category 24.3 *UNIX flavors*

2004-01-22 **Linux security certified IBM Novell SuSE**

NewsScan

CERTIFICATION GIVE A BOOST TO LINUX IN GOV'T CONTRACTS

IBM and Novell's SuSE Linux have won a security certification for their combined systems, an achievement indicating that their products have been tested against strict standards — including security capabilities. IBM executive James Sterlings says, "This further underscores government confidence in Linux." (VNUnet News 22 Jan 2004)

Category 24.3 *UNIX flavors*

2004-01-23 **OSAIA Linux security threat SCO**

NewsBits;
http://www.computerweekly.com/articles/article.asp?liArticleID=127789

Linux threatens US security, SCO tells Congress

The SCO Group has confirmed that it sent a letter to all 535 members of the US Congress which claimed that Linux and open-source software is a threat to the security and economy of the US. The letter, dated 8 January, was published on the internet this week by an open-source lobbying organisation called the Open Source and Industry Alliance (OSAIA). The letter states that the commoditising influence of open-source software such as Linux is bad for the US economy and argues that open source also skirts export controls governing commercial products.

Category 24.3 *UNIX flavors*

2004-02-18 **Sun Cobalt server security holes vulnerability update issued**

DHS IAIP Daily;
http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci950995,00.html?track=NL−358

February 18, SearchSecurity.com — Sun combats security holes in cancelled Cobalt line.

Sun Microsystems continues to battle operating system vulnerabilities in its doomed line of Cobalt appliance servers. Administrators should upgrade to prevent remote exploits that could include cracking private keys, exposing confidential data, spoofing identities, escalating privileges, executing arbitrary code and denial of service. Perhaps the most serious vulnerability is a heap-based buffer overflow in rsync. Remote attackers can use this to gain access to a system or execute arbitrary code. Sun has fixes for RaQ 550, Qube 3 and RaQ 4. A defect in gnupg incorrectly creates El Gamal sign and encrypt keys using the same key component. This could allow an attacker to get the private key from a signature, which could be used to spoof identities and decrypt confidential data. Fixes are available for Qube 3, RaQ 550 and RaQ XTR. An integer overflow in the ls program in the fileutils or coreutils packages can render applications that use ls, including wu-ftpd, vulnerable to remote exploitation. Attackers could cause a denial of service on the server. There are fixes for RaQ XTR, RaQ 550, Qube 3 and RaQ 4. Finally, an update is available for an unspecified vulnerability in IPtables on RaQ 550.

Category 24.3 *UNIX flavors*

2004-02-19 **Linux kernel 2.4 server flaws vulnerabilities update issued**

DHS IAIP Daily; http://news.com.com/2100−1002_3−5162055.html?tag=nefd_top

February 19, CNET News.com — Linux servers at risk from trifecta of flaws.

Three separate security flaws could be used by an ordinary user to gain total control of a Linux server or workstation, security researchers have warned. Two of the vulnerabilities lie in the way the Linux kernel--the core of the open-source operating system--manages memory. They affect all current versions of Linux, according to advisories released on Wednesday by iSEC Security Research, a Polish security company. The third flaw affects the module for the kernel that supports ATI Technologies' Rage 128-bit video card. Because Linux is frequently used on shared servers, security holes that allow a user to expand their access rights on a computer are serious, said Alfred Huger of Symantec. However, they are not as critical as flaws that allow an outsider to compromise the computer, he said. The Linux Kernel Project released a new version of the 2.4 series kernel--version 2.4.25--to fix the vulnerability. Linux companies and projects that package their own version of Linux have rushed to deliver updates. Red Hat, Novell's SuSE Linux, Debian and other Linux distributions had released fixes by Thursday, February 19.

Category 24.3 *UNIX flavors*

2004-03-10 **security vulnerability flaw hole patch fix Linux privilege escalation denial-of-service Gentoo**

NIPC/DHS

March 09, eSecurity Planet — Linux privilege escalation hole detected.

According to an advisory from computer security consultants iSEC Security Research, a flaw was found in the Linux kernel memory management code and is completely unrelated to a similar vulnerability reported in February. The flaw carries a "critical" rating and affects Linux versions 2.2 up to and including 2.2.25; it also impacts versions 2.4 up to and including 2.4.24 as well as versions 2.6 up to and including 2.6.2. "Proper exploitation of this vulnerability leads to local privilege escalation giving an attacker full super-user privileges. The vulnerability may also lead to a denial-of-service attack on the available system memory," iSEC warned. Linux distributor Gentoo confirmed its implementation of the open source operating system was susceptible to the flaw and strongly urged uses to upgrade to newer, more secure versions. The flaw was discovered in the memory subsystem which allows for shrinking, growing, and moving of chunks of memory along any of the allocated memory areas which the kernel possesses. iSEC Security Research found that the code doesn't check the return value of the memory function.

Category 24.3 *UNIX flavors*

2004-04-16 **Linux open-source operating system kernel flaws**

DHS IAIP Daily; http://www.esecurityplanet.com/trends/article.php/3341341

April 16, eSecurity Planet — Multiple Linux flaws reported.

Security researchers are warning of a buffer overflow security flaw in the Linux kernel that can be exploited to lead to privilege escalation attacks. According to an advisory issued by iDEFENSE, the vulnerabilities affect Linux Kernel 2.6.x; Linux Kernel 2.5.x and Linux Kernel 2.4.x. The company found that affected versions of Linux kernel performed no length checking on symbolic links stored on an ISO9660 file system, a problem that allows a malformed CD to perform an arbitrary length overflow in kernel memory. "Symbolic links on ISO9660 file systems are supported by the 'Rock Ridge' extension to the standard format. The vulnerability can be triggered by performing a directory listing on a maliciously constructed ISO file system, or attempting to access a file via a malformed symlink on such a file system. Many distributions allow local users to mount CDs, which makes them potentially vulnerable to local elevation attacks," according to the security alert. Updated Linux kernel versions are available at kernel.org. Separately, security firm Secunia warned of an information leak and denial-of-service holes in Linux Kernel 2.4.x and 2.6.x. The information leak problem was discovered with the ext3, XFS, and JFS file system code and can lead to the exposure of data like cryptographic keys to malicious attackers. Another error was found within the OSS code for SoundBlaster 16 devices that could be used to trigger denial-of-service attacks with odd numbers of output bytes are submitted.

Category 24.3 *UNIX flavors*

2004-05-03 **Linux operating systems vulnerabilities security**

DHS IAIP Daily; http://www.fcw.com/fcw/articles/2004/0503/feat-linux3-05-03-04.asp

May 03, Federal Computer Week — Linux has its own security holes.

There may be fewer viruses designed to attack the Linux operating system, but experts warn that Linux is no more bulletproof than any other system. Agencies that adopt Linux should be aware of its vulnerabilities, according to Travis Witteveen, of security firm F-Secure Corp. "Computing systems are very similar, whether they're called Linux, Windows, Unix, MacIntosh, or even PocketPC," he said. Vius writers will target Linux when the system gains a high enough profile, Witteveen said. But even now, there are some Linux viruses out in cyberspace. The most damaging Linux virus so far, the Slapper worm, infected 20,000 systems in 100 countries in late 2002, said Laura DiDio, senior analyst of application infrastructure and software platforms for the Yankee Group. "That pales in comparison to the most damaging Windows virus, MyDoom and its variants, which infected several million computers in three weeks," she said. Linux is "on everyone's radar screen," and creators of malicious code are increasingly taking notice, she said. Many Linux viruses don't require user interaction, unlike most Windows attacks that depend on the user to run an attached file in order to infect the computer.

Category 24.3 *UNIX flavors*

2004-06-28 **Project Looking Glass Sun Microsystems 3-D interface software**

NewsScan

SUN 3-D INTERFACE OFFERED TO OPEN-SOURCE COMMUNITY

Sun Microsystems has designed 3-D interface software to compete with the PC desktop metaphor of desktops and file folders. The new technology will be offered to the open source community, and a Sun executive says, "What we want to do is leverage the community of open-source developers to do things we might not have thought of." Produced through a company effort dubbed Project Looking Glass, the 3D interface allows windows containing documents or images to be turned sideways (like books on a shelf) and spun around so that notations can be made on the reverse side. It may eventually be used on Windows machines, but Sun is initially planning to use the
technology on desktop machines running Linux or Sun's own Solaris operating system. Sun president and COO Jonathan Schwartz says that Project Looking Glass reflects a swing in software development back toward desktop machines or other client devices, instead of running programs on centralized servers. (Wall Street Journal 28 Jun 2004)

Category 24.3 *UNIX flavors*

2004-07-29 **Gentoo Linux Samba vulnerability fix patch update SWAT buffer overflow**

DHS IAIP Daily; http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci996615,00.html

July 29, SearchSecurity.com — Gentoo fixes Samba vulnerabilities.

Gentoo Linux has fixed buffer overflow vulnerabilities in Samba. The buffer overflow found in SWAT is located in the base64 data decoder used to handle http basic authentication. The same flaw is present in the code used to handle the sambaMungedDial attribute value when using the ldapsam passdb backend. Another buffer overflow was found in the code used to support the 'mangling method = hash' smb.conf option. The SWAT authentication overflow could be exploited to execute arbitrary code with the rights of the Samba daemon process. The overflow in the sambaMungedDial handling code is not thought to be exploitable. The buffer overflow in 'mangling method = hash' code could also be used to execute arbitrary code on vulnerable configurations. For a workaround, the Gentoo advisory suggests users disable SWAT, not use ldapsam passdb backends and avoid the 'mangling method = hash' option. All Samba users should upgrade to the latest version, Gentoo said: http://www.gentoo.org/security/en/glsa/glsa-200407-21.xml

---

Category 24.3 *UNIX flavors*

2004-07-30 **Oracle database privilege escalation vulnerability UNIX Linux**

DHS IAIP Daily; http://www.securityfocus.com/bid/10829

July 30, SecurityFocus — Oracle database default library directory privilege escalation vulnerability.
Oracle database implementations are reportedly prone to a default library directory privilege escalation vulnerability. This issue arises due to a default configuration error that will permit the attacker to replace libraries required by setuid root applications with arbitrary code. This issue would allow an Oracle software owner to execute code as the superuser, taking control of the entire system. It should be noted that this vulnerability only affects Oracle on UNIX/Linux platforms. SecurityFocus is currently not aware of any vendor-supplied patches for this issue.

Category 24.3 *UNIX flavors*

2004-08-03 **Citadel UX buffer overflow vulnerability denial of service DoS**

DHS IAIP Daily; http://secunia.com/advisories/12197/

August 03, Secunia — Citadel/UX "USER" Command Buffer Overflow Vulnerability.

A vulnerability in Citadel/UX can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a vulnerable system. The vulnerability is caused due to boundary error within the citadel service when processing "USER" commands. This can be exploited to cause a stack-based buffer overflow by passing an overly long argument (about 94 bytes) to the "USER" command. Successful exploitation may allow execution of arbitrary code. The vulnerability has been reported in version 6.23 and prior.

Category 24.3 *UNIX flavors*

2004-08-04 **YaST2 SuSE Linux shell code injection vulnerability update patch**

DHS IAIP Daily; http://www.securityfocus.com/bid/10867/info/

August 04, SecurityFocus — YaST2 utility library file verification shell code injection vulnerability.

YaST2 utility library 'liby2util' is affected by a file verification shell code injection vulnerability. This issue is due to a design error that fails to properly validate files. An attacker could leverage this issue to inject malicious shell code into a file name being transferred using the vulnerable utility. This might facilitate privilege escalation and unauthorized access. S.u.S.E. has made updated binaries available on their FTP sites.

Category 24.3 *UNIX flavors*

2004-08-04 **Linux vulnerability pointer handling kernel memory disclosure**

DHS IAIP Daily; http://secunia.com/advisories/12210/

August 04, Secunia — Linux kernel file offset pointer handling memory disclosure vulnerability.

A vulnerability in the Linux kernel can be exploited by malicious, local users to disclose sensitive information in kernel memory. The vulnerability is caused due to race conditions and conversion errors when handling 64-bit file offset pointers. Successful exploitation may disclose large portions of kernel memory. The vulnerability has been reported in version 2.4.26 and prior and in version 2.6.7 and prior. Users should grant only trusted users access to affected systems.

Category 24.3 *UNIX flavors*

2004-08-09 **HP Tru64 UNIX Mozilla libpng vulnerabilities**

DHS IAIP Daily; http://secunia.com/advisories/12240/

August 09, Secunia — Mozilla Application Suite for Tru64 UNIX libpng Vulnerabilities.

HP has confirmed some vulnerabilities in the Mozilla Application Suite for Tru64 UNIX, which can be exploited by malicious people to cause a DoS (Denial of Service) or compromise a vulnerable system. The vulnerabilities affect versions prior to 1.7. Users should install Mozilla Application Suite for HP Tru64 UNIX V1.7. http://h30097.www3.hp.com/internet/download.htm

---

Category 24.3 *UNIX flavors*

2004-08-11 **Sun Solaris X Display Manager XDMCP request vulnerability remote protocol**

DHS IAIP Daily; http://www.kb.cert.org/vuls/id/139504

August 11, US-CERT — Vulnerability Note VU#139504: Sun Solaris X Display Manager does not properly handle invalid XDMCP requests.

The X Display Manager (xdm(1)) is responsible for managing collections of X displays from local or remote servers using the X Display Manager Control Protocol (XDMCP). The Sun Solaris X Display Manager contains a denial-of-service vulnerability that could be triggered by an invalid XDMCP packet. A remote attacker with the ability to send XDMCP packets to a vulnerable system could cause the X Display Manager to crash. For more information on patches available for your system, please refer to Sun Security Alert 57619: http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert/5761 9

Category 24.3 *UNIX flavors*

2004-08-16 **SuSE Linux operating system rsync program vulnerability Red Hat Package Manager rpm update issued**

DHS IAIP Daily; http://www.suse.com/de/security/2004_26_rsync.html

August 16, SUSE, Inc. — SUSE Linux rsync vulnerability.

If rsync is running in daemon-mode and without a chroot environment it is possible for a remote attacker to trick rsyncd into creating an absolute pathname while sanitizing it. As a result it is possible to read/write from/to files outside the rsync directory. SUSE Linux 8.1, 8.2, 9.0, and 9.1 are vulnerable. Please download the update package for your distribution and verify its integrity by the methods listed in section three of this announcement. Then, install the package using the command "rpm -Fhv file.rpm" to apply the update. Our maintenance customers are being notified individually. The packages are being offered to install from the maintenance web.

Category 24.3 *UNIX flavors*

2004-08-25 **OpenBSD kernal panic attack ICMP request system reboot**

DHS IAIP Daily; http://www.zone−h.org/advisories/read/id=5413

August 25, zone-h.org — OpenBSD kernel panic.

A vulnerability exists in OpenBSD 3.4 and 3.5 configured to act as a gateway. This vulnerabilty may cause the kernel to crash. An OpenBSD 3.5 machine, configured as a gateway, with active bridging, and the link2 option given (for IPSec processing), is vulnerable to a crash when to a single ICMP echo request sent from a machine on interface A's network is sent to a machine on interface B's network. No core file is generated. If the DDB_PANIC option is set, the machine reboots upon receipt of the ICMP echo request. Patches are available at: ftp://ftp.openbsd.org/pub/OpenBSD/patches

---

Category 24.3 *UNIX flavors*

2004-09-02 **Linux 2.6 kernel open source operating system panic integer overflow vulnerability XDR decode functions update issued**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Sep/1011138.html

September 02, SecurityTracker — Linux Kernel integer overflow in kNFSd lets remote users panic the system.

An integer overflow vulnerability exists in the Linux kernel in kNFSd. A remote user can cause the target system to crash. SuSE reported that there are various "signedness issues and integer overflows" in the kNFSd and the XDR decode functions in the Linux 2.6 kernel. A fix is available for the kNFSd overflow in the upstream 2.6.9-rc1 kernel version.

Category 24.3 *UNIX flavors*

2004-11-10 **Linux kernel loader vulnerability root access arbitrary code execution attack**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Nov/1012165.html

November 10, SecurityTracker — Linux Kernel binfmt_elf Loader lets local users obtain root access.

A local user can execute arbitrary code with setuid privileges to obtain root access on the target system. Several flaws have been discovered in the ELF loader in the processing of set user id (setuid) binaries. There is no solution at this time.

Category 24.3 *UNIX flavors*

2004-11-19 **FreeBSD fetch utility integer overflow vulnerability**

DHS IAIP Daily; http://secunia.com/advisories/13226/

November 19, Secunia — FreeBSD fetch utility integer overflow vulnerability.

A vulnerability has been reported in FreeBSD which potentially can be exploited by malicious people to compromise a user's system. The vulnerability is caused due to an integer overflow in the fetch utility when processing HTTP headers. This can be exploited to cause a buffer overflow by returning a specially crafted response. Successful exploitation may allow execution of arbitrary code, but requires that a user is tricked into connecting to a malicious Web server. Original advisory and updates are available at: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/advisories/FreeBSD-SA-04:16.fetch.asc

---

Category 24.3 *UNIX flavors*

2004-11-30 **Linux kernel datagram serialization error user privilege escalation update issued**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Nov/1012363.html

November 30, SecurityTracker — Linux Kernel datagram serialization error may let local users gain elevated privileges.

A local user may be able to obtain elevated privileges because the kernel does not properly serialize received datagrams. A local user can exploit this flaw to modify kernel space memory and potentially obtain elevated privileges. A fix is available in 2.4.28 and via BitKeeper at: http://linux.bkbits.net:8080/linux-2.4/cset@4199284dnTPrPLR- yhP_rOBHXJlltA

Category 24.3 *UNIX flavors*

2004-12-02 **IBM AIX privilege escalation vulnerabilities code execution attack update issued**

DHS IAIP Daily; http://secunia.com/advisories/13589/

December 02, Secunia — IBM AIX multiple privilege escalation vulnerabilities.

Four vulnerabilities have been reported in AIX, which can be exploited by malicious, local users to gain escalated privileges. These vulnerabilities are due to errors in the paginit utility, the "/bin/Dctrl" utility, the uname utility, and the grep utility. Successful exploitation of the vulnerabilities allows execution of arbitrary code with "root" privileges. Apply APARs: http://www-912.ibm.com/eserver/support/fixes/fcgui.jsp

---

Category 24.3 *UNIX flavors*

2004-12-03 **AIX operating system startup script vulnerability Object Data Manager ODM update issued**

DHS IAIP Daily; http://secunia.com/advisories/13370/

December 03, Secunia — AIX unspecified system startup scripts vulnerability.

A vulnerability has been reported in AIX, which can be exploited by malicious, local users to inject arbitrary data into the ODM (Object Data Manager) or cause a vulnerable system to hang during boot. The vulnerability is caused due to an unspecified error within the system startup scripts. Apply APARs available at: http://www-912.ibm.com/eserver/support/fixes/fcgui.jsp

---

Category 24.3 *UNIX flavors*

2004-12-13 **Linux flaws Microsoft security research reliability security open-source**

NewsScan;
http://news.com.com/Security+research+suggests+Linux+has+fewer+flaws/2100
-1002_3-5489804.html

REPORT CONCLUDES LINUX HAS FEWER FLAWS

A four-year research effort by code-analysis firm Coverity has concluded that Linux has significantly fewer software bugs in it than most commercial counterparts. Coverity uncovered 985 flaws in the 5.7 million lines of code that make up the Linux core operating system, compared with the more than 5,000 defects typically found in commercial software of similar size. "Linux is a very good system in terms of bug density," says Coverity CEO Seth Hallem. Though Coverity's report doesn't contain any specific data about the frequency of glitches in Microsoft's Windows operating system, it's likely to add fuel to the debate over which system -- Linux, Mac OS or Windows -- is most secure. One recent report found that Red Hat Linux contained fewer critical flaws than Microsoft Windows, while a Forrester Research study (sponsored by Microsoft) unsurprisingly favored Microsoft. (CNet News.com 13 Dec 2004)

Category 24.3 *UNIX flavors*

2004-12-21 **Hewlett-Packard HP UX ftpd file transfer protocol daemon buffer overflow vulnerability update issued**

DHS IAIP Daily;
http://www.idefense.com/application/poi/display?id=175&type= vulnerabilities

December 21, iDEFENSE — Hewlett Packard HP-UX ftpd remote buffer overflow vulnerability.

Remote exploitation of a buffer overflow vulnerability in the file transfer protocol (FTP) daemon included in multiple versions of Hewlett-Packard Development Co.'s (HP) HP-UX allows attackers to gain remote root access in certain configurations. The severity of this issue is mitigated by the fact that in most production environments, administrators will not be using the debug-logging feature of FTP daemon. Apply patches: http://www.itrc.hp.com/service/patch/mainPage.do

---

Category 24.3 *UNIX flavors*

2004-12-26 **SHOUTcast software filename format string vulnerability DNAS Linux HTTP request no update issued**

DHS IAIP Daily; http://secunia.com/advisories/13661/

December 26, Secunia — SHOUTcast filename format string vulnerability.

A vulnerability in SHOUTcast DNAS/Linux version 1.9.4 has been reported which can be exploited by malicious people to compromise a vulnerable system. The vulnerability is caused due to a format string error in the URL handling within the processing of requested filenames. This can be exploited to execute arbitrary code by sending a specially crafted HTTP request containing format specifiers. No vender solution is available at this time.

Category 24.3 *UNIX flavors*

2005-01-11 **Linux kernel multiple vulnerabilities exploit information disclosure privilege escalation**

DHS IAIP Daily; http://secunia.com/advisories/13784/

LINUX KERNEL MULTIPLE VULNERABILITIES

Multiple vulnerabilities have been reported in the Linux kernel, which potentially can be exploited by malicious, local users to cause a denial of service, disclose sensitive information, or gain escalated privileges on a vulnerable system. The solution is to grant only trusted users access to affected systems.

Category 24.3 *UNIX flavors*

2005-01-11 **Sun Alert user account creation Solaris operating system quality assurance failure**

DHS IAIP Daily; http://sunsolve.sun.com/search/document.do?assetkey=1−26−577 17−1

SMC DEFAULT CONFIGURATION GUI CREATES USER ACCOUNTS WITH BLANK PASSWORD INSTEAD OF LOCKED ACCOUNT

User accounts created with the Solaris Management Console (SMC) GUI which are configured for password aging (the shadow(4) fields and fields will be set) may allow login without specifying a password. This issue can occur when a user account is created with SMC (default configuration) with aging fields set and no password supplied. The user account (when being created) is not prompted for a password. To work around the described issue, always supply a password while creating user accounts with SMC (locked by default).

Category 24.3 *UNIX flavors*

2005-01-11 **Netscape Directory Server access control stack buffer overflow vulnerability denial of service DoS code execution attack**

DHS IAIP Daily; http://rhn.redhat.com/errata/RHSA−2005−030.html

STACK BUFFER OVERFLOW IN THE NETSCAPE DIRECTORY SERVER ACCESS CONTROL CODE.

A stack buffer overflow was found in the access control code in Netscape Directory Server 6.21 and earlier. A remote attacker who can communicate with the LDAP service could trigger this flaw by creating a carefully crafted attribute change request. A successful exploit would lead to a denial of service (crash) or potentially to remote code execution on the server. Patches in the form of updated libraries that correct this issue are available on request from the Red Hat Security Response Team. Please contact secalert@redhat.com

---

Category 24.3 *UNIX flavors*

2005-01-12 **Linux kernel multiprocessor page fault privilege escalation vulnerability no update issued**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2005/Jan/1012862.html

LINUX KERNEL MULTIPROCESSOR PAGE FAULT HANDLER RACE CONDITION LETS LOCAL USERS GAIN ELEVATED PRIVILEGES

A vulnerability was reported in the Linux kernel in the page fault handler code for multiprocessor systems. A local user can obtain root privileges. If two concurrent threads share the same virtual memory space and request stack expansion at the same time, a race condition can be exploited on multiprocessor systems. A local user can cause arbitrary memory contents to be injected into memory locations used by a set user id (setuid) application to execute arbitrary code with elevated privileges. The flaw resides in the down_read() function in 'arch/i386/mm/fault.c'. No upstream solution is currently available.

Category 24.3 *UNIX flavors*

2005-01-13 **SGI IRIX operating system design error vulnerability code execution attack no update issued**

DHS IAIP Daily; http://idefense.com/application/poi/display?id=182&type=vuln erabilities&flashstatus=true

SGI IRIX INPVIEW DESIGN ERROR VULNERABILITY.

Local exploitation of a design error vulnerability in the inpview command included in multiple versions of Silicon Graphics Inc.'s IRIX could allow for arbitrary code execution as the root user. All that is required to exploit this vulnerability is a local account and an open X display, which could be the attacker's home machine or another compromised system. Exploitation does not require any knowledge of application internals, making privilege escalation trivial, even for unskilled attackers. Support for the InPerson product did not extend beyond 02/2002 as noted in the following publication: techpubs.sgi.com/library/manuals/4000/007-4526-001/pdf/007-4526-001.pdf. As a result, no patch will be issued for this vulnerability. A workaround is available on the iDefense Website.

Category 24.3 *UNIX flavors*

2005-01-28 **HP-UX TGA daemon vulnerability denial of service DoS attack**

DHS IAIP Daily; http://www.k−otik.com/english/advisories/2005/0076

HP-UX TGA DAEMON REMOTE DENIAL OF SERVICE VULNERABILITY

A new security vulnerability has been identified in HP-UX, which may be exploited by remote attackers to conduct denial of service attacks. The problem is caused due to an an unspecified error in the TGA daemon when handling certain network traffic, which may be exploited to cause a vulnerble system to stop responding. Original advisory and solution available at: http://www5.itrc.hp.com/service/cki/docDisplay.do?admit=5522 67591+1106928673434+28353475&docId=HPSBUX01111

Category 24.3 *UNIX flavors*

2005-02-01 **AIX network information server NIS vulnerability client system compromise code execution root privilege update issued**

DHS IAIP Daily; http://secunia.com/advisories/14095/

AIX UNSPECIFIED NIS CLIENT SYSTEM COMPROMISE VULNERABILITY

A vulnerability has been reported in AIX 5.3, which can be exploited by malicious people to compromise a vulnerable system. The vulnerability is caused due to an unspecified error allowing execution of arbitrary code with root privileges. Successful exploitation requires that the system has been configured as a NIS client. Apply Efix for AIX 5.3.0:

Category 24.3 *UNIX flavors*

2005-02-03 **Sun Solaris Samba integer overflow vulnerability smbd daemon command execution attack update issued**

DHS IAIP Daily; http://sunsolve.sun.com/search/document.do?assetkey=1−26−577 30−1

SUN SOLARIS SAMBA INTEGER OVERFLOW VULNERABILITY

Sun has acknowledged a vulnerability in Solaris, which can be exploited by malicious users to compromise a vulnerable system. An integer overflow security issue with the Samba(7) smbd(1m) daemon may allow a local or remote authenticated user the ability to execute arbitrary commands with the privileges of Super User (typically root), on a Solaris 9 system running as a Samba(7) server. Solution available through Source link below.

Category 24.3 *UNIX flavors*

2005-02-10 **IBM AIX operating system vulnerability file access root privileges solution issued**

DHS IAIP Daily; http://www.idefense.com/application/poi/display?type=vulnerabilities

IBM AIX MULTIPLE VULNERABILITIES

Multiple vulnerabilities in IBM AIX can be exploited to potentially allow a malicious user to read one line of any file on the system, regardless of permissions, and in some cases, gain root access on the system. Solution available to registered users at: https://techsupport.services.ibm.com

---

Category 24.3 *UNIX flavors*

2005-02-15 **Linux kernel proc filesystem signed integer error buffer overflow vulnerability code execution privilege escalation attack update issued**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2005/Feb/1013188.html

LINUX KERNEL '/PROC' SIGNED INTEGER ERRORS LET LOCAL USERS EXECUTE ARBITRARY CODE

A vulnerability was reported in the Linux kernel in '/proc'. A local user can execute arbitrary code or view kernel memory to gain elevated privileges. A local user can trigger a buffer overflow or view kernel memory. Some flaws reside in the proc_file_read() function in 'fs/proc/generic.c', where a call to min_t() uses an incorrect integer definition, and in the locks_read_proc() function where an integer parameter is incorrectly defined. A local user can trigger a buffer overflow. The vendor has released a fixed version (2.6.11-rc4), available at: http://www.kernel.org/

Category 24.3 *UNIX flavors*

2005-02-15 **Sun Solaris operating system crash vulnerability ARP packet processing denial of service DoS condition update issued**

DHS IAIP Daily; http://securitytracker.com/alerts/2005/Feb/1013179.html

SUN SOLARIS CAN BE CRASHED BY A REMOTE USER SENDING A FLOOD OF ARP PACKETS

A vulnerability was reported in Sun Solaris in the processing of ARP packets. A remote user can cause denial of service conditions. A remote user on a local network can send a large number of specific ARP packets to cause the target system to hang. Updates and original advisory at: http://classic.sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsal ert%2F57673

Category 24.3 *UNIX flavors*

2005-02-16 **Linux kernel multiple vulnerabilities sensitive information disclosure denial of service DoS**

DHS IAIP Daily; http://secunia.com/advisories/14295/

LINUX KERNEL MULTIPLE VULNERABILITIES.

Multiple vulnerabilities have been reported in the Linux kernel. These can be exploited by malicious, local users to gain knowledge of potentially sensitive information or cause a DoS (Denial of Service), or by malicious people to cause a DoS or bypass certain security restrictions. There is no complete solution at this time.

Category 24.3 *UNIX flavors*

2005-02-28 **Debian Linux operating system bsmtpd vulnerability command injection execution attack update issued**

DHS IAIP Daily; http://secunia.com/advisories/14412

DEBIAN BSMTPD ARBITRARY COMMAND INJECTION VULNERABILITY

A vulnerability has been reported in bsmtpd, which can be exploited by malicious people to compromise a vulnerable system. The vulnerability is caused due to lack of sanitation of email addresses. This can be exploited to execute arbitrary commands. Original Advisory and updates available: http://www.debian.org/security/2005/dsa-690

Category 24.3 *UNIX flavors*

2005-03-31 **Linux kernel deadlock error denial of service DoS condition futex function update issued**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2005/Mar/1013616.html

LINUX KERNEL DEADLOCK ERROR IN FUTEX FUNCTIONS LET LOCAL USERS DENY SERVICE.

A vulnerability was reported in the Linux kernel futex functions. A local user can cause the kernel to crash. The vulnerability resides in 'kernel/futex.c.' A development patch (and changeset) is available, as described at: http://lkml.org/lkml/2005/2/22/185

Category 24.3 *UNIX flavors*

2005-04-19 **Sun Solaris operating system local user hijack non-privileged port services**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2005/Apr/1013760.html

SUN SOLARIS MAY LET LOCAL USERS HIJACK NON-PRIVILEGED PORT SERVICES

A vulnerability was reported in Sun Solaris. A local user may be able to start a process that binds to a non-privileged network port to hijack future connections to the service that typically runs on that port. Only network services that run on non-privileged ports (e.g., NFS, NIS) are affected. Updates available: sunsolve.sun.com/search/document.do?assetkey=1-26-57766-1

Category 24.3 *UNIX flavors*

2005-04-25 **Citrix program neighborhood buffer overflow vulnerability command execution attack update issued**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/0390

CITRIX PROGRAM NEIGHBORHOOD AGENT BUFFER OVERFLOW VULNERABILITIES

Two vulnerabilities were identified in Citrix Program Neighborhood Agent, which may be exploited by remote attackers to execute arbitrary commands. Update to Citrix Program Neighborhood Agent for Win32 version 9.0 and later or Citrix MetaFrame Presentation Server client for WinCE version 8.33 and later. Updates: http://www.citrix.com/English/SS/downloads/downloads.asp?dID =2755

Category 24.3 *UNIX flavors*

2005-04-26 **Citrix neighborhood agent buffer overflow vulnerability code execution shortcut creation attack update issued**

DHS IAIP Daily;
http://www.securiteam.com/windowsntfocus/5HP0R20FFE.html

CITRIX NEIGHBORHOOD AGENT BUFFER OVERFLOW AND ARBITRARY SHORTCUT CREATION

Remote exploitation of a design error in Citrix Program Neighborhood Agent allows attackers to execute arbitrary code under the privileges of the client user and to create arbitrary shortcuts under the privileges of the client user. Exploitation requires that an attacker establish a malicious server and cause or convince the target user to connect to it via the Program Neighborhood Agent. This can be accomplished by social engineering or automatically when combined with a DNS or ARP spoofing attack. Updates available: http://www.citrix.com/English/SS/downloads/downloads.asp?dID =2755

Category 24.3 *UNIX flavors*

2005-04-26 **Sun Solaris operating system LibTIFF vulnerabilities hijack connections update issued**

DHS IAIP Daily; http://secunia.com/advisories/15113/

SUN SOLARIS MULTIPLE LIBTIFF VULNERABILITIES

Multiple vulnerabilities have been reported in LibTIFF, which potentially can be exploited by malicious people to compromise a user's system or cause a DoS (Denial of Service). A local user may be able to start a process that binds to a non-privileged network port to hijack future connections to the service that typically runs on that port. Original advisory and updates: http://sunsolve.sun.com/search/document.do?assetkey=1-26-577 69-1

Category 24.3 *UNIX flavors*

2005-05-17 **Linux kernel locally exploitable flaws no update issued**

DHS IAIP Daily; http://www.securiteam.com/unixfocus/5GP0F20FQI.html

LINUX KERNEL PKTCDVD AND RAWDEVICE IOCTL RACE CONDITION

Two locally exploitable flaws have been found in the Linux rawdevice and pktcdvd block device ioctl handler that allows local users to gain root privileges and also execute arbitrary code at kernel privilege level. The Linux kernel contains pktcdvd and rawdevice block device components. Due to the missing checks in pktcdvd and rawdevice ioctl handler parameter, the process can break user space limit and execute arbitrary code at kernel privilege level. There is no solution at this time.

Category 24.3 *UNIX flavors*

2005-06-15 **vulnerability hole remote buffer overflow ViRobot Linux server no solution**

DHS IAIP Daily; http://www.securityfocus.com/bid/13964/exploit

VIROBOT LINUX SERVER REMOTE BUFFER OVERFLOW VULNERABILITY

ViRobot Linux Server is prone to a remote buffer overflow vulnerability affecting the Web based management interface. This issue presents itself because the application fails to perform boundary checks prior to copying user supplied data into sensitive process buffers. An attacker can gain unauthorized access to a vulnerable computer by supplying malformed values through cookies. There is no solution at this time.

Category 24.3 *UNIX flavors*

2005-11-01 **vulnerability hole Linux kernel buffer overflow fixed update**

DHS IAIP Daily; http://secunia.com/advisories/17384/

LINUX KERNEL POTENTIAL BUFFER OVERFLOW VULNERABILITIES

Two vulnerabilities have been reported in the Linux Kernel. Currently they have an unknown impact. The first includes a boundary error due to missing parameter validation in the "map_to_seg7()" function in "drivers/usb/input/map_to_7segment.h" of the Yealink driver may cause out-of-bound memory references. The second vulnerability is a boundary error in "/drivers/i2c/i2c-core.c" when handling SMBus Block Write transactions may cause a buffer overflow. According to Secunia the vulnerabilities have been fixed in version 2.6.14-git4.

Category 24.3 *UNIX flavors*

2005-11-02 **vulnerability multiple NetBSD fix patch update**

DHS IAIP Daily; http://secunia.com/advisories/17389/

NETBSD UPDATE FIXES MULTIPLE VULNERABILITIES

There have been vulnerabilities reported in NetBSD. These vulnerabilities could be exploited by malicious, local users to gain escalated privileges, or by malicious users to cause a Denial of Service and compromise a vulnerable system, or by attacker's attempting to bypass security restrictions and compromise a user's system. According to Seunica, the vulnerabilities have been fixed NetBSD-current (October 31, 2005) and NetBSD-1.6 branch (November 1, 2005).

Category 24.3 *UNIX flavors*

2005-12-22 **Linux kernel socket buffer memory exhaustion denial of service vulnerability check memory resource**

DHS IAIP Daily; http://www.securityfocus.com/bid/16041/references

Linux kernel local socket buffer memory exhaustion denial of service vulnerability.

Linux kernel is susceptible to a local denial of service vulnerability. The issue is due to a failure of the kernel to properly check and enforce memory resource constraints. This is triggered by consuming excessive kernel memory by creating multiple sockets with large kernel buffers; this allows local attackers to consume excessive kernel memory, eventually leading to an out of memory condition, and a denial of service for legitimate users.

Category 24.3 *UNIX flavors*

2005-12-22 **Linux kernel remote denial of service vulnerability memory crash user address issue Ubuntu**

DHS IAIP Daily; http://www.securityfocus.com/bid/16044/references

Linux kernel ICMP_Push_Reply remote denial of service vulnerability.

Linux kernel is prone to a remote denial of service vulnerability. Remote attackers can exploit this to leak kernel memory. Successful exploitation will result in a crash of the kernel, effectively denying service to legitimate users. Solution: Linux kernel version 2.6.12.6 has been released to address this issue. Ubuntu Linux has released advisory USN-231-1, along with fixes to address various kernel issues. For further solution detail refer to: http://www.securityfocus.com/bid/16044/solution

---

Category 24.3 *UNIX flavors*

2005-12-24 **Sun Solaris PC Netlink vulnerabilities elevated privileges flaws script command files opened insecurely filesystem permission arbitrary commands solution patches**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/3083

Sun Solaris PC Netlink "slsadmin" and "slsmgr" local vulnerabilities.

Two vulnerabilities were identified in PC Netlink for Solaris, which could be exploited to obtain elevated privileges. These flaws are due to errors in the "/etc/init.d/slsadmin" script and the "/opt/lanman/sbin/slsmgr" command that allow files to be opened insecurely, which could be exploited to write to the filesystem with the permissions of the user running "slsadmin" or "slsmgr", and execute arbitrary commands with "root" privileges (when "slsadmin" or "slsmgr" are run as "root"). Affected products are PC NetLink 2.0 (for Solaris SPARC 7, 8 and 9). FrSIRT reports that a solution is available; apply patches 121332-01 and 121209-01. Solution: http://sunsolve.sun.com/search/document.do?assetkey=urn:cds: docid:1-21-121332-01-1 Solution: http://sunsolve.sun.com/search/document.do?assetkey=urn:cds: docid:1-21-121209-01-1

Category 24.3 *UNIX flavors*

2006-01-04 **denial of service privilege escalation vulnerability Linux kernel update**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2006/0035 23

LINUX KERNEL MULTIPLE DENIAL OF SERVICE AND PRIVILEGE ESCALATION ISSUES

Multiple vulnerabilities were identified in Linux Kernel, which could be exploited by malicious users to cause a denial of service and potentially obtain elevated privileges. The first issue is due to an error in "mm/mempolicy.c" when handling policy system calls, which could be exploited by local attackers to cause a denial of service via a "set_mempolicy" call with a 0 bitmask. The second flaw is due to a one-byte buffer overrun error in "kernel/sysctl.c" when processing an overly long user-supplied string, which could be exploited by local attackers to potentially execute arbitrary commands. The third vulnerability is due to an error in "net/ipv4/fib_frontend.c" when processing malformed "fib_lookup" netlink messages, which could cause illegal memory references. The fourth issue is due to a buffer overflow error in the CA-driver for TwinHan DST Frontend/Card [drivers/media/dvb/bt8xx/dst_ca.c], which could be exploited by malicious users to cause a denial of service or potentially execute arbitrary commands. Solution: Upgrade to Linux Kernel version 2.6.15: http://www.kernel.org/.

Category 24.3 UNIX flavors

2006-01-16 **Linux kernel remote denial of service DoS vulnerability upgrade**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2006/0220 23

LINUX KERNEL MULTIPLE REMOTE AND LOCAL DENIAL OF SERVICE VULNERABILITIES

Multiple vulnerabilities were identified in Linux Kernel, which could be exploited by remote or local attackers to cause a denial of service. The first issue is due to an infinite loop in the "netlink_rcv_skb" [af_netlink.c] function when handling a specially crafted "nlmsg_len" value, which could be exploited by local attackers to cause a denial of service. The second flaw is due to an error in the PPTP NAT helper that does not properly calculate the offset when handling an inbound "PPTP_IN_CALL_REQUEST" packet, which could be exploited by attackers to crash a vulnerable system. The third vulnerability is due to an error in the PPTP NAT helper that does not properly calculate the offset based on the difference between two pointers to the header, which could be exploited by attackers to cause a kernel crash. Solution: Upgrade to Linux Kernel 2.6.15.1: http://www.kernel.org/

Category 24.3 UNIX flavors

2006-01-31 **HP Tru64 UNIX BIND user privileged access DNS BIND**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2006/Jan/1015551.html 23

HP TRU64 UNIX BIND FLAW MAY LET REMOTE USERS GAIN PRIVILEGED ACCESS.

A vulnerability was reported in BIND on HP Tru64 UNIX. A remote user may be able to gain access on the target system. An unspecified vulnerability exists in the HP Tru64 UNIX operating system when running DNS BIND and configured as a DNS BIND name server. A remote user can gain privileged access. Solution: HP has issued Early Release Patch kits (ERPs). See source Website for more details.

Category 24.3 UNIX flavors

2006-03-14 **Linux XFS file system local information disclosure vulnerability solution update**

DHS IAIP Daily; http://www.securityfocus.com/bid/16921/references 23

LINUX KERNEL XFS FILE SYSTEM LOCAL INFORMATION DISCLOSURE VULNERABILITY.

The Linux kernel's XFS file system is susceptible to a local information disclosure vulnerability. Analysis: The flaw in the file system that may result in previously written data being returned to local users. A flaw was found in the module reference counting for loadable protocol modules of netfilter. By performing particular socket operations, a local attacker could exploit this to crash the kernel. A complete list of vulnerable products is given on the source advisory. Solution: The vendor has released version 2.6.15.5 to address this, and other issues. For more details: http://www.securityfocus.com/bid/16921/solution

---

Category 24.3 UNIX flavors

2006-03-16 **Linux kernel buffer overflow vulnerability race condition solution update**

DHS IAIP Daily; http://www.securityfocus.com/bid/14205/references 23

LINUX KERNEL IA32 EXECVE LOCAL BUFFER OVERFLOW VULNERABILITY.

The Linux kernel is susceptible to a local buffer overflow vulnerability. Analysis: This issue is due to a race condition in an IA32 emulation system call that leads to a memory copy operation that overflows a previously allocated memory buffer. During the time between two function calls to obtain buffer sizes, there exists a window of opportunity for attackers to alter memory contents. This race condition allows local attackers to overwrite critical kernel memory, facilitating kernel level machine code execution and privilege escalation. On multiprocessor computers, attackers can directly alter the memory contents to exploit this race condition. On uniprocessor computers, a blocking function call allows attackers to exploit the race condition. A complete list of vulnerable products is available in the source advisory. Solution: Version 2.4.32-pre1 or later of the 2.4 series, and 2.6.7 or later of the 2.6 series of the Linux kernel include a fix for this issue. It should be noted that the 2.4.32-pre1 version is not considered a stable, production quality kernel. Users of kernel series 2.4 may have to wait until proper vendor fixes, or a stable version of the kernel is released. For further solution details: http://www.securityfocus.com/bid/14205/solution

---

Category 24.3 *UNIX flavors*

2006-03-22 **Linux kernel buffer overflow vulnerabilities arbitrary command execution denial-of-service DoS**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2006/1046 23

LINUX KERNEL "DO_REPLACE" AND "NDIS" RESPONSE BUFFER OVERFLOW VULNERABILITIES.

Two vulnerabilities have been identified in Linux kernel, which could be exploited by attackers to execute arbitrary commands or cause a denial-of-service. Analysis: The first issue is due to a buffer overflow error in the do_replace() function [Netfilter module], which could be exploited by attackers to cause a kernel memory corruption and possibly execute arbitrary commands with elevated privileges. The second flaw is due to a buffer overflow error in drivers/usb/gadget/rndis.c when processing NDIS responses to OID_GEN_SUPPORTED_LIST, which could be exploited by attackers to cause a memory corruption and possibly execute arbitrary commands with elevated privileges. Affected products: Kernel versions prior to 2.6.16. Solution: Upgrade to kernel version 2.6.16: http://www.kernel.org/

Category 24.3 *UNIX flavors*

2006-03-28 **Sun Solaris process environment disclosure vulnerability solution update**

DHS IAIP Daily; http://www.hackerscenter.com/archive/view.asp?id=23886 23

SUN SOLARIS PROCESS ENVIRONMENT DISCLOSURE SECURITY ISSUE.

A security issue has been reported in Sun Solaris, which can be exploited by malicious, local users to gain knowledge of potentially sensitive information. Analysis: The security issue is caused due to the "/usr/ucb/ps" command revealing the environment variables and values of all processes to an unprivileged user when run with the "-e" option. This can potentially reveal certain information of processes that belong to the root user. Affected: Sun Solaris 8 and Sun Solaris 9. Solution: Apply patches. See source advisory for further solution details.

Category 24.3 *UNIX flavors*

2006-03-28 **Linux kernel IP ID value increment vulnerability information disclosure solution update**

DHS IAIP Daily; http://www.hackerscenter.com/archive/view.asp?id=23887 23

LINUX KERNEL IP ID VALUE INCREMENT WEAKNESS.

A weakness in the Linux kernel, which can be exploited to disclose certain system information and potentially to bypass certain security restrictions. Analysis: The weakness is caused due to an error within the "ip_push_pending_frames()" function when creating a packet in reply to a received SYN/ACK packet. This causes RST packets to be sent with a IP ID value that is incremented per packet. This can potentially be exploited to conduct idle scan attacks. Affected products: Linux Kernel 2.4.x; Linux Kernel 2.6.x. Solution: Update to version 2.6.16.1: http://www.kernel.org/ Secunia is currently not aware of any official patches for the 2.4 kernel.

Category 24.3 *UNIX flavors*

2006-04-04 **Linux kernel IP ID information disclosure vulnerability solution update**

DHS IAIP Daily; http://www.securityfocus.com/bid/17109/references 23

LINUX KERNEL IP ID INFORMATION DISCLOSURE WEAKNESS.

The Linux kernel is susceptible to a remote information disclosure weakness. This issue is due to an implementation flaw of a zero 'ip_id' information disclosure countermeasure. This issue allows remote attackers to use affected computers in stealth network port and trust scans. The replies to TCP SYN packets contain a correct IP ID value of zero, but replies to TCP SYNACK packets have an incremental IP ID field instead. This means a remote attacker can abuse this behavior for malicious purposes to perform an idle scan with nmap. For a complete list of vulnerable products: http://www.securityfocus.com/bid/17109/info Solution: Various Linux kernel versions, such as some in the 2.4 series, are not affected by this issue. The vendor has released version 2.6.16.1 of the Linux kernel to address this issue. For further solution details: http://www.securityfocus.com/bid/17109/solution

---

Category 24.3 *UNIX flavors*

2006-04-11 **Linux ioctl() denial-of-service DoS vulnerability no solution**

DHS IAIP Daily; http://www.securityfocus.com/bid/14902/discuss 23

LINUX KERNEL 64-BIT SYMMETRIC MULTI-PROCESSOR ROUTING_IOCTL() LOCAL DENIAL-OF-SERVICE VULNERABILITY.

A local denial-of-service vulnerability affects the Linux kernel on 64-bit Symmetric Multi-Processor platforms. Analysis: Specifically, the vulnerability presents itself due to an omitted call to the 'sockfd_put()' function in the 32 bit compatible 'routing_ioctl()' function. That insufficient input validation in the zisofs driver for compressed ISO file systems allows a denial-of-service attack through maliciously crafted ISO images. Multiple overflows exist in the io_edgeport driver which might be usable as a denial-of-service attack vector. A race condition in the /proc handling of network devices. A (local) attacker could exploit the stale reference after interface shutdown to cause a denial-of-service or possibly execute code in kernel mode. For a complete list of vulnerable products: http://www.securityfocus.com/bid/14902/info Solution: Linux kernel 2.6.13.2 is not vulnerable to this issue. For solution details: http://www.securityfocus.com/bid/14902/references

---

Category 24.3 *UNIX flavors*

2006-04-12 **Sun Solaris denial-of-service DoS vulnerability solution update**

DHS IAIP Daily; http://www.securityfocus.com/bid/17478/discuss 23

SUN SOLARIS SH(1) LOCAL DENIAL-OF-SERVICE VULNERABILITY.

Sun Solaris Bourne shell sh(1) is prone to a local denial-of-service vulnerability. Analysis: A security vulnerability in the Bourne shell may allow an unprivileged local user to cause sh(1) processes to crash while creating temporary files. This can lead to a denial-of-service for scripts or for users (such as 'root') that use sh(1). Vulnerable: Sun Solaris 10.0 _x86; Sun Solaris 10.0; Sun Solaris 9.0 _x86; Sun Solaris 9.0; Sun Solaris 8.0 _x86; Sun Solaris 8.0. Solution: Sun has released an advisory and fixes to address this issue. For more information: http://sunsolve.sun.com/search/document.do?assetkey=1-26-102 282-1

Category 24.3 *UNIX flavors*

2006-04-18 **Linux kernel child auto reap denial-of-service DoS vulnerability local remote solution update**

DHS IAIP Daily; http://www.securityfocus.com/bid/15625/discuss 23

LINUX KERNEL PTRACED CHILD AUTO REAP LOCAL DENIAL-OF-SERVICE VULNERABILITY.

Several local and remote vulnerabilities have been discovered in the Linux kernel that may lead to a denial-of-service or the execution of arbitrary code. Analysis: The kernel improperly auto reaps processes when they are being ptraced, leading to an invalid pointer. Further operations on this pointer result in a kernel crash. This issue allows local users to crash the kernel, denying service to legitimate users. For a complete list of vulnerable products: http://www.securityfocus.com/bid/15625/info Solution: Please see the referenced vendor advisories for further information on obtaining and applying the appropriate updates: http://www.securityfocus.com/bid/15625/references Linux kernel versions 2.6.15-rc3 and 2.6.14.3 have been released to address this issue.

Category 24.3 *UNIX flavors*

2006-04-29 **Linux kernel CIFS/SMB CHRoot security restriction bypass vulnerability no solution**

DHS IAIP Daily; http://www.securityfocus.com/bid/17742/references 23

LINUX KERNEL CIFS/SMB CHROOT SECURITY RESTRICTION BYPASS VULNERABILITY.

The Linux kernel is prone to a vulnerability that allows attackers to bypass a security restriction. Analysis: This issue is due to a failure in the kernel to properly sanitize user-supplied data. The problem affects chroot inside of an SMB-mounted filesystem ('cifs' or 'smbfs'). A local attacker who is bounded by the chroot can exploit this issue to bypass the chroot restriction and gain unauthorized access to the filesystem. For a complete list of vulnerable products: http://www.securityfocus.com/bid/17742/info Solution: Currently, Security Focus is not aware of any vendor-supplied patches for this issue.

Category 24.3 *UNIX flavors*

2006-04-29 **Linux kernel USB denial-of-service vulnerability solution update**

DHS IAIP Daily; http://www.securityfocus.com/bid/14955/discuss 23

LINUX KERNEL USB SUBSYSTEM LOCAL DENIAL-OF-SERVICE VULNERABILITY.

A local denial-of-service vulnerability affects the Linux kernel's USB subsystem. Analysis: This issue is due to the kernel's failure to properly handle unexpected conditions when trying to handle USB Request Blocks. Local attackers may exploit this to trigger a kernel 'oops' on computers where the vulnerable USB subsystem is enabled. This would deny service to legitimate users. For a complete list of vulnerable products: http://www.securityfocus.com/bid/14955/info Solution: Please see the referenced vendor advisories for further information on obtaining and applying the appropriate updates: http://www.securityfocus.com/bid/14955/references

---

Category 24.3 *UNIX flavors*

2006-05-02 **Department of Homeland Security code audit critical Linux bugs**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1956652,00.asp 23

DEPARTMENT OF HOMELAND SECURITY AUDIT FLAGS 'CRITICAL' LINUX BUG.

An open-source security audit program funded by the U.S. Department of Homeland Security has flagged a critical vulnerability in the X Window System which is used in Unix and Linux systems. Coverity, the San Francisco-based company managing the project under a $1.25 million grant, described the flaw as the "biggest security vulnerability" found in the X Window System code since 2000. Coverity Chief Technical Officer Ben Chelf said the flaw resulted from a missing parenthesis on a small piece of the program that checked the ID of the user. It could be exploited to allow local users to execute code with root privileges, giving them the ability to overwrite system files or initiate denial-of-service attacks.

Category 24.3 *UNIX flavors*

2006-05-02 **vulnerabilities Linux Cisco products software CLI application arbitrary code execution**

DHS IAIP Daily; http://www.securiteam.com/unixfocus/5LP050KIKW.html 23

MULTIPLE VULNERABILITIES IN LINUX-BASED CISCO PRODUCTS.

A vulnerability in the CiscoWorks WLSE "show" CLI application allows execution of arbitrary code as the root user. Analysis: The Cisco shell presents the administrator with a restricted set of commands which includes a "show" application. The "show" application has several vulnerabilities which allow an attacker to "break out" of the shell and execute commands (including /bin/sh) as the root user. A cross site scripting flaw exists in: /wlse/configure/archive/archiveApplyDisplay.jsp with the "displayMsg" parameter. This can be used to steal the JSP session cookie, therefore giving a targeted attacker admin level access to the system. Once the attacker has admin Web GUI access to the system via the XSS, they can then change the admin password or create a new admin user (without requiring the admin password). Affected software: Cisco Wireless Lan Solution Engine (WLSE); Cisco Hosting Solution Engine (HSE); Cisco Ethernet Subscriber Solution Engine (ESSE); Cisco User Registration Tool (URT); CiscoWorks2000 Service Management Solution (SMS); Cisco Vlan Policy Server (VPS); Cisco Management Engine (ME1100 Series); CiscoWorks Service Level Manager (SLM). Solution: Cisco has released patches for the vulnerabilities. Cisco Security Advisory: http://www.cisco.com/warp/public/707/cisco-sa-20060419-wlse. shtml Cisco Security Response: http://www.cisco.com/warp/public/707/cisco-sr-20060419-priv. shtml

---

Category 24.3 *UNIX flavors*

2006-05-09 **Linux kernel SCTP denial-of-service vulnerabilities solution update**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2006/1734 23

LINUX KERNEL SCTP CHUNKS HANDLING REMOTE DENIAL-OF-SERVICE VULNERABILITIES.

Multiple vulnerabilities have been identified in Linux kernel, which could be exploited by remote attackers to cause a denial-of-service. Analysis: The first issue is due to an error in the Stream Control Transmission Protocol (SCTP) code that uses incorrect state table entries when certain ECNE chunks are received in CLOSED state, which could be exploited by attackers to cause a kernel panic via a specially crafted packet. The second flaw is due to an error when handling incoming IP-fragmented SCTP control chunks, which could be exploited by attackers to cause a kernel panic via a specially crafted packet. Affected products: Linux kernel version 2.6.16.14 and prior. Solution: Upgrade to Linux Kernel version 2.6.16.15: http://www.kernel.org

---

24.4 TCP/IP & HTTP

Category 24.4 TCP/IP & HTTP

1998-12-23 **TCP/IP vulnerability hole weakness advisory threat denial**

CNET news.com http://www.news.com/News/Item/Textonly/0,25,30250,00.html

CERT-CC announced that another vulnerability to IP spoofing in the TCP/IP that underlies the Internet would allow denial-of-service attacks by criminal hackers. Using forged source address in packet headers, the attackers could crash vulnerable systems. CERT-CC posted solutions to the exploit on its site, recommending that vulnerable Web sites reconfigure their routers or firewalls and install filtering on the routers to prevent IP spoofing attacks.

Category 24.4 TCP/IP & HTTP

2000-09-25 **availability single point of failure dynamic addressing**

RISKS 21 07

William P. N. Smith reported in RISKS on an interesting failure of his cable-modem service on the 24th September due to failure of the DHCP (Dynamic Host Configuration Protocol) servers that temporarily assign ("lease") IP addresses to users on TCP/IP networks: "Turns out the DHCP server for the entire northeast went down, and as people's leases on their IP addresses expired, they were dropped off the network. I asked about the secondary or backup DHCP servers, but apparently there was so much demand due to expired leases that the backup server couldn't respond quickly enough, and was getting overloaded with requests."
[A personal note from your editor: I have a secondary ISP with which I contract for only 5 hours a month at a very low cost. Although I use it rarely, it has prevented me from snarling in frustration on the odd occasion when my primary ISP has rejected connections.]

Smith drew two particularly interesting conclusions from this case:
* "Even single users ought to have a backup Internet connection" such as a dialup ISP;
* "Your backups might have to be more powerful than your primary servers. . . ."

Category 24.4 TCP/IP & HTTP

2000-12-16 **Web site redirection spoof HTTP syntax misleading trickery hoax joke**

RISKS 21 16

A hoax taking advantage of a little-used and practically unknown feature of HTTP syntax for URLs convinced many victims that the CNN.com site had been hacked. Rob Warnock explained what happened in a report for the RISKS Forum: "An MIT student named Eric Varady took a parody news article from The Onion <URL:http://www.theonion.com/onion3637/bush_horrified.html>, edited the layout to resemble CNN's format, and copied it to his own site <URL:http://salticus-peckhamae.mit.edu/evarady/www/top_story.htm>." He then circulated a false story about a hack of the CNN site and pointed people to < URL:http://www.cnn.com&story=breaking_news@18.69.0.44/evarady/www/top_story.htm>. It turns out that although this URL follows the correct syntax, anyone assuming that the Web page resides on "www.cnn.com" is being misled. The section between the "//" delimiter and the "@" sign is actually interpreted as a _user_ field and then discarded. The actual URL is therefore the part following the "@" sign and is therefore equivalent to < http://18.69.0.44/evarady/www/top_story.htm >. The numerical IP address is "salticus-peckhamae.mit.edu." Moral: any URL containing the "@" sign should be parsed carefully to find out where it is _really_ pointing. Warnock concluded, "The RISK is that users are being bombarded with these monstrosities so often that they've grown used to it, and that they'll fail to recognize when they're being sent someplace they might not really want to go!! (Perhaps when it's not a joke, such as being sent to a porn site while working at a company with a "no tolerance" policy.)"

Category 24.4 *TCP/IP & HTTP*

2001-05-01 **vulnerability sequence number datagrams packets alert CERT/CC**

NIPC Daily Report

On 1 May, CERT/CC released Advisory CA-2001-09, Statistical Weaknesses in TCP/IP Initial Sequence regarding a new vulnerability (CERT VU#498440, CVE CAN-2001-0328) which is present when using random increments to constantly increase TCP ISN values over time. Attacks against TCP initial sequence number (ISN) generation have been discussed for some time now. The reality of such attacks led to the widespread use of pseudo-random number generators (PRNGs) to introduce some randomness when producing ISNs used in TCP connections. Previous implementation defects in PRNGs led to predictable ISNs despite some efforts to obscure them. The defects were fixed and thought sufficient to limit a remote attacker's ability to attempt ISN guessing. It has long been recognized that the ability to know or predict ISNs can lead to manipulation or spoofing of TCP connections. What was not previously illustrated was just how predictable one commonly used method of partially randomizing new connection ISNs is in some modernTCP/IP implementations. Additional information regarding this advisory can be found at
http://www.cert.org/advisories/CA-2001-09.html. (Source: CERT/CC, 1 May)

Category 24.4 *TCP/IP & HTTP*

2003-01-16 **buffer overflow vulnerabilities Internet Software Consortium ISC BIND**

NIPC/DHS

January 16, CERT/CC — VU#284857: Buffer overflows in ISC DHCPD minires library.

During an internal source code audit, developers from the Internet Software Consortium (ISC) discovered several vulnerabilities in the error handling routines of the minires library, which is used by NSUPDATE to resolve hostnames. These vulnerabilities are stack-based buffer overflows that may be exploitable by sending a DHCP message containing a large hostname value. Note: Although the minires library is derived from the BIND 8 resolver library, these vulnerabilities do not affect any current versions of BIND. At this time, CERT is not aware of any exploits. The ISC has addressed these vulnerabilities in versions 3.0pl2 and 3.0.1RC11 of ISC DHCPD. More information may be found on the ISC Website:
http://www.isc.org/

Category 24.4 *TCP/IP & HTTP*

2003-07-16 **MS03-026 buffer overrun RPC remote procedure call interface code execution DCOM 135 changing viewing deleting data installing programs unauthorized**

NIPC/DHS

July 16, Microsoft — Microsoft Security Bulletin MS03-026: Buffer Overrun In RPC Interface Could Allow Code Execution.

Remote Procedure Call (RPC) is a protocol used by the Windows operating system which provides an inter-process communication mechanism that allows a program running on one computer to seamlessly execute code on a remote system. There is a vulnerability in the part of RPC that deals with message exchange over TCP/IP which results because of incorrect handling of malformed messages. This vulnerability affects a Distributed Component Object Model (DCOM) interface with RPC, which listens on TCP/IP port 135. This interface handles DCOM object activation requests that are sent by client machines to the server. To exploit this vulnerability, an attacker would need to send a specially formed request to the remote computer on port 135. If successful, an attacker could then run code with Local System privileges on an affected system and then be able to take any action on the system, including installing programs, viewing changing or deleting data, or creating new accounts with full privileges. Microsoft has assigned a risk rating of "Critical" to this issue and recommends that system administrators install the patch immediately.

Category 24.4 *TCP/IP & HTTP*

2003-07-17 **flaw vulnerability Windows Cisco Microsoft routers**

NewsScan

YESTERDAY A MICROSOFT FLAW, TODAY A CISCO FLAW
Cisco, which makes communications routers and switches, has found a flaw in its software that could be used by network vandals to cause widespread outages; the company has released a free patch to fix the flaw in its Internetworking Operating System. No vandals have exploited the vulnerability up to this point, and Cisco says: "We literally have people working around the clock right now to get this situation taken care of." According to the company, the vulnerability could only be exploited by sending a "rare sequence" of data packets to a device running IOS, the equivalent of Windows for routers and switches. (AP/San Jose Mercury News 17 Jul 2003)

Category 24.4 *TCP/IP & HTTP*

2003-09-03 **MS03-034 NetBIOS information Disclosure BNBS NetBT Name Service UDP port 137 Internet Browser query**

NIPC/DHS

September 03, Microsoft — Microsoft Security Bulletin MS03-034: Flaw in NetBIOS Could Lead to Information Disclosure.

Under certain conditions, the response to a NetBT Name Service (NBNS) query may, in addition to the typical reply, contain random data from the target system's memory. This data could, for example, be a segment of HTML if the user on the target system was using an Internet browser, or it could contain other types of data that exist in memory at the time that the target system responds to the NBNS query. An attacker could seek to exploit this vulnerability by sending a NBNS query to the target system and then examine the response to see if it included any random data from that system's memory. If best security practices have been followed and port 137 UDP has been blocked at the firewall, Internet based attacks would not be possible. Microsoft has assigned a risk rating of "Low" to this vulnerability and a patch is available on the Microsoft website.

Category 24.4 *TCP/IP & HTTP*

2003-12-11 **Moonv6 Internet Protocol IPv6 security testing network**

NIPC/DHS

December 09, Government Computer News — Moonv6 testing to continue.

Initial ten-day testing in October on the nation's largest native IPv6 network by the Department of Defense (DoD) and the University of New Hampshire demonstrated IPv6 linkage of academic and military sites from New Hampshire to San Diego. Time was short, and there was a dearth of applications written for the new Internet Protocol. "We had a limited number of vendor implementations to work with," said Ben Schultz, managing engineer of the University of New Hampshire's interoperability laboratory. Opportunities to test security also were limited, he said Tuesday, December 9, at the U.S. IPv6 Summit in Arlington, VA. Under those constraints, the File Transfer Protocol, Hypertext Transfer Protocol, Secure HTTP, Telnet and Domain Name System applications worked, Schultz said. The Moonv6 test bed is a collaboration by JITC, the university lab and the North American IPv6 Task Force. The second phase of testing, scheduled to run from February 2 to April 14, will dig deeper into security, mobility and routing protocol testing, as well as network stability and management, JITC's Major Roswell Dixon said.

Category 24.4 *TCP/IP & HTTP*

2003-12-11 **Internet Protocol IPv6 security implementation IPSec**

NIPC/DHS

December 10, Government Computer News — IPv6 will need security, too, experts warn.

Security has been one of the selling points for the new Internet protocol, but IPv6 is not inherently secure, say those planning its implementation. The Internet Engineering Task Force is still working on IPv6 security elements and "many of them need to be tested in the real world," security consultant Richard Graveman said Wednesday, December 10, at the U.S. IPv6 Summit in Arlington, VA. One of the key security elements in IPv6 is IPSec encryption, which is mandatory in the new protocol. But security is more than IPSec, Graveman said. "Downloading an encrypted virus and installing it is just as bad as downloading an unencrypted virus," he said. Good encryption will not stop hackers either, he said. "You don't break good crypto, you go around it," he said, so proper implementation of IPv6 and a secure platform still are key to securing networks. Latief Ladid, president of the IPv6 Forum, said warned that hackers already are studying the new protocols and are uncovering security flaws.

Category 24.4 *TCP/IP & HTTP*

2004-01-14 **Microsoft security bulletin patch flaw vulnerability fix Exchange Server http**

DHS/IAIP Update

MICROSOFT SECURITY BULLETIN MS04-002: VULNERABILITY IN EXCHANGE SERVER 2003 COULD LEAD TO PRIVILEGE ESCALATION.

A vulnerability exists in the way that Hypertext Transfer Protocol (HTTP) connections are reused when NTLM authentication is used between front-end Exchange 2003 servers providing Outlook Web Access (OWA) and, OWA on Windows 2000 and Windows Server 2003, and when using back-end Exchange 2003 servers that are running Windows Server 2003. Users who access their mailboxes through an Exchange 2003 front-end server and OWA might get connected to another user's mailbox if that other mailbox is (1) hosted on the same back-end mailbox server and (2) if that mailbox has been recently accessed by its owner. Attackers seeking to exploit this vulnerability could not predict which mailbox they might become connected to. The vulnerability causes random and unreliable access to mailboxes and is specifically limited to mailboxes that have recently been accessed through OWA. This vulnerability is exposed if the Website that is running the Exchange Server 2003 programs on the Exchange back-end server has been configured not to negotiate Kerberos authentication, causing OWA to fall back to using NTLM authentication. The only known way that this vulnerability can be exposed is by a change in the default configuration of Internet Information Services 6.0 on the Exchange back-end server. Microsoft has assigned a severity rating of "Moderate" to this issue.

Category 24.4 *TCP/IP & HTTP*

2004-03-22 **security vulnerability flaw hole patch fix exploit open source Apache Web server HTTP**

DHS IAIP Daily;

March 19, eWEEK — Security holes uncovered in Apache.

Security researchers on Friday, March 19, uncovered a vulnerability in the open-source Apache Web server software that could easily enable a denial of services attack. The Apache problem is one of several reported in Version 2.0.48, and lets an attacker open a short-lived connection on a particular, rarely accessed listening socket. The software will block out all other connections until another connection comes in on the same socket. The Apache Software Foundation released update to its HTTP Server software that fixed the problem as well as several others:
http://www.apacheweek.com/redirect.cgi?link=http://www.apache.org/

Category 24.4 *TCP/IP & HTTP*

2004-04-20 **TCP Transmission Control Protocol design flaw disrupt Internet router**

NewsScan

SERIOUS FLAW IN TCP FOUND

Computer security experts in the U.S. and Britain have identified an inherent design flaw in the transmission control protocol (TCP) that could make it easy for hackers to disrupt Internet activities worldwide. Paul Watson, the security researcher who sounded the alarm over the flaw, warns it could be used to disable Internet routers -- the complex machines that direct most Internet traffic -- by tricking them into resetting themselves. Apparently, security experts have known for years about the basic vulnerability, but discounted its threat because attackers would have to successfully guess several specific sets of information in order to exploit it -- something that many thought would take several years using powerful computers. Watson appears to have discovered a shortcut that makes it possible to complete that task in just a few minutes. U.S. Homeland Security cybersecurity director Amit Yoran says despite the seriousness of the problem, most of the world's major Internet service providers have already quietly taken steps to protect themselves: "It's important to note that this is a significant discovery, but it's also important to provide a fair degree of assurance that the sky is not falling." (Washington Post 20 Apr 2004)

Category 24.4 *TCP/IP & HTTP*

2004-04-20 **Internet security flaw fix experters disrupt communications routers TCP/IP protocol**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/articles/A27890−2004Apr 20.html

April 20, Washington Post — Experts race to fix serious Internet flaw.

Computer security experts in the U.S. and UK confirmed Tuesday, April 20, that a new method has been identified that could make it easy for hackers to disrupt Internet communications worldwide. The exploit, identified by Milwaukee security researcher Paul Watson, could give hackers the ability to crash Internet routers--the complex machines that direct most of the world's Web traffic. Watson's method takes advantage of an inherent design flaw in transmission control protocol (TCP)--the language that all computers use to communicate on the Internet--that could place ordinary computers at greater risk of attack. Watson is slated to present his findings at a security conference in Canada later this week. Amit Yoran, director of the cybersecurity division for the Department of Homeland Security, said most of the world's major Internet service providers had already taken steps to prevent the attack. Additional information is availabe in "Technical Cyber Security Alert TA04-111A: Vulnerabilities in TCP," available on the U.S. Computer Emergency Readiness Team Website: http://www.us-cert.gov/cas/techalerts/TA04-111A.html. The UK's National Infrastructure Security and Coordination Center has posted a vulnerability notice here: http://www.uniras.gov.uk/vuls/2004/236929/index.htm

---

Category 24.4 *TCP/IP & HTTP*

2004-04-21 **TCP injection vulnerability Border Gateway Protocol Initial Sequence Number DoS routers**

http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci960715,00.html?track=NL-102&ad=480263

In April 2004, the technical press responded strongly to notices of some fundamental flaws in the TCP/IP suite.
* The "TCP Injection Vulnerability" could work with a problem in the Border Gateway Protocol to allow remote termination of network sessions, potentially leading to denial of service.

* The "TCP/IP Initial Sequence Number Vulnerability" could permit data corruption, session hijacking and denial of service.<

Internet Security Systems (ISS) stated that "network infrastructure providers and enterprises' internal networks …[are] the most vulnerable to potential denial-of-service/distributed denial-of-service attacks that can cause significant outages and downtime to users and customers."

Shawna McAlearney, writing for SearchSecurity.com, summarized recommendations as follows: "Experts recommend immediately applying patches issued by affected vendors. Workarounds include: ingress and egress filtering; prohibiting externally initiated inbound connections to non-authorized services and preventing machines providing public services from initiating outbound connections to the Internet; deploying and using cryptographically secure protocols, such as IPSec; and network isolation."

Category 24.4 *TCP/IP & HTTP*

2004-07-31 **domain name service DNS vulnerability Defcon 12 presentation intellectual property theft**

DHS IAIP Daily; http://news.com.com/Internet%27s+%27white+pages%27+allow+data+attacks/2100−1002_3−5291874.html?tag=nefd.hed

July 31, CNET News.com — Internet's 'white pages' allow data attacks.

The same technology that allows Web surfers to locate and connect to computers on the Internet can be used to create covert communications channels, bypass security measures and store distributed content, a security researcher said at the Defcon hacking conference in Las Vegas, NV, Saturday, July 31. The security hack essentially uses data transferred by domain name service (DNS) servers to hide additional information in the network communications. DNS servers act as the white pages of the Internet, invisibly transforming easy-to-remember domain names into the numerical network addresses used by computers. Moreover, corporate security measures, such as firewalls, tend to ignore DNS data because they assume it's harmless, said Dan Kaminsky, a security researcher for telecommunications firm Avaya said. That flaw in most companies' network security leaves a vulnerability that can be used by hackers to sneak intellectual property outside a company, communicate with a compromised server inside the company, or gain free access to many wireless and Internet services found in coffee houses and hotels, he said.

Category 24.4 TCP/IP & HTTP

2004-08-11 **IBM Tivola vulnerability http response splitting input validation patch issued**

DHS IAIP Daily; http://www.zone−h.org/advisories/read/id=5254

August 11, zone-h — IBM Tivoli Access Manager HTTP response splitting vulnerability.

A vulnerability has been discovered in IBM Tivoli Access Manager for e-business, which can be exploited by malicious people to conduct cross-site scripting attacks. The vulnerability is caused due to insufficient input validation and can be exploited to inject malicious characters into HTTP headers. This may allow execution of arbitrary HTML and script code in a user's browser session associated with an affected site. According to the vendor, successful exploitation may allow people to gain access and control over an affected system. A patch is available from the vendor.

Category 24.4 TCP/IP & HTTP

2004-10-07 **Internet Protocol IP v6 security protocol adoption interest Internet**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/27552−1.html

October 07, Government Computer News — Market for IPv6 security is starting to grow.

Internet Protocol Version 6 (IPv6) is still in the early adoption phase, but commercial demand for tools to secure IPv6 networks is beginning to grow, according to one vendor. The Defense Department, which has committed to moving its networks to IPv6 by fiscal 2008, is the largest government customer for the security products. IPv6 provides improved security, increased IP address space and greater authentication capabilities to the Internet. Jim Bound, chairman of the North American IPv6 Task Force, said Japan now is the only country with a production IPv6 Internet backbone. Other networks, such as the Moonv6 test bed in the United States, are in pilot phases.

Category 24.4 TCP/IP & HTTP

2005-02-15 **Sami HTTP server input validation vulnerability directory traversal attack no update issued**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2005/Feb/1013191.html

SAMI HTTP SERVER INPUT VALIDATION VULNERABILITIES

A remote user can view files on the target system or cause the web service to crash by sending a specially crafted HTTP request containing '../' directory traversal characters to obtain files on the system that are located outside of the web document directory. Encoded directory traversal characters can also be used. The user can also send an HTTP request to cause the web service to crash. There is no solution at this time.

Category 24.4 TCP/IP & HTTP

2005-02-16 **Hewlett-Packard HP Web-enabled Management Software HTTP buffer overflow vulnerability code execution attack update issued**

DHS IAIP Daily; http://secunia.com/advisories/14311/

HP WEB-ENABLED MANAGEMENT SOFTWARE HTTP SERVER BUFFER OVERFLOW

A vulnerability has been reported in HP HTTP Server, which can be exploited by malicious people to compromise a vulnerable system. The vulnerability is caused due to an unspecified boundary error within the handling of input parameters and can be exploited to cause a buffer overflow. Successful exploitation may allow execution of arbitrary code. Update to HP HTTP Server 5.96 or Systems Management Hompage version 2.0. Management Software Security Patch for Windows Version 5.96: http://h18023.www1.hp.com/support/files/Server/us/download/2 2192.html

---

Category 24.4 *TCP/IP & HTTP*

2005-02-22 **PuTTY shell integer overflow vulnerabilities code execution attack update issued**

DHS IAIP Daily; http://secunia.com/advisories/14333/

TWO NEW VULNERABILITIES HAVE BEEN REPORTED IN PUTTY

The first vulnerability is an integer overflow in the "fxp_readdir_recv()" function in "sftp.c" that can be exploited to execute arbitrary code via a malicious SFTP (SSH File Transfer Protocol) server sending a specially crafted respond to the "FXP_READDIR" command. The second is an integer overflow in the "fxp_open_recv()" function in "sftp.c" that can be exploited to execute arbitrary code via a malicious SFTP server sending a specially crafted string field. Successful exploitation is only possible after host key verification. Update to version 0.57:
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.h tml

---

Category 24.4 *TCP/IP & HTTP*

2005-03-30 **Kerberos MIT open source authentication application telnet client heap based buffer overflow vulnerabilities update issued**

DHS IAIP Daily; http://secunia.com/advisories/14745/

MIT KERBEROS TELNET CLIENT HAS BUFFER OVERFLOW VULNERABILITIES

Two vulnerabilities have been reported in Kerberos V5, which can be exploited by malicious people to compromise a vulnerable system. A boundary error in the "slc_add_reply()" function in the included telnet client when handling LINEMODE sub-options can be exploited to cause buffer overflow via a specially crafted reply containing a large number of SLC (Set Local Character) commands. A boundary error in the "env_opt_add()" function in the included telnet client when handling NEW-ENVIRON sub-options can be exploited to cause a heap-based buffer overflow via a specially crafted reply containing a large number of characters that need escaping. Original advisory and patch available at:
http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2005-0 01-telnet.txt

---

Category 24.4 *TCP/IP & HTTP*

2005-03-30 **Telnet client heap based buffer overflow multiple vulnerabilities command execution attack update issued**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/0300

MULTIPLE TELNET CLIENTS BUFFER OVERFLOW VULNERABILITIES

Two vulnerabilities were identified in several Telnet clients, which may be exploited by attackers to execute arbitrary commands. The first flaw is due to a heap overflow error in the "env_opt_add()" function (telnet.c), which may be exploited to execute arbitrary commands in the context of the user who launched the telnet client. The second vulnerability is due to a buffer overflow error when handling LINEMODE suboptions and processing replies containing a large number of SLC (Set Local Character) commands, which may be exploited to execute arbitrary commands in the context of the user who launched the telnet client. Solutions available through Source link below.

Category 24.4 *TCP/IP & HTTP*

2005-04-13 **Internet Protocol IP Control Message Protocol ICMP flaw attack router Internet software UK short term denial of service DoS**

DHS IAIP Daily;
http://www.infoworld.com/article/05/04/13/HNipflaw_1.html?SE CURITY

IP FLAW COULD ALLOW ATTACKS ON ROUTERS AND INTERNET SOFTWARE

The UK's National Infrastructure Co-Ordination Center (NISCC) has warned of a flaw in Internet Protocol (IP) that could allow significant attacks on a wide range of products, including routers and Internet software from Microsoft, Cisco Systems, IBM, Juniper Networks, and others. While the flaw in ICMP, IP's control protocol, will be only moderately critical for some vendors' products, in others it could allow a denial-of-service attack with medium-term effects, effectively putting the system out of commission for a significant period of time while it is reset, the NISCC said in an advisory. In other products, attacks could merely slow down traffic or result in short-term denial-of-service. "Most vendors include support for this protocol in their products and may be impacted to varying degrees," the agency said in its advisory. NISCC Advisory:
http://www.niscc.gov.uk/niscc/docs/al-20050412-00308.html?la ng=en

---

Category 24.4 *TCP/IP & HTTP*

2005-04-14 **Transmission Control Protocol TCP sequence number approximation vulnerability reset session update issued**

DHS IAIP Daily; http://www.securityfocus.com/bid/10183/info/

MULTIPLE VENDOR TCP SEQUENCE NUMBER APPROXIMATION VULNERABILITY

A vulnerability in TCP implementations has been reported that may permit unauthorized remote users to reset TCP sessions. This issue affects products released by multiple vendors. This issue may permit TCP sequence numbers to be more easily approximated by remote attackers. Vendor advisories and solutions through Source link.

Category 24.4 *TCP/IP & HTTP*

2005-05-09 **Internet Protocol Security IPSec information disclosure vulnerability**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/0507

IPSEC ESP CONFIGURATIONS INFORMATION DISCLOSURE VULNERABILITY

Three vulnerabilities were identified in certain configurations of IPSec, which may be exploited by attackers to disclose sensitive information. These attacks are possible when IPSec uses Encapsulating Security Payload (ESP) in tunnel mode with confidentiality only, or with integrity protection being provided by AH or a higher layer protocol. A remote attacker that is able to intercept and modify IPSec and ICMP communications between security gateways, could exploit this vulnerability and perform "Destination Address Rewriting", "IP Options modification", and "Protocol Field modification" attacks, which will cause the plaintext version of the IPsec communications between the protocols to be disclosed. See Source link for suggested workarounds.

Category 24.4 *TCP/IP & HTTP*

2005-05-17 **Internet Protocol IPv6 TCP IP LAN denial of service DoS Microsoft vulnerability**

DHS IAIP Daily; http://www.securityfocus.com/bid/13658/info/

MICROSOFT IPV6 TCPIP LOOPBACK LAND DENIAL OF SERVICE VULNERABILITY

The Microsoft Windows IPV6 TCP/IP stack is prone to a "loopback" condition initiated by sending a TCP packet with the "SYN" flag set and the source address and port spoofed to equal the destination source and port. When a packet of this type is handled, an infinite loop is initiated and the affected system halts. A remote attacker may exploit this issue to deny service for legitimate users. There is no solution at this time.

Category 24.4 *TCP/IP & HTTP*

2005-07-27 **IPSec Incorrection networking AES XCBC MAC algorithm encryption forge packets disclosure privilege**

DHS IAIP Daily; http://www.zone−h.org/advisories/read/id=7851

IPSEC INCORRECT KEY USAGE IN AES-XCBC-MAC

IPsec is a security protocol for the Internet Protocol networking layer. It provides a combination of encryption and authentication of system, using several possible cryptography algorithms. A programming error in the implementation of the AES-XCBC-MAC algorithm for authentication resulted in a constant key being used instead of the key specified by the system administrator. If the 10 AES-XCBC-MAC algorithm is used for authentication in the absence of any encryption, then an attacker may be able to forge packets which appear to originate from a different system and thereby succeed in establishing an IPsec session. If access to sensitive information or systems is controlled based on the identity of the source system, this may result in information disclosure or privilege escalation.

Category 24.4 TCP/IP & HTTP

2005-08-03 **domain name system DNS services WWW Internet vulnerable cache poisoning**

EDUPAGE; http://news.com.com/2100-7349_3-5816061.html

RESEARCHER SAYS DNS SERVERS VULNERABLE

In a presentation at the Black Hat conference last week, security researcher Dan Kaminsky argued that domain name system (DNS) servers represent a broad vulnerability in the Internet. Kaminsky said that of 2.5 million DNS servers he tested, nearly 10 percent could be susceptible to so-called DNS cache poisoning. In total, about 9 million DNS servers are operating globally. DNS servers translate typed URLs into numbers necessary to locate Web sites. In cache poisoning, legitimate numeric Web addresses are replaced, causing users to be redirected to sites of the hacker's choosing. Often, users are sent to Web sites that install malware or that deceive users into disclosing personal information, which can then be used in identity theft. Incidents of cache poisoning have disrupted Internet service in the past, including this March, when users trying to access CNN.com and MSN.com were sent to sites that installed spyware. Security experts advise operators of DNS servers to audit their machines and make sure they configure them in the safest manner possible.
CNET, 3 August 2005

Category 24.4 TCP/IP & HTTP

2006-01-02 **cross-site scripting command execution vulnerability Nortel SSL VPN**

DHS IAIP Daily; 23
http://www.securiteam.com/windowsntfocus/5GP060KHFE.html

NORTEL SSL VPN CROSS-SITE SCRIPTING AND COMMAND EXECUTION

The Nortel SSL VPN is a remote access security solution. By using secure sockets layer (SSL) as the underlying security protocol, Nortel SSL VPN allows for using the Internet for remote connectivity and the ubiquitous Web browser as the primary client interface. Due to insufficient input validation within the Web interface of Nortel's SSL VPN appliance, it is possible to hide commands in links to certain pages of the Web interface. As the Java Applet which is called from those Web pages is cryptographically signed, it may execute operating system commands with the privileges of the user sitting in front of the browser. An attacker can thus supply a victim with malicious link where remote commands are hidden. If the victim clicks on the link and logs onto the SSL VPN Web interface (where it is automatically taken), arbitrary commands are executed locally on the client of the victim.

Category 24.4 TCP/IP & HTTP

2006-01-09 **Internet Protocol IPv6 technology upgrade US government DoD OMB**

DHS IAIP Daily; 23
http://www.compliancepipeline.com/news/175803121;jsessionid=
AYA3DIDAR5V2OQSNDBECKHSCJUMEKJVN

IPV6: WORLD'S LARGEST TECHNOLOGY UPGRADE ON DECK

Bugs, spam, viruses, software security issues, quality of service and more have spurred experts to push for commercial deployment and government reform on Internet Protocol version 6 (IPv6). A panel battled the topic of when companies should deploy IPv6 and where the technology will make the greatest impact. The discussion took place at the 2006 International Consumer Electronics show in Las Vegas, NV, last week. In the end, the four panelists agreed to disagree. IPv6, the latest version of Internet Protocol, provides more IP addresses than today's version 4. It supports auto-configuration to help correct most shortcomings in the current version, and has security, quality of service, digital rights management and mobile communications features. The debate has heated up in the U.S. now that Asian countries are mandating adoption where IP addresses are in short supply. The U.S. government and the Department of Defense, two of IPv6's strongest proponents, are estimated to spend billions to make the transition happen. The White House Office of Management and Budget has directed U.S. federal agencies to develop IPv6 transition plans by February and requires that agencies comply with the mandate by June 2008.

Category 24.4 *TCP/IP & HTTP*

2006-04-06 **Cisco Optical Networking System multiple vulnerabilities denial-of-service DoS**

DHS IAIP Daily; http://secunia.com/advisories/19553/ 23

CISCO OPTICAL NETWORKING SYSTEM 15000 SERIES MULTIPLE VULNERABILITIES.

Some vulnerabilities have been reported in Cisco Optical Networking System 15000 Series, which can be exploited by malicious people to cause a denial-of-service (DoS) or compromise a vulnerable management system. Multiple services are vulnerable to ACK DoS attacks where an invalid response is sent instead of the final ACK packet during the 3-way handshake. This can be exploited to cause the control cards to exhaust memory resources, not respond to further connections, or reset by establishing multiple of these connections. Successful exploitation requires that IP is configured on the LAN interface (enabled by default). For more information please see source advisory. Solution: Updated versions are available -- see patch matrix in vendor advisory: http://www.cisco.com/warp/public/707/cisco-sa-20060405-ons.s html Also update to Cisco Transport Controller version 4.1.0 or later.

Category 24.4 *TCP/IP & HTTP*

2006-05-09 **Sun Solaris IPSec IKE processing bug remote denial-of-service DoS vulnerability solution update**

DHS IAIP Daily; http://securitytracker.com/alerts/2006/May/1016043.html 23

SUN SOLARIS LIBIKE IPSEC IKE PROCESSING BUG LETS REMOTE USERS DENY SERVICE.

A vulnerability was reported in the 'in.iked' daemon on Sun Solaris. A remote user can cause denial-of-service conditions. Analysis: The 'libike' library does not properly process certain Internet Key Exchange (IKE) packets. A remote user can send specially crafted packets to the target system to cause the in.iked(1M) daemon to crash or to potentially send invalid data to a peer system, which may in turn cause the peer system's in.iked daemon to crash. Solution: Sun has issued the following fixes: SPARC Platform: Solaris 9 with patch 113451-11 or later; Solaris 10 with patch 118371-07 or later. x86 Platform: Solaris 9 with patch 114435-10 or later; Solaris 10 with patch 118372-07 or later. Sun advisory: http://sunsolve.sun.com/search/document.do?assetkey=1-26-102 246-1

24.5 LAN OS

Category 24.5 *LAN OS*

2001-10-15 **wireless networks wired LANs cache poisoning vulnerability penetration hacker**

RISKS 21 69

Gary McGraw summarized a new class of wireless attacks in RISKS:

Bob Fleck, a security consultant at Cigital, working with Jordan Dimov, has discovered new class of wireless attacks that can be used to gain unauthorized access to normally-protected machines on a standard wire-based internal network. Wireless networks involve installation of a wireless Access Point on a normal internal network. This Access Point is usually connected to the wired network through a switch or a hub. The attacks discovered by Cigital are based on an adaptation of a well understood network attack from the non-wireless world known as ARP cache poisoning. This emphasizes the importance of re-considering old risks in light of new technologies, something that is especially important in software-based systems!

The new class of attacks encompasses: 1) the ability to monitor and manipulate traffic between two wired hosts behind a firewall 2) the ability to monitor and manipulate traffic between a wired host and a wireless host 3) the ability to compromise roaming wireless clients attached to different Access Points 4) the ability to monitor and manipulate traffic between two wireless clients

Previous wireless attacks have demonstrated that wireless traffic on an 802.11b network is vulnerable to monitoring and manipulation, even when it is "protected" with WEP encryption. This new class of attacks discovered by Cigital is based on abusing the Address Resolution Protocol (ARP) which binds internal IP addresses to ethernet addresses.

Mitigating the risks of these attacks is possible. The best fix involves placing a technical barrier between the wireless network and the normal wired network. This provides only a partial solution that leaves the wireless network in a compromised state, though it protects against the worst of the attack class Cigital discovered. Further risks can be mitigated through advanced design of any and all software applications that make use of the wireless network.

For more, see:
http://www.cigital.com/news/wireless-sec.html
http://www.cigital.com/news/wireless/faq.html

Category 24.5 *LAN OS*

2003-01-09 **protocol vulnerability note CERT IEE 802.3 Ethernet information leakage**

NIPC/DHS

January 06, CERT/CC — CERT Vulnerability Note VU#412115: "Network device drivers reuse old frame buffer data to pad packets".

The Ethernet standard (IEEE 802.3) specifies a minimum data field size of 46 bytes. If a higher layer protocol such as IP provides packet data that is smaller than 46 bytes, the device driver must fill the remainder of the data field with a "pad". For IP datagrams, RFC1042 specifies that "the data field should be padded (with octets of zero) to meet the IEEE 802 minimum frame size requirements." Researchers from @stake Inc., a digital security company in Cambridge, Mass, have discovered that, contrary to the recommendations of RFC1042, many Ethernet device drivers fail to pad frames with null bytes. Instead, these device drivers reuse previously transmitted frame data to pad frames smaller than 46 bytes. This constitutes an information leakage vulnerability that may allow remote attackers to harvest potentially sensitive information. Depending upon the implementation of an affected device driver, the leaked information may originate from dynamic kernel memory, from static system memory allocated to the device driver, or from a hardware buffer located on the network interface card.

Category 24.5 *LAN OS*

2003-06-13 **windows 2003 server third-party device drivers TCP transmissions Chris Taget NGS data leakage**

NIPC/DHS

June 13, vnunet — Flaws expose Win Server 2003.

Several third-party device drivers that ship with Windows Server 2003 contain a vulnerability that causes them to leak potentially sensitive data during TCP transmissions. Security experts have criticized many of the vendors for failing to act quickly enough to guide users to fixes, and warned that the flaw could lead to attacks through local area networks (LANS). The so-called Etherleak flaw, first identified in January, occurs when messages transmitted between two machines are padded with arbitrary data in order to bring their byte size in line with the accepted standard. Chris Taget of security consultancy NGS Software warned that the vulnerability could be extremely serious and suggested that "IT directors should find out whether their vendors have updated the driver to resolve the issue."

Category 24.5 *LAN OS*

2004-08-09 **RSA Cfengine daemon vulnerability network administration tool fix patch issued**

DHS IAIP Daily;
http://www.coresecurity.com/common/showdoc.php?idx=387&idxse ccion=10

August 09, Core Security Technologies — Cfengine RSA authentication heap corruption.

Cfengine, the configuration engine, is a very high level language for simplifying the task of administrating and configuring large numbers of workstations. Two vulnerabilities were found in cfservd, a daemon which acts as both a file server and a remote cfagent executor. This daemon authenticates requests from the network and processes them. If exploited, the first vulnerability allows an attacker to execute arbitrary code with those privileges of root. The second vulnerability allows an attacker to crash the server, denying service to further requests. Cfservd uses an IP based access control (AllowConnectionsFrom) which must be passed before the vulnerabilities can be exploited. The level of risk thus depends on how this access control is configured. These vulnerabilities are present in versions 2.0.0 to 2.1.7p1 of cfservd. Release 2.1.8 which fixes these vulnerabilities is available from http://www.cfengine.org.

Category 24.5 *LAN OS*

2004-12-06 **Novell NetMail network messaging application protocol NMAP authentication failure**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2004/Dec/1012429.html

December 06, SecurityTracker — Novell NetMail default authentication credentials lets remote user access the mail store.

Novell reported that if the default Network Messaging Application Protocol (NMAP) authentication credentials have not been changed after installation, a remote user can connect to port 689 to gain access to the mail store. A remote user can also send unauthorized messages to other local or remote users. The default NMAP authentication credential is set automatically during installation but should be changed after installation using the nmapcred utility. As a solution, Novell indicates that you should use the NMAP Server Credential Generator (nmapcred) to set a unique NMAP authentication credential. Original advisory: http://support.novell.com/cgi-bin/search/searchtid.cgi?/2970 344.htm

---

Category 24.5 *LAN OS*

2005-01-11 **Novell NetWare CIFS.NLM software denial of service DoS vulnerability update issued**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2005/Jan/1012817.html

NETWARE RUNNING CIFS.NLM. A DENIAL OF SERVICE VULNERABILITY WAS REPORTED IN NETWARE WHEN RUNNING CIFS.NLM

A remote user can conduct a network port scan against the target system to cause the target system to 'hard lock' if the system is running CIFS.NLM at the time of the scan. This creates a denial of service condition. As a solution, the vendor has issued a CIFS update for NetWare 5.1 and 6.0, described at: http://support.novell.com/cgi-bin/search/searchtid.cgi?/2970 488.htm

---

Category 24.5 *LAN OS*

2005-01-26 **Cisco Internetwork Operating System IOS reload vulnerability denial of service DoS update issued**

DHS IAIP Daily; http://www.us−cert.gov/cas/techalerts/TA05−026A.html

MULTIPLE DENIAL-OF-SERVICE VULNERABILITIES IN CISCO IOS

Several denial-of-service vulnerabilities have been discovered in Cisco's Internet Operating System (IOS). A remote attacker may be able to cause an affected device to reload the operating system. Although the underlying causes of these three vulnerabilities is different, in each case a remote attacker could cause an affected device to reload the operating system. This creates a denial-of-service condition since packets are not forwarded through the affected device while it is reloading. Repeated exploitation of these vulnerabilites would result in a sustained denial-of-service condition. Since devices running IOS may transit traffic for a number of other networks, the secondary impacts of a denial of service may be severe. Cisco has updated versions of its IOS software to address these vulnerabilities. Additional information is available on the US-CERT Website.

24.6 WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2001-04-03 **802.11 wireless local area networks bug flaw vulnerability eavesdropping spoofing man-in-the-middle attack**

NewsScan

FLAW IN STANDARD FOR LOCAL WIRELESS NETWORKS
Computer science researchers at the University of Maryland have found new security flaws in the 802.11 wireless standard used in many local area wireless networks deployed in corporations and in public areas such as airports and cafes. Researchers from Intel and the University of California at Berkeley had previously found weaknesses in the standard. William A. Arbaugh, in the Maryland group, said: "We're seeing a great proliferation of wireless activity now in products, and people have not paid close enough attention to security issues. When we began looking at this I was flabbergasted by what I found." The newly discovered flaw might be used by someone physically close to private wireless computer network to masquerade as a legitimate user. (New York Times 3 Apr 2001)
http://partners.nytimes.com/2001/04/03/business/03FLAW.html

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2001-05-03 **wireless network interception intrusion spam penetration e-mail**

RISKS 21 39

Thor Lancelot Simon commented on a bad implementation of wireless network access in a report in RISKS:

>A local university has deployed a large 802.11 wireless network without WEP or any other security measure. Given the complexity of distributing WEP keys to huge numbers of students, faculty, and staff, not to mention the need for periodic changes, and the notorious insecurity of WEP itself, this might seem to be a reasonable choice. They have decided to provide public access to their IP connectivity for those within radio range of their campus rather than tackle the very significant issues associated with restricting access.

The RISK? Their campus mail-handling machines will relay mail to any inside or outside destination if it's received from an address "inside" their campus network. The network architecture they've chosen for their wireless deployment dictates that anyone can walk onto their (large, urban) campus, or even just park his car outside, and spam away freely with hundreds of megabits per second of bandwidth to most points on the Internet.

Basically, their entire campus just became a "safe harbor" for anyone owning a laptop and wireless card to do nefarious things to outside hosts with, essentially, perfect, impenetrable anonymity. There's not even a billing record for a throwaway dialup account to trace back; just a MAC address that can be trivially changed and the knowledge that it was used *somewhere* on their campus to do Bad Things at some point in the past.<

In a followup posting to RISKS, Danny Burstein confirmed by direct experimentation that fears of abuse were perfectly justified. Burstein wrote, "Furthermore, any mail coming through them will have an envelope indicating it came from a well known and trusted source. Meaning not only would people be more likely to let it through their filters (whether computerized or the Mark One Eyeball method of glancing at the 'from' and 'subject' line), but they're also far more likely to open it."

In addition, wrote Burstein, "Getting back to spamming: this system doesn't block outgoing 'port 25' access, meaning a spammer could set up their own mail server and pseudo-anonymously engage in all sorts of socially deviant activities."

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2001-06-07 **wireless communications interception Bluetooth**

NewsScan

PALM TO GET BLUETOOTH WIRELESS LINKS
New expansion cards will allow Palm m500 and m505 handheld computers to use Bluetooth short-range wireless technology to communicate with Bluetooth-enabled printers, mobile phones, and other devices. The cards will be priced below $150. (San Jose Mercury News 7 Jun 2001)
http://www.siliconvalley.com/docs/news/svfront/023533.htmg

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2001-08-12 **wireless communications Internet access confidentiality vulnerabilities**

NewsScan

WIRELESS INTERNET SPARKS SECURITY CONCERNS
Business travelers plugging into wireless Wi-Fi networks now found in airports and coffee shops should beware -- those networks can easily be intercepted, according to security experts. "When you sit in an airport and use your laptop you might as well be broadcasting to anyone within listening distance," says a digital forensics specialist with Predictive Systems. No special software is required to intercept data off a Wi-Fi network, and eavesdropping on other's e-mail exchanges is easy to do, says one security expert. "Everyone who is touching the Internet should know that it is wide open to everyone," says MobileStar chief technology officer Ali Tabassi. "People should think of it as a pay phone or a cell phone, in a public place." (AP 12 Aug 2001)
http://news.cnet.com/news/0-1004-200-6853688.html?tag=mn_hd

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2001-08-19 **wireless network intrusion penetration confidentiality eavesdropping WEP 802.11 WiFi medical informatics privacy integrity safety**

RISKS 21 62

Cryptographer Avi Rubin demonstrated the weakness (or absence) of wireless network security in a hospital in Morristown, NJ. Peter G. Neumann of RISKS summarizes what happened: ". . . Avi Rubin . . . noticed that his laptop wireless connection card was blinking, and then discovered that the hospital's wireless network was open to his laptop, using 802.11b (Wi-Fi) and automatically granting him access. . . ."

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2001-11-06 **wireless security penetration firewall encryption**

NewsScan

DRIVE-BY HACKING
An experiment conducted by BBC Online found that the "wifi" (wireless) computer networks in London's financial center have serious security gaps that would allow network vandals to drive, pedal a bike, or walk through the streets and pick up information from the networks almost at will. The problem will only be solved when companies take security seriously and protect wireless networks behind a firewall that allows only encrypted, authenticated traffic to pass from a wifi network to a wider corporate network. (BBC News 6 Nov 2001
http://news.bbc.co.uk/hi/english/sci/tech/newsid_1639000/1639661.stm

---

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2002-01-25 **wireless tunneling firewall network workstation**

RISKS 21 89

Jeremy Epstein noted in RISKS that, "Wireless carriers including Sprint, Cingular, and Seven (a startup) are putting together products that tunnel through the firewall to allow you to access the e-mail, calendars, etc. on your desktop machine remotely from a wireless device. . . . "
http://www.infoworld.com/articles/hn/xml/02/01/28/020128hnport.xml

---

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2002-01-28 **wireless networks Wi-Fi vulnerability implementation installation problems weakness ban**

NewsScan

WIRELESS TECHNOLOGY CRITICIZED FOR VULNERABILITIES
Lawrence Livermore National Laboratory in California has banned all wireless networks, including Microsoft's Wi-Fi, because of security concerns. Wi-Fi supporters say the technology is secure when it's been properly installed, but experts say that only about 10% of all users install them correctly. (USA Today, 28 Jan 2002)
http://www.usatoday.com/life/cyber/tech/2002/01/29/wifi.htm

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2002-02-20 **wireless security Wi-Fi 802.1X protocol weakness man-in-the-middle attack hot spots session hijacking**

RISKS, http://www.pcworld.com/news/article/0,aid,84424,00.asp 21 92

Prof. William Arbaugh and graduate student Arunesh Mishra of the University of Maryland published a paper entitled, "An Initial Security Analysis of the IEEE 802.1X Standard" in which they demonstrated specific methods of session hijacking in the Wi-Fi protocol. Hijacking involves monitoring the authentication process and then sending a forged "disassociate" message apparently from the access point. The attacker then continues using the established session while the original user simply assumes there's been a communications error and establishes a new connection.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2002-03-14 **hacking tools cost ease wireless networks eavedropping**

RISKS, http://news.bbc.co.uk/hi/english/sci/tech/newsid_1860000/1860241.stm 21 96

Wireless networks can be hacked easily, in part using directional antennas made from discarded Pringles potato-chip tubes.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2002-04-01 **satellite radio wireless communications interference jamming Wi-Fi frequencies**

NewsScan

SATELLITE RADIO OPERATORS COMPLAIN ABOUT WI-FI INTERFERENCE
XM Satellite Radio and Sirius Satellite Radio have petitioned the FCC to regulate Wi-Fi technology more closely, threatening to stymie innovation in the nascent wireless technology market. The satellite radio broadcasters say that even though Wi-Fi operates on a different frequency, the frequencies are so close that it's possible for energy to leak over from Wi-Fi devices and interfere with their services. They're asking the FCC to set limits on the services, although they say they're not trying to shut them down. "I think wireless devices are going to blossom," says Sirius co-founder Robert Briskman, who says Wi-Fi device manufacturers could alleviate the problem by installing filters and making other changes to wireless transmitters. Wi-Fi advocates say their systems comply with current FCC rules and that if the satellite radio folks are worried about interference, they should tinker with their own systems. Meanwhile, FCC Chairman Michael Powell is keeping mum on the satellite proposals, but has cautioned that heavy usage of Wi-Fi and other devices that use unlicensed frequencies could eventually cause a "meltdown." (Wall Street Journal 1 Apr 2002)
http://online.wsj.com/article/0,,SB1017613134883515920.djm,00.html (sub req'd)

XM, DELPHI TEAM UP ON PORTABLE SATELLITE RADIO DEVICE
XM Satellite Radio and auto parts maker Delphi unveiled their Delphi XM SKYFi Radio receiver -- a pocket-sized portable device that enables listeners to tune into XM's satellite radio channels using a home stereo system or a portable boombox. The device, which will be available in stores next month, will be priced around $130. The kit to connect it to a home or car stereo will retail for around $70. XM says it's received orders from retailers for between 120,000 and 150,000 units and expecting brisk sales through the holiday season. The company is hoping to have 350,000 subscribers by the end of the year. (Reuters 25 Sep 2002)
http://makeashorterlink.com/?H27252BE1

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2002-04-11 **Radio Frequency Identification Tags REIG Electronic Product Code ePC privacy wireless communication**

NewsScan

THINGS COME ALIVE
We're just at the beginning of a new age of products, devices and objects that talk to us -- and to each other. "We're really talking about the next 50 years of computing," says the executive director of the Auto-ID Center at MIT, which is one of the organization studying ways of using computer chips embedded in tiny pieces of plastic attached to just about everything, including egg cartons, eyeglasses, books, toys, trucks, and money. The tags are currently known as Radio Frequency Identification Tags (REIG), and the Auto-ID Center calls the core of its standard "ePC" or Electronic Product Code. Companies such as Wal-Mart, Gillette, and Procter & Gamble have committed to using the technology. As for privacy issues? Accenture scientist Glover Ferguson agrees that privacy will be an issue, and says: "There will have to be a social discourse about what we want and don't want. But the technology isn't going away. You can't un-invent it." (USA Today 11 Apr 2002)
http://www.usatoday.com/life/cyber/tech/2002/04/12/tinyband.htm

---

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2002-05-23 **wireless cash registers hackers theft fraud penetration eavedropping**

RISKS; http://www.msnbc.com/news/746380.asp 22 09

According to a report by Bob Sullivan of MSNBC, several large retail stores, including Best Buy, Walmart and Home Depot are using unencrypted traffic over wireless point-of-sale devices. Experimenters (perhaps more usually known as "hackers") monitoring traffic from parking lots at the stores claimed to have picked up sensitive data such as customer credit-card numbers in transit.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2002-06-12 **Wi-Fi wireless ISP Internet service provider**

NewsScan

EARTHLINK TO OFFER WI-FI SERVICE
EarthLink is marketing its "EarthLink Wireless High Speed" service to customers eager to take advantage of about 650 Wi-Fi networks in coffee shops, hotels, airports and other public spaces throughout the country. The deal makes EarthLink among the first traditional ISPs to sell services based on the Wi-Fi wireless networking standard. Analysts say many ISPs are interested in selling Wi-Fi services, but have been waiting on the sidelines for heavyweights, like EarthLink or AOL, to make the first move. "This is what people have been waiting for: stronger backing by service providers," says an analyst with Synergy Research Group. EarthLink's service is offered in conjunction with Wi-Fi networking firm Boingo Wireless, a startup headed by EarthLink founder Sky Dayton. EarthLink customers will use Boingo's networks, and have the option of buying access in 24-hour chunks, during which they can log on and off as many times as they choose. A single "day pass" costs $8, or customers may purchase a package of 10 "day connects" for $25. (CNet News.com 11 Jun 2002)
http://news.com.com/2100-1033-935034.html?tag=fd_top

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2002-07-25 **broadband services sharing piracy contract wireless**

NewsScan

BROADBAND PROVIDERS CRACK DOWN ON 'SHARING'
Broadband providers are not looking kindly on some subscribers' hobby of "sharing" their high-speed connections with friends and neighbors who pay nothing. Time Warner Cable recently sent letters to 10 subscribers in New York giving them three days to cease their sharing activities, and threatening to cut off their service if they failed to do so. "When you contract for high-speed access, it's for your use in your household and not to share with neighbors," says a Time Warner spokeswoman. Meanwhile, AT&T Broadband also plans to contact connection-sharing users. In both cases, subscribers need simply to install an antenna on the roof of their house, which enables up to 50 people to use the connection. The signal can travel as far as 20 miles. (Investor's Business Daily 25 Jul 2002 -- print only)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2002-08-12 **wireless Wi-Fi standard telecommunications Internet access**

NewsScan

IS WI-FI THE FUTURE OF TELECOM?
Working with Athens, Georgia, to develop a wireless communications "cloud" over the city's downtown, Scott Shamp, the director of the University of Georgia's New Media Institute, says: "We're designing a sandbox. We want a place where people can experiment... This feels like the Internet from 1994." Will Wireless Fidelity (or WiFi) networks, based on the technical standard 802.11b, provide competition for the large telecom companies? Not just yet, but experts such as MIT Media Laboratory director Nicholas Negroponte recently told a Congressional committee that the telecom industry may not recover its former market value, because in the future "we're going to use telecommunications very differently." Wireless clouds can support a new generation of technology, including always-on portable digital devices and environmental sensors. The hope of WiFi enthusiasts is that the low-cost, grass-roots technology will grow "organically" into a nationwide communications system. (AP/San Jose Mercury News 12 Aug 2002)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2002-09-11 **Wi-Fi roaming sharing network ISP Internet service provider penetration wireless communications e-commerce billing payment**

NewsScan

WI-FI FANS WANT TO ROAM
The popularity of Wi-Fi — the wireless networking technology that broadcasts an Internet connection over a radius of 300 feet — is spawning efforts to expand the service so that customers of one wireless provider could use the network of another. The barrier lies not in the technology, but in the billing technicalities. "The bits, the bytes and the hardware exist for roaming. We just need someone to start pulling it all together," says Barry Davis, Intel's director of platform architecture. And while a technical standard isn't required to create roaming capability, there is industry pressure on the IEEE (Institute of Electrical and Electronic Engineers) and the ETSI (European Telephone Standards Institute) to agree one, because it would cut costs and help jumpstart the development of future Wi-Fi technology. Meanwhile, some Wi-Fi carriers are teaming up on their own: Boingo Wireless, the second-largest U.S. carrier, has already established roaming agreements with two other wireless providers and is looking for more. In Europe, a number of companies, including Swiss carrier Monzune, are testing Wi-Fi roaming, and in Japan, Multimedia Mobile Access Communication Systems has created its own wireless roaming standard. "The Asian market is getting faster adoption, and the Europeans are next in line," says John Baker, CEO of Transat, which makes software that enables Wi-Fi roaming. (CNet News.com 10 Sep 2002)
http://news.com.com/2102-1033-957411.html

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2002-09-13 **wireless cellular mobile phone peer-to-peer P2P networking picture music**

NewsScan

TECHNOLOGY TURNS WIRELESS NETWORK INTO P2P PLAYGROUND
Apeera, based in France, has developed a technology that enables mobile phone users to set up an unlimited digital storage "cabinet" for their own media files and allows them to share the files with other cell phone users. Apeera's creators say the system could prove popular with wireless carriers eager to convert customers into multimedia services subscribers. "Peer-to-peer is the cornerstone of making a service successful," says an Apeera spokesman. "Logos and icons are going to become pictures, ringtones are going to become music files." Apeera users can send files to any WAP- or Java-enabled phone, even if the recipient isn't signed up for the Apeera service. (BBC News 12 Sep 2002)
http://news.bbc.co.uk/1/hi/technology/2253185.stm

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2002-09-30 **wardriving wireless law enforcement scanning security vulnerabilities commercial networks**

NewsScan

WIRELESS 'WARDRIVING'
Secret Service agents in Washington are driving the city's streets (in an effort called "wardriving") to detect security holes in wireless communications systems. Special Agent Wayne Peterson says, "Everybody wants wireless, it's real convenient. Security has always been an afterthought." He regards what he is doing as a normal part of police work, and compares it to a patrolman driving through a neighborhood to make sure everyone is safe. When he or his colleagues find a security gap, they report it to the companies that operate the vulnerable wireless networks, so that the problem can be fixed. The Secret Service calls security holes in wireless communications systems one of the most overlooked threats to computer networks. (AP/San Jose Mercury News 30 Sep 2002)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2002-10-30 **wireless ISP Internet service provider**

NewsScan

WIRELESS BROADBAND MAKES SPLASH
A new wireless Internet service provider is offering its customers speeds up to 20 times faster than typical dialup services using the CDMA20001xEV-DO standard. By November, Monet Mobile Networks plans to offer its Monet Broadband service in cities in North Dakota, South Dakota and Wisconsin. EV-DO, as it's nicknamed, offers downloads at speeds up to 2.4Mbps, and leading wireless carriers Verizon Wireless and Sprint PCS may be considering building EV-DO networks by 2005. Both companies now use the CDMA standard, which is adaptable to the faster version. Verizon says it is already testing EV-DO networks in San Diego and Washington, DC. Meanwhile, Monet plans to focus its business strategy on bringing broadband Internet access to rural areas, which typically are underserved. "We've received tremendous welcome by these communities which have been overlooked by most of the technology sector," says a Monet spokesman. For $40 a month, Monet subscribers get unlimited Web access, three e-mail addresses and 5MB of data storage. An alternative plan offers five accounts and 25MB of storage for $60 a month. (CNet News.com 29 Oct 2002)
http://news.com.com/2100-1033-963808.html?tag=fd_top

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2002-11-13 **wireless tokens I&A identification authentication tracing monitoring surveillance radio**

NewsScan

THE FUTURE OF COMPUTING WILL BE INVISIBLE
Computing power will be easier to harness as it pervades every corner of our lives, and at the same time will be increasingly transparent, according to an annual technology forecast from PriceWaterhouseCoopers. The proliferation of printable, low-power, short-range radio ID tags will imbue many formerly dumb household appliances with "smart" computing power. Alongside these developments will go efforts to hide the difficulties of tying these devices together and managing large numbers of networked computers, phones or gadgets. "Users do not want to see that complexity," says PWC analyst Kevin Findlay. Meanwhile, businesses will discover the power of in-house grid computing, which from time to time could give a pharmaceutical firm, for instance, the processing power of a supercomputer, just by linking their own idle desktop machines. Findlay also noted that companies likely will move toward renting data storage as they need it, rather than buying it and having it sit idle. (BBC News 13 Nov 2002)
http://news.bbc.co.uk/1/hi/technology/2449009.stm

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2002-11-18 **Wi-Fi wireless communications ISP Internet service provider**

NewsScan

IS WIRELESS THE NEXT GREAT THING?
Life goes on even in a downturn, and there's always the next great thing around the corner. Many people now thing that next great thing will be Wi-Fi, the wireless Internet-access technology that allows anyone with an enabled computing device to connect to the Internet at high speeds and offers "location aware" communications capable of such tricks as showing you where the closest restaurant or movie theater is. The impact of wireless communications will be huge, both on business and on the way we live. Leslie L. Vadaz of the Intel Capital investment unit says, "There is no question in my mind that wireless 'bitways' will make the traditional communications business obsolete." And Ken Biba of the wireless communications company Vivato adds: "This feels like the opening of the PC era when for the first time you could own your own computer. With Wi-Fi you can own your own communications. That's a profound social change." (New York Times 18 Nov 2002)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2002-11-22 **Wi-Fi wireless ISP Internet service providers growth**

NewsScan

WI-FI REACHING MAINSTREAM
Verizon's announcement yesterday that it will install Wi-Fi wireless Internet technology for small and medium-size businesses is the latest sign that Wi-Fi is becoming a mainstream communications technology. Recently, T-Mobile and Boingo Wireless made similar moves, though Yankee Group analyst Sarah Kim characterized Verizon's position as "arguably in the forefront." Still, the big phone companies in countries such as South Korea, the United Kingdom, Sweden and Japan have been quicker to embrace Wi-Fi and install it to create wireless "hotspots" in public locations such as stores, cafes, airports and hotels. (AP/USA Today 22 Nov 2002)
http://www.usatoday.com/tech/news/digest.htm

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2002-12-05 **wireless networks Internet access growth Wi-Fi**

NewsScan

WI-FI: BIGGER THAN BUDWEISER?
To illustrate his vision of the future of Wi-Fi wireless networking, Wi-Fi Alliance chairman Dennis Eaton told attendees at the 802.11 Planet Conference that "We're looking at Budweiser potential, going forward." Citing revenue expectations of about $2 billion this year, Eaton estimated that profits related to the wireless networking industry will grow at a compounded rate of 30% through 2006, surpassing revenue estimates of household products such as Budweiser beer, which will bring in about $5 billion this year. Eaton says Wi-Fi's ability to complement other emerging technologies, such as broadband and next-generation cellular networks, will boost its growth, but the major obstacles in the industry remain consumer education about what wireless networking can do, what sort of transfer rates and range can be expected, and which standards are compatible. (CNet News.com 4 Dec 2002)
http://news.com.com/2100-1033-976076.html?tag=fd_top

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2003-01-09 **wireless Internet LAN networking WiFi Denver airport tested secured**

NIPC/DHS

January 06, Computerworld — American Airlines secures wireless LANs in Denver.

Last January it was discovered that the wireless local area networks (LANs) American Airlines Inc. had been operating at their Denver International Airport (DIA) terminal were highly vulnerable to hackers. White Hat Technologies Inc., a Colorado-based security firm, found they had been operating without any encryption and had even pasted the IP addresses of curbside terminals on the monitors. A test at DIA on December 20 by White Hat was unable to detect a single airline wireless network operating without encryption protection, said Thubten Comerford, CEO of White Hat. In addition, American had not only removed the IP addresses from its OneStop self-service kiosks, but it had also added Cisco Systems Inc.'s Lightweight Extensible Authentication Protocol (LEAP) authentication technology on top of the standard 40-bit Wired Equivalent Privacy (WEP) encryption. LEAP is an authentication algorithm that leverages the 802.1x framework and provides dynamic, per-user WEP keys to protect data in transit. On the downside, Comerford said the recent test of the DIA facility still managed to pick up a suspected rogue access point (AP), as well as a significant number of vulnerable wireless transmissions emanating from public traveler lounges and frequent-flier clubs throughout the airport. "The biggest danger at DIA is the sniffing of sensitive information being transmitted by travelers. Few, if any, airports have addressed this security vulnerability, [and] few airports or airlines warn travelers of the danger of using the wireless networks," Comerford said.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2003-01-15 **wireless WiFi technology security implications concerns**

NIPC/DHS

January 14, Government Computer News — Spread of handheld devices raises security questions.

Wireless security is a major concern for agencies that deal with ever-more tech-savvy employees bringing to work handheld devices that don't mesh with federal security guidelines, said CDW Government Inc. president James R. Shanks. As agencies are working to bolster network security, the proliferation of wireless devices is raising new security challenges, said Shanks. The potential mobilization of military troops for a war with Iraq is "adding fuel to the fire," Shanks said. Meanwhile, agencies also are working to merge a vast range of applications for use on wireless devices and figure out how to manage the applications from central servers. Some companies that develop wireless software have met with standards writers to better align their products to meet federal and commercial security needs, said Larry S. Kirsch, senior vice president of CDWG. And a few companies have begun to pitch products that inventory and update network administrators when any user taps into the server via a wireless device.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2003-01-15 **cellular mobile telephone Wi-Fi networks**

NewsScan

COMPANIES SEEK TO LINK CELLULAR, WI-FI NETWORKS
A triad comprising Avaya, Proxim and Motorola is developing a mobile device capable of roaming between cell phone networks and Wi-Fi hotspots. "Our vision is to connect the various spaces, be they public hotspots, private hotspots or office networks," says Motorola official Bo Pyskir. Wi-Fi networks have a range of about 300 feet and offer transmission rates of up to 11mbps, while cellular networks cover enormous distances, but crawl at less than 56kbps when sending data like e-mail or Web pages. The effort currently underway at the three companies includes development of a Motorola phone that uses both Wi-Fi and cell phone networks, networking equipment and software from Avaya, and a new kind of Wi-Fi access point from Proxim. Early trials of prototypes are expected to start sometime in the second half of this year, with a commercial release in about 12 to 18 months. (CNet News.com 14 Jan 2003)
http://news.com.com/2100-1033-980582.html

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2003-01-29 **wireless Bluetooth cellular mobile telephones**

NewsScan

HYPERTAG SYSTEM LINKS CELL PHONES TO BILLBOARD ADS
Hypertag, based in Cambridge, England, has developed cheap, smart tags that can beam Web site links to mobile phones, giving passersby additional information about the poster, billboard or shop to which the tag is attached — for instance, links could lead to descriptions of historic monuments or exhibits in a museum, or contact information for products advertised on an outdoor kiosk. Hypertag CEO Jonathan Morgan says 40% of modern cell phones can already accept information sent via infrared technology, and added that his company was also working on a Bluetooth version , which would transfer data via short-range radio link. Many wireless firms see location-based information services as a potentially lucrative revenue stream, but the technological limitations of such systems are still being overcome. "The granularity of GPS and cell-ID is rather large," says Morgan, "and you have to have a lot of infrastructure behind it to make it work." By contrast, the Hypertag system is cheap to use ("It is just like using a remote control on the TV," says Morgan) and the tags can be attached to ads adjacent to each other without muddling the data streams. (BBC News 26 Jan 2003)
http://news.bbc.co.uk/1/hi/technology/2687179.stm

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2003-02-27 **Wi-Fi wireless networks consumer hotels**

NewsScan

MARRIOTT, INTEL CUT DEAL FOR WI-FI ACCESS IN HOTELS
Marriott International and Intel are launching a joint marketing campaign to promote the availability of Wi-Fi access at 400 Marriott, Renaissance, Courtyard, Residence Inn and other hotels. "Customers are making decisions about where they stay based on where this technology is available," says Lou Paladeau, Marriott VP in charge of technology development. "If you don't have it, you're not getting them in the door." Wi-Fi hotspots will be located in lobbies, meeting rooms, and other public spaces. Guests will pay $2.95 for the first 15 minutes of service, and 25 cents a minute thereafter. Marriott estimates that 10% of its guests have Wi-Fi capability. About 19% of laptops sold last year came with Wi-Fi circuitry included, according to IDC, which estimates that percentage will grow to 91% by 2005. (Wall Street Journal 27 Feb 2003)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2003-03-03 **Department Homeland Security DHS wireless security ISAC analysis**

NIPC/DHS

February 28, Government Computer News — Wireless security on DHS agenda.

Four groups in the Information Sharing and Analysis Center (ISAC) for the information and communications sectors, a public-private security forum, are meeting to evaluate commercial wireless security. The Cellular Telecommunications Industry Association (CTIA), Telecommunications Industry Association, Information Technology Association of America, and United States Telecom Association, have begun meeting with the National Infrastructure Simulation and Analysis Center and other Energy organizations, said Kathryn Condello, vice president of operations for CTIA. The ISAC currently has no industrywide way to review security gaps in the networks and services of wireless carriers. But that's just what the Department of Homeland Security will likely need to know to toughen security as more government employees adopt mobile devices and agencies integrate wireless platforms into their programs. Individual companies "know what their problems are," said Condello, who spoke yesterday on a panel about asset security at the Armed Forces Communications and Electronics Association's homeland security conference. But expanding individual assessments to a competitive telecom market with a half-dozen major carriers, each operating its own distinct network elements, is "really tough," Condello said. "That's a lot of data points."

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2003-03-11 **WiFi wireless ISP Internet service provider**

NewsScan

MCDONALD'S JUMPS ON WI-FI BANDWAGON
McDonald's announced ten stores in Manhattan will begin offering one hour of Wi-Fi high-speed Internet access to anyone who buys a combination meal, and plans to extend the program to 300 McDonald's restaurants in New York, Chicago and a yet-unannounced California town. "You can come in and have an extra value meal and send some e-mail," says a McDonald's spokeswoman. McDonald's joins more than 400 Borders bookstores, hundreds of hotels and a couple of U.S. airports where Wi-Fi access will be available by summer. (AP 11 Mar 2003)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2003-03-13 **Wi-Fi wireless ISP Internet service provider**

NewsScan

WI-FI SEAL OF APPROVAL
The Wi-Fi Alliance, a trade group whose members include a number of major technology companies (Cisco, Dell, Intel, etc.) is putting a Wi-Fi logo ("Wi-Fi" stands for wireless fidelity) at places where the network card of any kind of laptop will be able to connect reliably to the network. Wi-Fi Alliance board member Andrea Vocale, a Cisco executive, says: "The pervasiveness of Wi-Fi is what it's about. We want the experience to be the same, with one standard everywhere." The Wi-Fi Alliance's site is http://www.wifizone.org. (AP/San Jose Mercury News 13 Mar 2003)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2003-03-17 **Wi-Fi ISP Internet service provider**

NewsScan

PAYPHONES SEEK NEW LIFE AS INTERNET TERMINALS
Bell Canada is in the midst of a pilot program that offers customers in Toronto, Montreal and Kingston free Wi-Fi Internet access through hotspots originating in 16 former payphone booths located in airports, hotels, libraries, train stations and other public transit locales. As with regular Wi-Fi access, customers must be within 100 feet of the booth to use the signal. Bell Canada spokesman Don Blair says the company has received positive feedback so far: "We've received phone calls and e-mails from people using the service. The are very positive responses from users, as well as a lot of calls from location providers — people wanting to offer (wireless Internet) hotspots to their customers." Meanwhile, in Singapore, InfiniTech has a different idea for resuscitating the payphone booth. The company is looking for U.S. partners to help roll out booths where people could recharge their cell phones when their batteries run down. Users would deposit coins and then recharge their phones. (Wired.com 17 Mar 2003)
http://www.wired.com/news/wireless/0,1382,58050,00.html

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2003-03-27 **wireless Wi-Fi network communication infrastructure unguarded protection**

NIPC/DHS

March 26, Government Computer News — Wireless infrastructure goes unguarded.

The national wireless infrastructure "is one of the most important and least protected parts" of U.S. communications capability, a technology strategist said today. David Porte, an executive with technology incubator Astrolabe Innovations of Cambridge, Mass., said the World Trade Center attacks on September 11, 2001, were a case in point. Porte spoke at a Newport, R.I., conference sponsored by the National High-Performance Computing and Communications Council. The trade center towers housed hubs for multiple types of communications, he said: broadcast, land-line telecommunications and cellular phones. Yet when the towers fell, "cell phones became the primary means of national security communications," Porte said. The result was widespread congestion with a ripple effect that ended in loss of many communications spokes, he said. Lack of wireless interoperability also interfered with government communication in that crisis. The wireline infrastructure, although the first to go down on September 11, "was the first to recover because of built-in redundancy," he said. Porte encouraged greater density of cells and wireless hubs, saying, "Government and industry need to get wireless ready for emergencies."

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2003-04-09 **802.16 Wi-Fi wireless technology vendor support**

NewsScan

NEW WIRELESS STANDARD BUILDS SUPPORT
A new wireless standard — 802.16 — is gaining support, with Intel, Proxim and Fujitsu announcing yesterday they'd joined an industry group called WiMax, which is charged with helping to certify equipment based on the new standard. Unlike the increasingly popular WiFi standard, which is generally limited to a 300-foot radius from the base station antenna, 802.16 technology has a range of more than 31 miles. That means it can be used to extend broadband access to rural and remote locations that currently aren't served. "We believe it's the next big thing in the wireless broadband arena," says Margaret LaBrecque, president of WiMax and an Intel manager. WiMax says its goal is to ensure that 802.16 equipment from different companies will be able to communicate with each other. Analysts expect products using 802.16 to be available during the second half of 2004 and carriers may introduce high-speed Internet service based on the standard in 2005. (Wall Street Journal 9 Apr 2003)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2003-04-15 **UPS tracking multiple protocols networks**

NewsScan

UPS DEVICE CONNECTS SIX WAYS
United Parcel Service is giving its drivers new handheld devices that connect to six different wireless networks. The Delivery Information Acquisition Device (DIAD) connects via infrared, WiFi, Bluetooth, GPS, and two cell networks: CDMA1x and GSM/GPRS. "It reminded me of 'shock and awe,'" says telecom analyst Jeff Kagan. "There are just so many different kinds of weapons, tools and technologies." A UPS manager says the handheld's battery, which is about the same size as a typical laptop battery, has enough power to last through normal workday because a driver likely would use only two connections at a time — for instance, using Bluetooth to read a packing slip and then connecting to a cell phone network to send information back to UPS headquarters. (CNet News.com 15 Apr 2003)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2003-04-28 **WiFi technology compete cellular wireless phone**

NewsScan

WHY WIFI WON'T COMPETE WITH CELLULAR ANYTIME SOON
Business Week columnist Andy Reinhardt says despite the recent buzz over WiFi technology, there are fundamental limitations that will restrict its ability to break into the voice communications market. "Just look at roaming. In the mobile world, a fantastically complex system of databases and electronic billing is completely hidden from consumers, whose handsets magically switch from one network to another as they move around. Not so for WiFi, where going online from an unfamiliar hot spot is no easy feat. WiFi will definitely siphon off some of the revenues the Bell-heads [traditional phone companies] want to score from mobile data. But as long as users have to fiddle with Internet protocol settings and quirky, unpredictable connections, WiFi will remain a niche occupied by the technoscenti." (Business Week Online 28 Apr 2003)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2003-05-08 **Wi-Fi security violators LAN hacker virus attacks Delaware Department Technology sniffer software**

NIPC/DHS

May 08, Washington Technology — State CIO hunts for Wi-Fi security violators.

The new Delaware Department of Technology and Information has employed sniffer software to see whether state agencies have deployed wireless fidelity, or Wi-Fi, networks that meet state standards for such networks. Each month the department checks a different location for non-standard, or "illegal," use of a Wi-Fi local area network. During the course of one such check, the department discovered a serious violation, Delaware Chief Information Officer Tom Jarrett Jarrett said "I told the agency to cease and desist or in two days I would take them off the network." Because the agency was "running wide open" with Wi-Fi, they were putting the entire network community at risk from hacker and virus attacks, he said.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2003-05-20 **GPS data stop wireless attacs Yi-Chi Hu Adrian Perrig Carnegie Mellon wormhole Ad-Hoc networks**

NIPC/DHS

May 20, New Scientist — GPS data could stop wireless network attacks.

U.S. computer researchers Yi-Chin Hu and Adrian Perrig of Carnegie Mellon University, PA, and David Johnson at Rice University, TX have revealed that a "wormhole attack" could be used to knock a vulnerable network out of action or defeat a wireless authentication system. "Ad-hoc" wireless computer networks, which are used to extend the range of wireless LAN networks, and are used by the military and emergency services, could be severely disrupted using the technique. But the same researchers have also devised a radical scheme designed to counter it. The researchers propose defending networks against the attack by attaching identifying tags to each packet. They suggest tagging packets with GPS information or a timestamp based on a synchronized network clock. Both could be used to verify that a packet genuinely comes from another nearby node and not one intercepted much further away. The threat and countermeasure are outlined in the paper "Packet Leashes: A Defense Against Wormhole Attacks in Wireless Networks" presented at the Twelfth World Wide Web conference in Bucharest, Romania.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2003-06-18 **IEEE new wi-fi standard 802.11g**

NewsScan

IEEE RATIFIES NEW WI-FI STANDARD
The new 802.11g wireless standard, which has now been approved by the Institute of Electrical and Electronics Engineers (IEEE), is likely to prompt a new surge of interest in WiFi, the technology which uses a radio signal allowing laptops and other mobile devices to connect to the Internet through access points called "hot spots" located in cafes, airports, etc. The 802.11g standard will allow wireless transmission at speeds four to five times faster than the current standard, and make it possible to send bigger files (e.g., videos) and connect more computers to an access point. (Chicago Sun-Times 18 Jun 2003)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2003-06-25 **wireless networking security school password protection**

NewsScan

[WIRELESS]...NEEDS TO BE WATCHED FOR SECURITY BREACHES
Using a laptop with a wireless card outside the main office of a Palo Alto, California school district, a reporter was able to gain access to such data as grades, home phone numbers and addresses, emergency medical information, student photos , and psychological evaluations. Unlike the majority of the district's information, the documents available on this wireless network were not password-protected. Superindent Mary Frances Callan says: "I don't see this as such a huge news story." The real story, says Callan, is the great progress represented by the network itself, which was made possible by new software purchases, employee training sessions, and technology-use policies. (Palo Alto Weekly 25 Jun 2003)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2003-06-26 **pda corporate scheme end user Wi-Fi support bluetooth**

NewsScan

PDAs IN THE CORPORATE SCHEME OF THINGS
Handheld computers are in evidence everywhere in corporate America — yet they typically belong to individual employees rather than to the corporations that employ them. (Gartner Research analyst Todd Kort says that only 28% of all PDA's worldwide were purchased by businesses.) Microsoft is hoping that its new Windows Mobile software for the Pocket PC handheld operating system will bring that percentage up to a much higher level. Gartner's Kort says, "Most of the cool stuff is under the hood. The average end user isn't going to be immediately aware that any kind of major changes have taken place. What they're doing is a lot of things to satisfy IT managers." IT departments "don't want those support calls," so Microsoft has created a new configuration manager for automatically detecting and connecting to Wi-Fi and Bluetooth networks and allowing users to connect wirelessly without having to deal with any complicated configurations or setups — and without having to ask for help. (Information Week 26 Jun 2003)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2003-07-02 **Cisco Systems Aironet flaw access point wireless Vigilante 1100 wi-fi 300 foot radius zone computer network**

NIPC/DHS

July 28, CNET News — Cisco releases fix for Aironet flaw.

Cisco Systems has patches for a pair of security flaws that were discovered in its Aironet 1100 access points. One flaw would have allowed an attacker to use a "classical brute technique to discover account names, according to security troubleshooter Vigilante. said the second flaw could freeze the access point and bring down the wireless access Cisco posted advisories on the flaws Monday, July 28. "To date, Cisco is not aware active exploitations of the vulnerability," a Cisco representative said in a statement. Cisco Aironet 1100 Wi-Fi access point creates a 300-foot radius zone where laptops wirelessly connect to the Web or a corporate computer network. Additional information available on the Vigilante Website: http://www.vigilante.com/inetsecurity/advisories/VIGILANTE-2 003002.htm

---

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2003-07-03 **Wi-Fi encryption eavesdropping AirDefense POP e-mail passwords**

NIPC/DHS

July 03, SecurityFocus — Study: Wi-Fi users still don't encrypt.

Two days of electronic eavesdropping at the 802.11 Planet Expo in Boston last week sniffed out more evidence that most Wi-Fi users still aren't getting the message. Security vendor AirDefense set up two of its commercial "AirDefense Guard" sensors at opposite corners of the exhibit hall at the Boston World Trade Center, the site of the conference. The company provided attendees with ample notice of the study. "There were huge signs throughout the place saying AirDefense is monitoring all conference traffic." They found that users checking their e-mail through unencrypted POP connections vastly outnumbered those using a VPN or another encrypted tunnel. Only three percent of e-mail downloads were encrypted on the first day of the conference, 12 percent on the second day. That means the other 88% could easily be intercepted by eavesdroppers using commonly-available tools, compromising both the e-mail and the user's passwords.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2003-07-31 **Sony Playstation wireless LAN**

NewsScan

SONY'S GAME PLAN
Sony's new handheld PlayStation console will come with wireless capability that allows gamers in close proximity to play together and download game characters. "We will be using some challenging technologies," including wireless LAN (local area network), says Sony Computer Entertainment president Ken Kutaragi. "The PSP is a product with huge potential, following the PlayStation and PlayStation 2. The video game market may change in a big way." The new device, set to debut in the fourth quarter of 2004, will process data at blazing speeds 10 times faster than the original PlayStation console. PSP games will come in the form of high-capacity optical discs created especially for the new device, and the PSP will also be able to play movies and music. The move pits Sony directly against Nintendo, which produces the market-leading GameBoy Advance device. (Reuters/CNet 30 Jul 2003)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2003-08-29 **Wi-Fi ship short transmission radio satellite Internet**

NewsScan

SHIP-TO-SHORE WI-FI
For years, mariners have been reliant on pricey maritime radio and satellite services for connectivity afloat, but Wheat Wireless Services of Reston, Virginia is now selling a tweaked version of Wi-Fi Internet access that is functional up to 30 miles offshore. The boat receiver is a 4-foot antenna, and the Wi-Fi service piggybacks off T1 lines in data centers along the coast beamed from radio towers up to 300 feet tall perched atop coastal structures. The service isn't cheap — it costs $7,500 for installation and another $500 a month for unlimited Internet access — but that's pocket change for wealthy yacht owners and cruise lines, says In-Stat/MDR analyst Daryl Schooler. "Basically, they're delivering more than a T1 worth of bandwidth to people. Satellite is slower than that and could be tens of thousands of dollars a month." Two casino ships have signed up for Wheat's service, but not to provide their passengers with Internet access. "They want people to gamble," says Wheat CEO Forrest Wheat. "They don't want them to surf the Internet. (The Internet service) is for the crew." (Wired.com 29 Aug 2003)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2003-11-07 **wireless Wi-Fi security protocol vulnerability**

NIPC/DHS

November 06, InternetNews.com — Weakness found in Wi-Fi security protocol.

Wireless security expert Robert Moskowitz has detected a glaring weakness in the interface design of a Wi-Fi Protected Access (WPA) protocol deployed in numerous Wireless LAN products. According to a research paper written by Moskowitz, the weakness could allow intruders to crack poorly chosen passphrases via offline dictionary attacks. The paper means that Wi-Fi hardware products that ship with WPA might be less secure than the older Wireless Encryption Protocol (WEP), which it replaced in 2002. The WPA standard was designed to improve upon the security features in wireless networks. The weakness only takes effect when short, text-based keys are used and does not reflect a fault in the WPA protocol. The weakness can be avoided if WLAN hardware manufacturers build units with the ability to generate random keys that can be copied and pasted across systems. Manufacturers can also restrict the ability to enter weak keys by requiring passphrases with numerous characters instead of words that can be found in the dictionary. Moskowitz warned that dictionary based programs used to crack passwords are heavily used by criminal hackers. The paper is available online: http://wifinetnews.com/archives/002452.html

---

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2003-11-21 **Wi-Fi wireless railway operation Burlington Northern Sante Fe**

RISKS; http://www.theregister.co.uk/content/69/34101.html 23 5

US railroad uses Wi-Fi to run 'driverless' trains

Lars Kongshem contributed the following to RISKS:

"The Burlington Northern and Santa Fe Railway Company (BNSF) has found a novel use for Wi-Fi. It has started using the wireless networking technology to control trains remotely. BNSF locomotives carry freight across the continental US. However, it is using wireless technology to move units around its rail yards…. (Drivers) operate a control panel that mirrors what they'd see if they were sitting in the cab. Their instructions are relayed to each loco via the 'industrial strength' WLAN."

Given Wi-Fi's security problems, this novel use of 802.11 certainly gives a new meaning to the word "loco"! [Source: *The Register*, Nov 20 2003]

http://www.theregister.co.uk/content/69/34101.html

[Of course, if they were carrying fruit, it would be PLUM LOCO. PGN]

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2003-12-05 **Cisco Systems wirelss LAN security alert Wi-Fi SNMP vulnerability**

NIPC/DHS

December 04, VNUNet (UK) — Cisco issues wireless Lan security alert.

Cisco has warned firms using its Aironet access points running Cisco IOS operating software of a security flaw that allows hackers to gain full access to wireless networks. The vulnerability allows hackers to steal Wired Equivalent Privacy (Wep) encryption keys. The issue arises if the wireless Lan device's 'SNMP-server enable traps wlan-wep' command is enabled. "Under these circumstances, an adversary will be able to intercept all static Wep keys," Cisco said in a statement. If the command is switched on, which Cisco stressed is disabled by default, the access point will broadcast any network static Wep keys in cleartext to the SNMP server every time a key is changed or access points rebooted. Affected hardware models are the Cisco Aironet 1100, 1200 and 1400 series. Cisco has posted a workaround advising companies with deployments of these devices to disable this command, adding that any dynamically set Wep key will not be disclosed. The problem only applies to wireless Lan kit running its IOS software, so Aironet access point models running VxWorks are not affected. Customers are advised to upgrade their IOS version to a patched system. Cisco's advisory and workaround are available here: http://www.cisco.com/warp/public/707/cisco-sa-20031202-SNMP- trap.shtml

---

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2003-12-19 **wireless Internet test Rutgers WINLAB NSF**

NIPC/DHS

December 17, Rutgers University — Rutgers area to become test track for wireless Internet. The Wireless Information Network Laboratory (WINLAB) at Rutgers, The State University of New Jersey, has won a $5.45 million, four-year grant from the National Science Foundation (NSF) to construct and operate a facility for researchers around the nation to test the next generation of wireless and mobile networks. This wireless networking test bed will include both a large-scale "radio grid emulator" laboratory and a "field trial" system in and around the Rutgers campus and nearby Central New Jersey communities. The project is called the Open Access Research Testbed for Next-Generation Wireless Networks. Rutgers is managing the project in collaboration with Columbia University, Princeton University, Lucent Bell Labs, IBM Research, and Thomson Inc. The two-tiered project will include a new wireless system emulation laboratory to be headquartered at the Technology Centre of New Jersey. An indoor radio grid of about 625 stationary and mobile nodes will give researchers throughout the country remote access for testing of future network concepts under a variety of computer-generated topologies and radio conditions. The field test network will include about 50 nodes running a configurable mix of third generation high-speed cellular, along with wi-fi wireless access.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2004-01-08 **wireless tracking technology licensed Motorola Steve Wozniak**

NewsScan

MOTOROLA LICENSES WOZNIAK'S WIRELESS TRACKING TECHNOLOGY

Motorola is licensing technology developed by Apple co-founder Steve Wozniak's new venture, Wheels of Zeus. The wireless tracking system, dubbed "wOzNet," uses a wireless tag that links to GPS satellites and transmits location information via low-power radio signal. "Let's say you're a parent, you have four kids, and as soon as they hit the amusement park they run in four directions," says Motorola Broadband business development director Vince Izzo. "You could set the thing to let you know if any of them is more than 50 feet away from you." The technology could also enable a parent to monitor a child in the park without going along — the signal could be picked up by a cell phone company or local park operators and transmitted via the Internet to a base station in the parent's home. (AP/USA Today 8 Jan 2004)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2004-01-26 **wireless risks Wi-Fi security threat shared sensitive information**

RISKS 23 16

ANOTHER WIRELESS RISK

Contributor Chris Meadows writes about an experience of his with wireless networking. When at Kinko's, needing print a credit card invoice urgently, Meadows scanned for an available printer on a wireless network. He found an open router called "linksys" which had a Lexmark printer connected to it. Meadows printed his CC invoice on this linksys printer. When he asked the Kinko's clerk where this printer was, the clerk responded, "[B]ut we don't have a wireless network…and we don't have any Lexmark printers either." Meadows had printed his invoice to a "stranger's printer." But Meadows assures us that the invoice contained no really sensitive information, and was closing that account anyway. Commenting on his experience, he says the risk with wireless networking, instead of "you never know who might be using your network," is, "you never know whose network you might be using."

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2004-01-28 **WAN security wireless internet wardriving**

NewsBits; http://insight.zdnet.co.uk/0,39020415,39143769,00.htm

---

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2004-02-03 **NTIA Wi-Fi wireless broadband applications license**

DHS IAIP Daily;
http://www.govtech.net/news/news.php?id=87078&e=1&u=/nm/20040203/tc_nm/tech_microsoft_dc

February 03, Government Technology — NTIA seeks to expand spectrum available for high-speed Internet.

Last week, the National Telecommunications and Information Administration (NTIA) announced it was considering an expansion of the 3650-3700 MHz band to unlicensed devices for wireless broadband applications such as Wi-Fi while protecting federal operations in those bands from interference or other adverse effects. NTIA has invited interested parties to file comments on technical requirements and interference-mitigation techniques necessary for compatible unlicensed device usage in those bands. "We want to make more spectrum available so that people who live in rural areas can have access to wireless broadband," said Acting Assistant Secretary of Commerce Michael D. Gallagher. "This continues our progress in facilitating the sharing of spectrum among government and commercial users." The filing says it appears that "very significant benefits" to the economy, businesses, consumers, and government agencies can be gained by allowing unlicensed devices to operate in other certain bands at higher power levels than currently permitted.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2004-02-16 **Bluetooth mobile wireless transponders policy portable laptop notebook PDA**

http://searchmobilecomputing.techtarget.com/originalContent/0,289142,sid40_gci950572,00.html?track=NL-102

Gartner Group warned that Bluetooth-enabled devices pose a threat to data confidentiality due to security flaws in implementation. In particular, notebook computers and Internet enabled PDAs are at serious risk of compromise. Eric Panzo, News Editor of SearchMobileComputing.com, notes, "Gartner's recommendation comes after a week when two manufacturers disclosed that Bluetooth security vulnerabilities exist in nearly a dozen wireless handsets. On Wednesday [2004-02-11], Sony Ericsson revealed that several of its handsets, including the Sony Ericsson T610 and T68i and the Ericsson T39, T68 and R520, are vulnerable to attackers who could use Bluetooth to steal information stored on the devices. Earlier, Nokia had confirmed that a number of its handsets have a similar flaw. Affected handsets include the 6310, 6310i, 7650, 8910 and 8910i."

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2004-02-18 **Wi-Fi Internet connectivity spreading**

NewsScan

WI-FI EVERYWHERE

Wi-Fi is in the air, and increasingly is being used for such household tasks as paying bills, searching for recipes from the kitchen and doing e-mail, and in the future it will be used to connect lamps, stereos, computers, and to integrate the Internet fully into daily life. Now, Wi-Fi is already being used in some consumer electronics, such as TVs, DVD players, stereos and other systems from Gateway, Microsoft, Samsung and others that make it possible to download a movie or song from the Internet and send it wirelessly to a home entertainment system. Still on the way: Wi-Fi systems to control your lights remotely, adjust your thermostat, check whether you left the iron on, and live your life as Mr. or Ms. Internet of the 21st century. (USA Today 18 Feb 2004)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2004-03-28 **new WiFi wireless technology high speed networking Internet**

NewsScan

FOUR NEW WIRELESS TECHNOLOGIES

Four new wireless technologies are now in the pipeline, and are expected to be ready for use by early 2005. The first is WiMax, which will have a reach up to 30 miles away and be competitive with cable and DSL for use by Internet service providers. The second is the 802.16e standard, an extension to WiMax that will allow connection to the Internet while a user is in a moving vehicle. The third is 802.11n, a high-bandwidth extension to the current Wi-Fi standard that would increase the speed of Wi-Fi connections by 10 to 20 times. And the fourth is Ultrawideband, which could be used for transmitting large amounts of data short distances. Jeff Harris of General Atomics explains Ultrawideband by offering this example: "We want to eliminate that cable that goes between devices. If you go and drop a few thousand dollars on a flat-panel television, we want you to be able to put it on the best wall in your house — not just the wall that's closest to the cable outlet."(USA Today 28 Mar 2004)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2004-03-31 **Department of Defense DoD WiFi issue policy IEEE 802.11b**

NIPC/DHS

March 31, Government Computer News — DOD set to issue policy on WiFi use.

The Department of Defense (DoD) will soon issue a policy to guide the use of WiFi equipment, said Ronald Jost, director of wireless technology for the DoD. Jost spoke Wednesday, March 31, in Washington, D.C. at the National High Performance Computing Conference. The new policy will mandate that no information—either classified or unclassified—will be allowed to travel unencrypted across a wireless network. But DoD will encourage use of wireless networks, as they reduce the amount of time it takes to set up and tear down LANs. DoD currently has top-secret, local IEEE 802.11b networks running, Jost said. Offices can now procure military-grade secure equipment, so the remaining hurdles involve establishing policy, Jost said. The policy, DOD 8100.bb, is finished and awaiting sign-off, Jost said. DoD also will establish Websites instructing offices how to set up wireless networks for both classified and unclassified use. DoD is also developing a policy for the use of cellular phones. Jost said the department will establish relationships with selected commercial providers who will be able to provide military personnel with cellular voice and data connections. The process will involve companies certifying their equipment as secure. " All [cellular] data traffic will go through virtual private networks," Jost said.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2004-04-13 **WiFi wireless network hacking SANS threat**

NewsScan

WIRELESS HACKING

Pointing to a rise in wireless hacking, security expert Joshua Wright of the SANS Institute warns: "All the money you've spent to protect your corporate network is moot if someone hacks your laptop at a wireless access point." And Don LeBeau of security firm Aruba Wireless Networks says that at least one Silicon Valley company suspected it was the target of corporate espionage when it found an unauthorized device surrpetiously establishing a hot spot from a conference room. Shai Guday, group program manager for wireless at Microsoft, urges companies to take the wireless hacking threat seriously: "Wireless is happening. They can't bury their heads in the sand. Wireless is great, but security is more important." (USA Today 13 Apr 2004)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2004-05-03 **wireless airlines air travel snail mail**

DHS IAIP Daily; http://www.dmnews.com/cgi−bin/artprevbot.cgi?article_id=2734 5

May 03, DM News — Airlines use wireless tracking to comply with USPS contracts.

At least two airlines are working with a wireless company based in Redmond, WA, to track mail as it moves through their systems as part of their contracts with the U.S. Postal Service (USPS). The data is used by the postal service to verify whether an airline is adhering to on-time performance standards. Depending on the results, a carrier could lose, maintain, or gain postal business. As part of contracts awarded last year, carriers are required by the USPS to scan mail at the time it is received, when the carrier loads the mail onto a flight, during transfers to connecting flights, and upon delivery to the postal service. The change to the contract process came about in part from Federal Aviation Administration security restrictions put in place after September 11. Air Transport Association statistics indicate that carriers last year flew 1.3 billion mail revenue ton miles, which is one ton of mail payload transported one mile.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2004-05-05 **Wi-Fi Wireless security WPA WEP 802.11i**

DHS IAIP Daily; http://www.pcworld.com/news/article/0,aid,115999,00.asp

May 05, IDG News Service — Wi-Fi security improves.

Two key improvements for the security and performance quality of Wi-Fi devices are scheduled to reach wireless network users this year as businesses and consumers continue to adopt wireless technology in greater numbers. The Wi-Fi Alliance will certify products for the new 802.11i and 802.11e standards by September, says Frank Hanzlik, managing director of the Wi-Fi Alliance. The 802.11i standard is the complete version of the preliminary security standard WPA (Wi-Fi Protected Access) introduced last year, while 802.11e is a new standard that will improve the quality of wireless networks that transmit voice and video. Security has been one of the biggest obstacles to the growth of wireless networking. Last year, WPA replaced the flawed Wired Equivalent Privacy (WEP) protocol to shore up wireless security before the full 802.11i standard could be ratified. WPA uses a dynamic encryption key as opposed to the static key used by WEP, and it also improves the user authentication process. The 802.11i standard adds Advanced Encryption Standard (AES) technology, a stronger level of security than used in WPA.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2004-05-10 **wireless Wi-Fi security Trusted Computing Group TSG**

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1590243,00.asp

May 10, eWEEK — Spec in works to secure wireless networks.

The Trusted Computing Group (TSG) said Monday, May 10, that it is working on a specification to ensure that wireless clients connecting to a network won't serve as a back door to worms and crackers. The specification will be finalized later this year. Although a client or customer connecting to an enterprise network may not overtly be seeking to do harm, the laptop may in fact hide an unpatched system that could serve as an unexpected back door into an otherwise secure system. Likewise, a network administrator cannot be sure whether a laptop hides a worm that might otherwise have been blocked by a wired firewall. When completed, the specification will serve as a means by which network security and network infrastructure vendors can ensure a level of compliance with the best practices of network security, executives said. The specification will specify a level of trust for network endpoints, characterized by the version number of specific applications; whether those applications have been patched; and whether those OSes and applications are free from viruses, as defined by the revision numbers of the signature libraries used within antivirus applications. If a client fails to meet those specifications, the Trusted Network Connect specification will define a process by which the client is quarantined until the appropriate patches and anti-virus tools have been applied.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2004-05-11 **Bluetooth wireless security bluesnarfing**

DHS IAIP Daily;
http://www.computerworld.com/printthis/2004/0,4814,93066,00.html

May 11, Computerworld — Bluetooth group downplays security risks.

The Bluetooth Special Interest Group (SIG) is dismissing security fears about the technology. Mike McCamon of Bluetooth SIG said Monday, May 10, that Bluetooth device shipments have now hit one million per week and that any security problems with the wireless technology security problems are limited to a handful of phones manufactured by Nokia Corp. and Sony Ericsson Mobile Communications AB. Those phones, which include Sony Ericsson's R520m and T68i phones and Nokia's 6310, 6310i, 8910 and 8910i phones, are susceptible to a hacking technique known as "bluesnarfing," according to Nick Hunn, a Bluetooth security expert in London. Flaws in these phones can allow hackers to access data such as information stored in address books or calendars, he said. Both Nokia and Sony Ericsson are developing patches for the older phones, while newer models won't be vulnerable to a bluesnarfing attack, Hunn said. Nokia said that it views any security threat from bluesnarfing as minimal and that the technique can be easily prevented by setting Bluetooth on the phones to a "hidden" mode. That makes intrusion more difficult, "since the hacker will have to know or guess the Bluetooth address before establishing a connection," said Nokia.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2004-05-13 **CERT AusCERT vulnerability wireless 802.11**

DHS IAIP Daily; http://www.auscert.org.au/render.html?it=4091 Source:
http://www.kb.cert.org/vuls/id/106678

May 13, US-CERT — Vulnerability Note VU#106678: IEEE 802.11 wireless network protocol DSSS CCA algorithm vulnerable to denial of service.

The Clear Channel Assessment (CCA) algorithm used in conjunction with Direct Sequence Spread Spectrum (DSSS) transmission is vulnerable to an attack in which a specially crafted RF signal will cause the algorithm to conclude that the channel is busy, so that no device in range of the signal will transmit data. The attacker must be actively transmitting a signal and within range to affect wireless devices. AusCERT notes that devices that use 802.11 and DSSS transmission encoding are affected. An unauthenticated, remote attacker can cause any vulnerable device within range to stop transmitting, causing a denial of service. A complete solution is not available for 802.11 DSSS devices. This vulnerability and potential workarounds are available in AusCERT Advisory AA-2004.02: http://www.auscert.org.au/render.html?it=4091

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2004-05-16 **w-fi flaw Queensland University Australia 802.11 exploit**

NewsScan

RESEARCHERS FIND WIFI FLAW

Researchers at Queensland University of Technology in Australia have discovered an easily-exploited vulnerability that can be used to take down most 802.11 wireless networks. The flaw operates at lower network layers than most previously-discovered security flaws in 802.11 networking, and affects any network operating at the 2.4GHz frequency — which is the sole frequency used by the most popular wireless protocol, 802.11b. (The Australian 13 May 2004) rec'd from John Lamp, Deakin U.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2004-05-17 **Wi-Fi transportation airlines broadband**

DHS IAIP Daily; http://www.newscientist.com/news/news.jsp?id=ns99995001

May 17, New Scientist — Hi-flying Wi-Fi debuts on transatlantic flight.

Passengers flying on a Lufthansa flight from Munich to Los Angeles on Monday, May 17, became the first to experience in-flight Wi-Fi -- a broadband wireless internet connection. The satellite-based system enables passengers to surf the web and send emails from their own Wi-Fi-enabled laptop or handheld computers instead of using the more limited services some airlines offer through their seatback displays. The system, called FlyNet, has already been installed on five of Lufthansa's fleet, with plans to extend this to all 80 of the German airline's long-haul planes by the end of 2006. The cost to passengers is $10 for half an hour, or a flat rate of $30 for the entire flight. This is far cheaper that the $16 per email charged by some companies via seatback equipment. Internet traffic to and from the aircraft is handled via geostationary communications satellites orbiting the Earth at 36,000 kilometres.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2004-05-25 **Wireless Wi-Fi WLAN flaw vulnerability defense**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/holes/story/0,10801,93343,00.html?SKC=security−93343

May 25, ComputerWorld — IT managers ready defenses against flaw in wireless LANs.

Information technology managers last week said a denial-of-service vulnerability that affects some Wi-Fi wireless LANs (WLANs) could force companies to develop new skills and rethink the way their networks are set up. But, they added, it should be relatively easy to defend WLANs against attacks seeking to exploit the flaw. Companies that operate multiple access points on their WLANs could also switch network traffic to other access points if one or more were attacked, although doing so would require radio frequency management skills and tools. The flaw was discovered by a team of graduate students at Queensland University of Technology in Brisbane, Australia. Mark Looi, a professor there, suggested that one defense against attacks would be to replace all 802.11b access points with 802.11a technology, which uses a different form of modulation than DSSS.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2004-06-09 **Wi-Fi spread NBA stadium access**

NewsScan

WI-FI EVERYWHERE?

The head of arena operations for the Charlotte Bobcats, an NBA expansion team, is including Wi-Fi wireless communications in the design of the team's new $265 million arena. He says, "Some people will think this is the geeky thing, the nerdy thing. But they were probably saying that 10 years ago when other people were going to Web sites and using e-mail." Other professional sports teams are making the same moves, and Giants chief information officer Bill Schlough says: "It's like walking into Starbucks. Except our Wi-Fi is free." Using Wi-Fi, fans will be able to access content
such as historical videos, trivia games and real-time statistics from the Internet or through customized material available only in the stadium. Schlough says: "There's a lot of purist fans who scoff at anybody bringing laptops to games. I've been heckled when I go in the stands. But then
they'll end up wanting to look over your shoulder." His only fear: "The real problem is business people coming and doing their office e-mails at the game." (USA Today 9 Jun 2004)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2004-06-11 **broadband WiFi spectrum reconfiguration Federal Communications Commission FCC**

NewsScan

FCC PAVES THE WAY FOR SPECTRUM RECONFIGURATION

The Federal Communications Commission approved a plan to reconfigure a chunk of valuable airwave spectrum in an effort to boost wireless broadband use. The current configuration places spectrum intended for educational-video use adjacent to spectrum earmarked for commercial uses -- a situation that requires the agency to impose rigid rules on commercial users to avoid interference. The FCC also decided to maintain its policy of allowing educators to lease spectrum to companies such as Nextel and Sprint, but ruled against allowing the widespread sale of educational licenses. Currently, schools can license 120 megahertz of the 194 MHz band, and educators are permitted to lease as much as 95% of their airwaves to commercial users and spend the proceeds for educational purposes. Critics had charged that some educators had not made good use of their licenses, but most educators opposed outright sale of the licenses, comparing the idea to the sale of national parks. (Wall Street Journal 11 Jun 2004)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2004-08-06 **computer science research team Wi-Fi security study weakness RSA RPI**

DHS IAIP Daily; http://www.stevensnewsservice.com/pr/pr460.htm

August 06, Stevens News Service — CompSci team spots weaknesses in Wi-Fi security.

A research team led by Dr. Susanne Wetzel, an Assistant Professor of Computer Science at Stevens Institute of Technology, has produced a study of the weaknesses of Wi-Fi networks. Wetzel's team has discovered "stealth attack" methods of disrupting and draining power from individual nodes within an "ad hoc" wireless network--i.e., a network that one "connects to" as a visitor as one moves physically with one's mobile computer from location to location, without a dedicated access point. While still rare, ad hoc modes are the underpinning for many of the advanced data networking schemes now being proposed. "Most of today's communication infrastructure is based on trustworthy collaboration among information routers," says Wetzel. " However, given the increased economic reliance on a working communication infrastructure, this has become a potential target for terrorists and other criminals." Wetzel worked with researchers from Rensselaer Polytechnic Institute and RSA Labs, as well as Stevens' own Wireless Network Security Center (WiNSeC).

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2004-08-12 **Widcomm Bluetooth virus vulnerability PDA PC**

DHS IAIP Daily; http://www.esecurityplanet.com/alerts/article.php/3394181

August 12, eSecurity Planet — Widcomm Bluetooth a virus risk.

A security research firm has discovered a serious vulnerability in Widcomm's widely deployed Bluetooth Connectivity Software that could lead to wireless delivery of malicious worms and viruses. According to an advisory from British security firm Pentest, an unauthenticated remote attacker could exploit the flaw to submit malformed service requests via Bluetooth, which would trigger a buffer overflow. Buffer overflows are commonly used by malicious hackers to execute arbitrary code on vulnerable systems. In theory, security experts say this could pave the way for the creation of a wireless worm that spreads between PCs or PDAs using Bluetooth over the air. "Worms like this could spread very fast, especially in an environment like a seminar or a conference," said Jarno Niemela, a virus tracker at F-Secure.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2004-09-02 **Philidelphia free wireless Wi-Fi access Internet hot spot largest world**

NewsScan

SOFTWARE AND THE CITY

Philadelphia officials are considering a plan to turn the whole city into the world's largest wireless Internet hot spot, placing thousands of small Wi-Fi transmitters around the city. Philadelphia chief information officer Dianah Neff says, "If you're out on your front porch with a laptop, you could dial in, register at no charge, and be able to access a high speed connection. It's a technology whose time is here." The Philadelphia service wouldn't be the first city to do this, only the largest so far. The Minneapolis suburb of Chaska began offering citywide wireless Internet access this year for $16 a month (to an area of about 13 square miles), and Cleveland has positioned 4,000 wireless transmitters in several areas, offering free Wi-Fi Internet access for anyone who passes through those areas. Neff estimates it would cost Philadelphia $1.5 million a year to maintain the system it's considering. (AP 2 Sep 2004)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2004-09-02 **New York City NYC Republican National Convention RNC 2004 elections wireless security challenge Wi-Fi war driving unencrypted hot spots access points discovery**

DHS IAIP Daily;
http://www.computerworld.com/mobiletopics/mobile/story/0,10801,95641,00.html

September 02, Computerworld — Manhattan presents wireless security challenge for RNC.

IT security researchers have uncovered a significant number of unencrypted wireless devices in close proximity to the Republican National Convention (RNC) at New York's Madison Square Garden. During a two-hour "war drive" around the site of the RNC as well as Manhattan's financial district, security researchers from Newbury Networks Inc. discovered more than 7,000 wireless devices, 1,123 of which were located within blocks of the convention. More important, 67% of those devices were access points that did not have encryption protection. The findings underscore that the huge numbers of open, unsecured wireless networks represent a serious threat to the city's hard-wired infrastructure, said Newbury CEO Michael Maggio. "A wireless-enabled notebook computer powered up inside Madison Square Garden by a conventioneer or media representative could automatically associate with wireless networks outside of the building," said Maggio, noting that such a security gap could allow an attacker to "hop onto" the wired network inside the facility.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2004-10-26 **WiMax 802.16 Intel Craig McCaw**

NewsScan; http://www.nytimes.com/2004/10/26/technology/26intel.html

INTEL TEAMS WITH MCCAW STARTUP ON WIMAX NETWORKS

Intel is collaborating with Clearwire, a startup founded by cellular mogul Craig McCaw, to jumpstart WiMax technology by creating a series of new chips designed to support the WiMax standard. WiMax is intended to extend the limited reach of WiFi wireless networks by permitting a single transceiver to connect hundreds or thousands of customers to the Internet over distances of many miles. Clearwire recently began offering wireless Internet service in Jacksonville, Fla., for $25 a month and plans to be available in as many as 20 U.S. markets by next year. It's also deploying the service in Canada and Mexico, as well as in developing countries like Bangladesh. "We are tempered by the fact that everyone who has tried this has failed," says McCaw, "but w'ere crossing the river on the backs of pioneers." (New York Times 26 Oct 2004)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2004-11-17 **WiFi cellphones dual-network NTT DoCoMo 3G**

NewsScan; http://apnews.excite.com/article/20041118/D86E0F280.html

NTT OFFERS DUAL-NETWORK CELL PHONE NTT

DoCoMo is offering customers a cell phone that can make Internet calls via WiFi networks in addition to using the standard wireless networks. The dual-network N900iL phone uses 3G technology to deliver higher speed data transmissions. Nokia, the world's largest handset maker, says it will introduce a dual-network cell phone next year. (AP 17 Nov 2004)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2004-11-23 **municipal WiFi MAN Verizon Pennsylvania legislation**

NewsScan; http://online.wsj.com/article/0

TELCOS THREATENED BY MUNICIPAL WIFI

Dozens of municipalities around the country are installing WiFi networks in order to provide citizens with low- or no-cost wireless Internet access -- a phenomenon that has raised the ire of large telephone and cable companies, who see their lucrative broadband businesses eroding. In response, telcos and cable companies are pushing states to pass legislation that could make such municipal networks illegal. Last week, after intensive lobbying by Verizon, the Pennsylvania General Assembly passed a bill with a deeply buried provision that would make it illegal for any "political subdivision" to provide to the public "for any compensation any telecommunications services, including advanced and broadband services within the service territory of a local exchange telecommunications company operating under a network-modernization plan." Verizon is the local exchange operator for most of Pennsylvania and is planning a major fiber-optic cable rollout. Similar bills have passed in Utah, Louisiana and Florida. Critics say the telco giants' clout is stifling broadband expansion in the U.S., but the telcos argue it's unfair for them to have to compete against local governments, which have easy access to capital and pay no taxes. (Wall Street Journal 23 Nov 2004)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2004-11-29 **WiMax 802.16 TowerStream New York**

NewsScan; http://www.nytimes.com/2004/11/29/technology/29max.html

WIMAX PROSPECTS LOOKING UP

Upstart TowerStream is offering a new take on wireless broadband, delivering highspeed connections to business customers through antennas perched atop highrises in urban areas. The service, dubbed WiMax (worldwide interoperability for microwave access), uses fixed antennas to send and receive signals across entire metropolitan areas. The radio signals and antennas are unaffected by bad weather and provide a cheaper alternative to data cables buried below streets that are vulnerable to accidental severing by construction crews. Although other companies are getting into the WiMax business, TowerStream is currently the market leader, with a lock on prime locations like the top of the Empire State Building and the MetLife Building in New York City. "The real estate is the hard part of the business," says TowerStream COO Jeff Thompson. "When you tell people you can reach 10,000 clients, they don't believe you." It took him more than two years to negotiate those leases, but Thompson's optimism is warranted, say many analysts. The high-speed wireless Internet market is worth about $400 million globally and could quadruple in the next few years, according to the WiMax Forum, a group of WiMax equipment makers and providers. (New York Times 29 Nov 2004)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2004-11-30 **wireless MAN municipal Philadelphia Verizon**

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/10305668.htm

WIRELESS IN PHILADELPHIA

Verizon has struck a deal with the city of Philadelphia to provide wireless Internet access as a municipal service. A spokeswoman for Philadelphia Mayor John F. Street says the two parties "reached an understanding that protects our interests and allows us to move forward with the Wireless Philadelphia initiative." Under the Pennsylvania legislation, any political subdivision would have to get the permission of the local telephone company to provide a telecommunications service for a fee, including broadband Internet, and if the company rejects the plan it would have to offer a similar service within 14 months. (San Jose Mercury News 30 Nov 2004)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2004-12-15 **wireless FCC airplanes Internet access**

NewsScan; http://www.latimes.com/technology/ats-ap_technology10dec15

WIRELESS ACCESS ON JETS?

The Federal Communications Commission (FCC) is considering a plan that would allow air travelers wireless high-speed Internet access. David Stempler, president of the Air Travelers Association, says the changes under consideration would "make business travelers more efficient and while away the time for a lot of other passengers. This is all the wave of the future here." (AP/Los Angeles Times 15 Dec 2004)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2005-01-03 **WiFi Vonage VoIP voice over IP**

NewsScan; http://www.usatoday.com/tech/news/2005-01-03-wifi-phone_x.htm

VONAGE TO OFFER WI-FI INTERNET PHONE CALLS

Vonage, the No. 1 Internet phone company, is offering its subscribers a wireless Wi-Fi phone that can make calls over the Internet at homes or at public Wi-Fi hot spots. A phone will cost around $100. Wi-Fi calls are essentially free, in contrast to cell phone calls, and customers will plug a regular phone into an adapter linked to a broadband Internet line. Vonage will then turn the calls into data that travel by Internet before being converted back to voice at the other end. (USA Today 3 Jan 2005)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2005-01-13 **WiFi security wireless WiMax Bluetooth**

NewsScan; http://www.theregister.com/2005/01/13/wi_fi_paint/

PAINT ON A LITTLE WI-FI SECURITY

Tired of worrying whether your wireless hotspot is hosting "drive-by" users? Force Field Wireless has developed a do-it-yourself DefendAir paint "laced with copper and aluminum fibers that form an electromagnetic shield, blocking most radio waves and protecting wireless networks." One coat of the water-based paint "shields Wi-Fi, WiMax and Bluetooth networks operating at frequencies from 100 megahertz to 2.4 gigahertz," while two or three applications are "good for networks operating at up to five gigahertz." Force Field Wireless warns that the paint must be applied carefully -- too little, and the radio waves will "leak"; too much and you risk hindering the performance of radios, televisions and cell phones. And while the only color available is a dreary gray, DefendAir can also be used as a primer so you can paint over it with your favorite hue. (The Register 13 Jan 2005)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2005-01-20 **Wi-Fi privacy concern wireless point hot spot base station masquerading sensitive data interception signal strength**

DHS IAIP Daily; http://news.bbc.co.uk/1/hi/technology/4190607.stm

FAKE WIRELESS ACCESS POINTS OR "EVIL TWINS" WARNED FOR WIRELESS INTERNET

People using wireless high-speed Internet (Wi-Fi) are being warned about fake hotspots, or access points. The latest threat, nicknamed evil twins, pose as real hotspots but are actually unauthorized base stations, say experts at Cranfield University in the U.K. Once logged onto an Evil Twin, sensitive data can be intercepted. "Users can also protect themselves by ensuring that their Wi-Fi device has its security measures activated," said Professor Brian Collins, head of information systems at Cranfield University. In most cases, base stations straight out of the box from the manufacturers are automatically set up with the least secure mode possible. Cybercriminals who try to glean personal information using the scam, jam connections to a legitimate base station by sending a stronger signal near to the wireless client.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2005-01-20 **researchers bogus Wi-Fi access points wireless devices personal information cybercrime technology**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4190607.stm

RESEARCHERS WARN OF BOGUS WI-FI ACCESS POINTS

Researchers at Britain's Cranfield University are warning users of wireless computing devices about bogus Wi-Fi access points that can steal personal information. The so-called evil twin hotspots are set up near existing access points, where they can hijack signals sent between wireless devices and legitimate access points. Dr. Phil Nobles, a expert on cybercrime and wireless technology at Cranfield, said, "Because wireless networks are based on radio signals, they can be easily detected by unauthorized users tuning into the same frequency." Security experts said that setting up adequate protections for access points, as well as installing personal firewalls on wireless devices, can prevent users from being victimized by the unauthorized hotspots.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2005-01-28 **social engineering shoulder surfing confidential data theft threat greater Wi-Fi evil twin malicious hot spot**

DHS IAIP Daily; http://www.techweb.com/wire/mobile/57704010

LOW-TECH WAYS TO STEAL CONFIDENTIAL DATA WORSE THAN "EVIL TWIN" THREAT

You're more likely to have secrets stolen at a coffee shop from someone snooping over your shoulder or using wireless sniffing software than from sophisticated hackers deploying a so-called "Evil Twin" access point, said Jay Heiser, a U.K.-based research director with Gartner. "Unless the Wi-Fi session is encrypted in some way, which by default it's not, then all of the traffic is available for perusal by anyone with a wireless-enabled laptop and the right software." Heiser was reacting to an announcement last week by academic researchers in Britain who warned that rogue wireless access points -- dubbed "Evil Twin" -- posed a security risk to users in public places like coffee shops and airports where wireless Internet service is available. The lowest-tech way to lose confidential data while at a public hotspot -- which by definition are not encrypted -- is to be a victim of "shoulder surfing," where someone simply peeks over the shoulder of the user to watch for passwords and login names.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2005-02-21 **mobile phone virus Cabir US UK China Bluetooth Philippines standards international widespread infection**

NewsScan; http://www.nytimes.com/reuters/technology/tech-tech-security.html

MOBILE PHONE VIRUS INFILTRATES U.S.

The world's first mobile phone virus "in the wild," dubbed Cabir, has migrated to the U. S. from its point of origin in the Philippines eight months ago, infecting phones in a dozen countries along the way. Experts say the mobile-phone virus threat will increase as virus-writers become more sophisticated and phones standardize technologies that will make it easier to for viruses to spread not just across devices, but the whole industry. Up until now, disparate technical standards have worked against fast-moving virus infiltration, but Cabir has now been found in countries ranging from the China to the U.K., spread via Bluetooth wireless technology. The biggest impact of the relatively innocuous virus is that it's designed to drain mobile phone batteries, says Finnish computer security expert Mikko Hypponnen. Last November, another virus known as "Skulls" was distributed to security firms as a so-called "proof-of-concept alert, but was not targeted at consumers. (Reuters/New York Times 21 Feb 2005)

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2005-03-01 **wireless networking Wi-Fi security concern radio frequency identification RFID**

DHS IAIP Daily; http://www.fcw.com/fcw/articles/2005/0228/web−wireless−03 −01 −05.asp

WIRELESS STRUGGLES WITH SECURITY

Agency officials in charge of setting policies for wireless use and related technologies such as radio frequency identification (RFID) still have a difficult job. Technologies are evolving, as are the security standards that they use, and employees are not always judicious about using their own wireless devices on an agency network. What employees see as simple conveniences -- such as using a handheld device to send and receive e-mail -- can cause nightmares for security officials, according to panelists speaking today at the E-Gov Institute's Wireless/RFID conference in Washington, D.C. "Even a simple thing like putting a password on a cell phone is hard to sell" to employees, said Jaren Doherty, director of information security and awareness at the National Institutes of Health. "But it's important if the phone is also enabled to get your e-mail or log on to the Internet."

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2005-04-13 **radio-controlled wireless land mines identification authentication I&A control encryption vulnerabilities risks warfare battlefield**

RISKS; http://www.theregister.co.uk/2005/04/12/laptop_triggered_landmine/ 23 84

RADIO-CONTROLLED LAND MINES POSE SECURITY RISKS

Rob Slade pointed out that the new radio-controlled land mines pose significant security risks. "There are very few details provided in regard to the new mines. There appear to be different types. They have some kind of wireless capability. They have remote detonation capability."

He added,

"Based upon what is said, we can determine some additional aspects of the technology, as well as surmise more. They likely communicate via radio frequencies. They will have some kind of (likely minimal) software for reception of signal, authentication, and activation. (Deactivation is likely accomplished by activating the mine when [hopefully] nobody is around.) The mines are probably individually addressable: blowing an entire minefield for a single intrusion would not seem to be an effective use of resources. Radio communication would imply that either the mines are battery powered, or that they contain an antenna and transponder. Given the purpose and use of mines, it is likely that there is an alternate and more standard triggering mechanism such as pressure plates or tripwires that does not require wireless activation."

. . . .

"The potential risks are numerous. With radio communications mines that are buried, or placed under or behind metal or water, may fail to detonate when needed, or deactivate. Any kind of software is, of course subject to failures (which, in this case, could be literally catastrophic). Authentication would be a fairly major issue: sniffing of radio traffic could easily determine commands, replay attacks, static passwords, or number sequences. (Note that the mines require "minimal training" for use.) Failure of authentication could, again, result in failure of either detonation or deactivation. Battery failure would be an issue and therefore transponders are more likely, but transponders would be more difficult to troubleshoot. (Should the transponders retransmit? That would assist with finding and disarming mines, but broadcasting a signal with known improper authentication would result in a means of determining the location of mines.)"

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2005-04-25 **hacker infiltration attack information technology IT conference London wireless hot spot Wi-Fi evil twin attack steal sensitive information theft**

DHS IAIP Daily; http://news.zdnet.co.uk/internet/security/0,39020375,3919595 6,00.htm

HACKERS ATTACK IT CONFERENCE IN LONDON

Hackers infiltrated an IT exhibition last week and attacked delegates' computers with a new type of wireless attack. Security experts attending the Wireless LAN Event in London last Wednesday, April 20, found that anonymous hackers in the crowd had created a Website that looked like a genuine login page for a Wi-Fi network, but which actually sent 45 random viruses to computers that accessed it. Spencer Parker, a director of technical solutions at AirDefense, said that the hackers walked around the exhibition carrying a Linux-based laptop running software that turned it into a wireless access point. The technique has evolved from an "evil twin" attack, where hackers host fake log-in Websites at commercial Wi-Fi hotspots. This was originally used to lure people into typing in credit card details onto the Web page, so the hacker could steal them.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2005-04-28 **Wireless Wi-Fi leader alliance security discussion WEP**

DHS IAIP Daily; http://www.vnunet.com/news/1162761

WIRELESS LEADERS FORM ALLIANCE TO ADDRESS SECURITY

BT, Cisco and Intel announced a formal alliance at InfoSec Europe to promote better security for users of wireless networks. The trio are concerned that fears about security will harm the rollout of wide-scale wireless networks, and have produced advice sheets for businesses, homes and public Wi-Fi access points. BT, Cisco and Intel also agreed to standardize on the Wireless Encryption Protocol, and to implement stronger encryption and identity systems as soon as they are finalized.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2005-05-06 **laptop computer car breakins vulnerability identification target wireless Bluetooth**

RISKS 23 87

WAR DRIVING FOR TARGETS OF THEFT

Andrew Nicholson reported on an interesting finding while searching for his lost rental car in a big parking lot at Disney World. Seems that all of the breakins reported to DW security involved laptops equipped with Bluetooth responders. Nicholson wrote, "Apparently if you just suspend the laptop the bluetooth device will still acknowledge certain requests allowing the thief to target only cars containing these laptops."

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2005-05-17 **US Government Accounting Office report wireless network security concern**

DHS IAIP Daily; http://www.gao.gov/cgi−bin/getrpt?GAO−05−383

INFORMATION SECURITY: FEDERAL AGENCIES NEED TO IMPROVE CONTROLS OVER WIRELESS NETWORKS (REPORT)

The Government Accountability Office (GAO) was asked to study the security of wireless networks operating within federal facilities. GAO found that federal agencies have not fully implemented key controls such as policies, practices, and tools that would enable them to operate wireless networks securely. Further, tests of the security of wireless networks at six federal agencies revealed unauthorized wireless activity and "signal leakage"—wireless signals broadcasting beyond the perimeter of the building and thereby increasing the networks' susceptibility to attack. Without implementing key controls, agencies cannot adequately secure federal wireless networks and, as a result, their information may be at increased risk of unauthorized disclosure, modification, or destruction. GAO recommends that the Director of the Office of Management and Budget (OMB) instruct the agencies to ensure that wireless network security is incorporated into their agencywide information security programs in accordance with the Federal Information Security Management Act. OMB generally agreed with the contents of this report. Highlights: http://www.gao.gov/highlights/d05383high.pdf

---

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2005-05-17 **GAO report Wi-Fi security criticism government agencies unauthorized access NIST OMB**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=8521359

GAO WARNS OF INSECURE WI-FI

A report released this week by the Government Accountability Office (GAO) strongly criticizes the Wi-Fi security of federal agencies. Wireless networks with no security or with poorly configured security pose significant risks of unauthorized access. Hackers within range of the network could access the network and potentially other computers on the network. Despite guidelines issued by the National Institute for Standards and Technology stating that government agencies should forgo wireless networks unless their security can be ensured, 13 of 24 major agencies do not require security for wireless networks, and 9 agencies do not have wireless-security plans. Investigators from the GAO monitored six agencies and detected Wi-Fi signals outside all of them. The GAO report recommends that the Office of Management and Budget require all federal agencies to use a variety of security measures, including encryption and virtual private networks. Reuters, 17 May 2005

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2005-06-04 **Bluetooth wireless networking security breach weakness vulnerability exploit demonstration**

RISKS; http://www.newscientist.com/article.ns?id=dn7461 23 89

METHOD DISCOVERED OF CRACKING BLUETOOTH SECURITY

Avishai Wool and Yaniv Shaked of Tel Aviv University in Israel have demonstrated a method of cracking Bluetooth security. Every Bluetooth device broadcasts its ID code to everything in the vicinity. The method is to pick up an ID code, then send a message to another device, spoofing the ID code, and telling it that the 'link key' used for encrypting communication has been 'forgotten'. This forces the two devices to go through a 'pairing' exercise to establish another link key. (Normally this is done only on the first occasion on which two devices communicate with each other.) The attacker can then eavesdrop on the messages exchanged in the pairing session, and analyse these using software which implements the Bluetooth algorithm. The four-digit PIN (set on each device by the legitimate user) can be cracked by 'brute force'. The link key can then be derived, and the attacker can then communicate with either device by pretending to be the other.

[Abstract contributed to RISKS by Pete Mellor]

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2005-07-12 **wireless attack threat "phlooding" overloading AirMagnet dictionary attacks flood operations VPN firewall businesses**

DHS IAIP Daily; http://www.ebcvg.com/articles.php?id=802

NEW WIRELESS ATTACK DISCOVERED

The security threat of wireless networks to the enterprise keeps growing, this time with the discovery of a new wireless attack. Dubbed “phlooding,” this new exploit targets businesses central authentication server with the goal of overloading it and cause a denial-of-service attack. The “phlooding” attack, discovered by AirMagnet, describes a group of simultaneous but geographically distributed attacks that targets wireless access points with login requests using multiple password combination in what are known as dictionary attacks. The multiple requests create a flood of authentication requests to the company’s authentication server, which could slow down logins and potentially interfere with broader network operations, since many different users and applications often validate themselves against the same identity management system. Phlooding could effectively block broadband VPN or firewall connections that use a common authentication server to verify an incoming user's identity, making it temporarily impossible for employees to access their corporate network. Businesses with multiple office locations served by a single identity management server could be particularly vulnerable to phlooding attacks.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2005-10-10 **wireless networks Wi-Fi consortium standards speed range**

EDUPAGE; http://www.usatoday.com/tech/wireless/2005-10-10-wi-fi-standards_x.htm

WIRELESS COMPANIES FORM NEW GROUP

A new alliance among 27 technology companies intends to accelerate the development of the 802.11n standard for wireless transmission. Members of the Enhanced Wireless Consortium include Broadcom, Intel, Cisco, Lenovo, Sony, and Toshiba. The standard promises speeds of between two and ten times faster than current wireless technologies, as well as increased range, while being compatible with products based on the 802.11a, 802.11b, and 802.11g standards. With the new standard, less capacity is used to verify that transmissions are accurate, leaving room for the speed and distance improvements. Members of the consortium said they expect to have drafts of the standard available by early 2006 and the standard ratified by late 2006, well ahead of the timeline if it followed traditional procedures. Organizers said they hope makers of consumer electronics will take advantage of the early release of drafts of the 802.11n standard to develop products that can be available to consumers before ratification. USA Today, 10 October 2005

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2005-11-30 **wireless Internet Wi-Fi hurricane Katrina disaster New Orleans municipal network equipment donations**

DHS IAIP Daily; http://news.yahoo.com/s/nm/20051130/wr_nm/hurricanes_wifi_dc;_ylt=Ave0Wgcuh0iCd_qtk2hgWVIjtBAF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

HURRICANE-RAVAGED NEW ORLEANS GETS WI-FI

Hurricane-stricken New Orleans is largely destroyed and abandoned, but city officials said on Tuesday, November 29, it will soon have universal wireless Internet service. A free, municipally run Wi-Fi system has begun operation in the French Quarter and central business district and should cover the entire city within a year, Mayor Ray Nagin said. "We are among the first cities to feature a citywide wireless network and that's especially important to the recovery of our community," he said. Much of the equipment for the system has been donated by private companies.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2005-12-05 **research study SRI wireless data communications safety US Canada technology experiment**

DHS IAIP Daily; http://www.telematicsjournal.com/content/newsfeed/5602.html

U.S.-CANADA TECHNOLOGY EXPERIMENT ASSESSES SECURE WIRELESS DATA COMMUNICATION ENHANCEMENTS

SRI International Monday, December 5, announced the completion of tests that aim to improve the security of wireless data communications among domestic public safety, emergency preparedness, and law enforcement agencies, as well as for use in cross-border situations. The test exercise was commissioned by the U.S. Department of Homeland Security Science and Technology Directorate and its Cyber Security Research and Development Center. The test was conducted in late October in partnership with Defense Research and Development Canada (an agency of the Canadian Department of National Defense). The trial assessed various technologies developed by Voltage Security, CipherTrust, and Research in Motion/RIM. The technologies were evaluated under operationally relevant conditions, using repeatable procedures, automated tools, and infrastructure and instrumentation that could be refined and re-used to support future, related activities. "Recent natural disasters emphasize a critical need for secure mobile data communications in cross-agency and cross-border environments. This exercise proves that commercially available, secure mobile communications are available to government agencies," said Douglas Maughan, program manager of the DHS Cyber Security R&D Center. Exercise participants discussed the trial, its results, and the benefits of deploying a secure wireless solution for data communications at the InfoSecurity New York conference Wednesday, December 7.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2005-12-06 **Network Chemistry wireless threat database resource**

DHS IAIP Daily;
http://www.newsfactor.com/story.xhtml?story_id=01300000B4F7

WIRELESS THREAT DATABASE DEBUTED

Wireless security vendor Network Chemistry has announced the creation of an online Wireless Vulnerabilities and Exploits database intended to be a universal collection point for credible information about security threats affecting multiple wireless technologies, including 802.11 Wi-Fi, CDMA 1X EV-DO, EDGE, Bluetooth, and RFID, as well as emerging protocols like HSDPA and 802.16 WiMAX. The database is co-sponsored by Network Chemistry, wireless LAN training and certification firm CWNP, and the Center for Advanced Defense Studies, a non-profit, non-governmental institute. Brian de Haaff, vice president of product management and marketing at Network Chemistry, said of the database, "We hope it grows into an industry initiative. We've been talking quite a bit to other network security people and carrier people about it. No one has ever tried before to collect this kind of information in one place." Wireless Vulnerabilities and Exploits database: http://www.wirelessve.org/

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2006-01-16 **Windows 2000 2K XP Wi-Fi flaw vulnerability**

DHS IAIP Daily; http://www.vnunet.com/vnunet/news/2148609/microsoft−wi− 23
flaw−found

WINDOWS 2000/XP FALL THROUGH WI-FI FLAW

Hackers have exposed details of a previously undocumented flaw in Microsoft's handling of Wi-Fi which affects users of Windows 2000 and XP. The vulnerability was detailed at the Shmoocon hackers conference in Washington, DC, by self-confessed hacker Mark Loveless, (a.k.a. Simple Nomad), a senior security researcher for Vernier Threat Labs. Loveless explained that the issue centers on the way in which the operating systems look for wireless networks during start-up. When a Wi-Fi equipped laptop starts up using Windows 2000 or XP it immediately starts scanning for wireless networks. If none is found it sets up an ad hoc link using the name of the last wireless network accessed. If a hacker was aware of the last used network ID, for example knowing the name of a corporate Wi-Fi network address, it could be used to establish a direct local link with the Windows PC offering access to all local drives. However, the problem only arises if the target machine is not running a firewall. One of the changes in Windows XP SP2 turns the built-in firewall on by default.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2006-02-22 **London Wi-Fi network McAfee concern security**

DHS IAIP Daily; http://news.zdnet.co.uk/internet/security/0,39020375,3925373 23
0,00.htm

SECURITY FEARS OVER LONDON'S BLANKET WI-FI.

Security company McAfee on Tuesday, February 21, raised security concerns over the London's plan to install a Wi-Fi network throughout the Square Mile. The system will be constructed by The Cloud, and should give most of the city's workers wireless access within six months. However, McAfee has raised concerns about the security implications of the project. "Our big concern is that most people care more about connectivity than security. Always-on broadband makes it easier for hackers to find and target people. There is also a knowledge gap -- most people aren't that savvy when it comes to this technology," said Sal Viveros, security expert at McAfee. McAfee recommended that companies prepare themselves for always-on wireless access by learning about the techniques that hackers are using to target susceptible mobile employees, as London is a tempting target for hackers.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2006-03-23 **KisMAC Cisco vendor tag SSID parsing buffer overflow vulnerability solution update**

DHS IAIP Daily; http://secunia.com/advisories/19354/ 23

KISMAC CISCO VENDOR TAG SSID PARSING BUFFER OVERFLOW.

A vulnerability exists in KisMAC, which potentially can be exploited by malicious people to compromise a user's system. Analysis: The vulnerability is caused due to a boundary error in the "WavePacket:parseTaggedData()" function when parsing the Cisco vendor tag for additional SSIDs in a received 802.11 management frame. This can be exploited to cause a stack based buffer overflow and potentially allows arbitrary code execution. Successful exploitation requires that the user is e.g. tricked into opening a malicious pcap file containing special crafted management frames, or via raw management frames that are sent onto the wireless network while the user is performing a passive network scan. Vulnerable software: KisMAC 0.x. Solution: Update to version R73p: http://kismac.de/download.php The vulnerability has also been fixed in developer version 113.

Category 24.6 *WAP, WEP, Wi-Fi, Bluetooth, 802.11, WiMax*

2006-04-03 **IEEE 802.11w wireless standard security improvement**

DHS IAIP Daily; http://www.networkworld.com/news/tech/2006/040306−80211w−wir eless−security.html 23

IEEE 802.11W FILLS WIRELESS SECURITY HOLES.

IEEE 802.11i, the standard behind Wi-Fi Protected Access and WPA 2, patched the holes in the original Wired Equivalent Privacy specification by introducing new cryptographic algorithms to protect data traveling across a wireless network. Now, the 802.11w task group is looking at extending the protection beyond data to management frames, which perform the core operations of a network. Traditionally, management frames did not contain sensitive information and did not need protection. But with new fast handoff, radio resource measurement, discovery and wireless network management schemes, new and highly sensitive information about wireless networks is being exchanged in these non-secure frames. IEEE 802.11w proposes to extend 802.11i to cover these important frames.

24.7 SWDR (Software-defined radio)

Category 24.7 *SWDR (Software-defined radio)*

2000-12-07 **software-defined radio vulnerability**

NewsScan, San Jose Mercury News
http://www.mercurycenter.com/svtech/news/breaking/merc/docs/071981.htm

Called "software-defined radio," an emerging technology allow wireless devices to download new software to add capabilities or perform different functions, thereby enabling a single product to switch, for example, from serving as a cell phone to receiving FM radio broadcasts or providing Internet access — all without requiring new hardware. Seeing this innovation as offering a better way of managing the nation's airwaves, the Federal Communications Commission is developing new rules for approving equipment that can be altered. The technology makes it possible to switch the part of the airwaves on which the gadget can operate and seek out less crowded frequencies that are not being used. (AP/San Jose Mercury News 7 Dec 2000)

Category 24.7 *SWDR (Software-defined radio)*

2002-11-11 **software defined radio SDR frequency spectrum overload**

NewsScan

SDR CAN SOLVE WIRELESS GADGET OVERLOAD
Software defined radio (SDR) technology may hold the key to developing a single standard for the numerous portable devices now on the market, thereby unlocking new opportunities for wireless communications. As the line between "smart" phones and PDAs blurs, the multifunctional devices are becoming cluttered with software designed for each specific activity. "You could have your cell phone going, be using a Bluetooth headset and at the same time use GPS to check where you are," says Mark Cummings, an SDR proponent who notes that without SDR, that scenario would require cramming three separate radio circuits into a single handset. John Watson, VP of marketing for QuickSilver Technology, says SDR software would enable handset design that's more flexible and able to respond to changing market demands. "Right now, you have to do electronics design a couple of years ahead of time" before bringing new equipment to market. "The only thing you know is you're going to be wrong. What you really want is to be able to design it at the last minute." (Wired.com 11 Nov 2002)

Category 24.7 *SWDR (Software-defined radio)*

2004-11-08 **P2P peer-to-peer Internet radio music sharing copyright**

NewsScan; http://news.com.com/Music+sharing+thats+free+and+legal/2100-1027_3-5441036.html

P2P RADIO IS LATEST TWIST IN MUSIC SHARING

Now there's a new way to share music that's free and perfectly legal -- the trick involves marrying peer-to-peer technology with Internet radio. Pioneers in the field include Apple, Virgin Digital, and startups Mercora and Live 365, which offer tools that automatically stream users' private playlists over the Web while in some cases storing them in a searchable database for later retrieval. Mercora operates a Web-based network of about 8,000 "broadcasters" who serve up their playlists to somewhere between 175,000 and 200,000 listeners worldwide. "We're doing for music what Google did for the Web," says Mercora CEO Srivats Sampath. The company reasons that by using an Internet broadcast network model, it can take advantage of lower copyright fees, which are set by the U.S. Copyright Office rather than the record labels. As a result, Mercora can afford to pay the fees on behalf of broadcasters and offset the costs through advertising sales. "The big nut we had to crack is how to do this legally," says Sampath. "The law says you can broadcast as long as you pay. Fine, we will pay you." And if listeners happen to download a song? Technically, if the legally broadcast song is for personal use only, that's okay. "It's like a tape recorder," says Sampath. However, the downloader runs into legal trouble only when she tries to sell a track or transfer it to another person. (CNet News.com 8 Nov 2004)

Category 24.7 SWDR (Software-defined radio)

2005-02-16 **P2P peer-to-peer RIAA radio Internet broadcast legal law**

NewsScan; http://online.wsj.com/article/0

'PEER-TO-PEER' RADIO PASSES RIAA SCRUTINY

With the pressure on peer-to-peer file-sharing networks to stop enabling illegal musicswapping, several companies are trying to find ways to squeeze P2P technology into a legal framework. Mercora offers users a way to create playlists of their favorite songs and then "broadcast" them over the Internet to fellow users. When the "broadcasters" aren't online, neither are their "radio stations." America Online offers a similar service called Shoutcast, and Live365 charges amateur broadcasters a fee to upload their music to a central server, which then sends the music out to listeners' PCs. A London Web site, Last.fm, takes an "affinity sharing" approach, using a list of each user's favorite music to find "neighbors" with similar tastes. It then creates a customized broadcast for each listener, based on what their neighbors are listening to. Because in these cases the music files are temporarily "streamed" to listeners' PCs instead of taking up residence permanently on their hard drives, the Recording Industry Association of America has given its blessing and is working with some of the companies to ensure they stay within legal boundaries. KEXP executive director Tom Mara says traditional radio stations can learn a lot from these grassroots efforts. "It's no longer a case of a person in a booth broadcasting to people anonymously. Now we need to figure new modes of interaction -- not only between the listener and the station, but between listeners." (Wall Street Journal 16 Feb 2005)

24.8 MAC OS

Category 24.8 *MAC OS*

2000-01-03 **operating system patch DDoS distributed denial of service**

SecurityPortal.com (reprinted with permission), ZDNet
http://macweek.zdnet.com/1999/12/26/dosbug.html

Apple . . . released a patch for Mac OS 9's Open Transport networking protocol to correct a "flaw" that leaves Macs vulnerable to hackers who could enlist the computers over an Internet connection in distributed denial-of-service attacks without the users' knowledge.

Category 24.8 *MAC OS*

2002-05-18 **spam filtering documentation ISP Internet service provider**

RISKS 22 07

A mild ruckus broke out when Mac OS users discovered undocumented spam filters on the free POP3/IMAP e-mail servers available to them through thye Apple company. Apparently the false positives were bouncing legitimate messages, but since the victims neither knew about the filtering nor (naturally) had any control over this function, there was very little they could do about it other than stop using the service.

Category 24.8 *MAC OS*

2003-10-29 **Macintosh Operating System X @Stake systemic flaws buffer overflow exploitable Apple patches released**

NIPC/DHS

October 29, ZDNet Australia — Three flaws discovered in Mac OS X.

Security-research company @Stake has warned of three vulnerabilities affecting the Mac OS X operating system. The first details "systemic" flaws in the way OS X handles file and directory permissions, while the second details a kernel level vulnerability that does not affect default installations of the operating system. The third involves a buffer overflow condition that may be remotely exploitable. Apple has not yet released patches for the security issues. Mac users are advised to upgrade to the latest Apple operating system, which is not vulnerable to the flaws, for a fee. The full advisories are available online: http://www.atstake.com/research/advisories/2003/

Category 24.8 *MAC OS*

2003-10-31 **Apple Powerbook LCD white spots unexplained**

NewsScan

WHITE SPOTS ON POWERBOOK SCREENS
The new 15-inch-screen PowerBooks have unexplained white blotches showing up on the LCD screens. Some customers say they sent their laptops in for repair, only to see the spots reappear when the systems came back. A statement from Apple says: "The new 15-inch PowerBook has been a big hit with customers since its introduction last month. However, some customers are reporting the appearance of faint, white spots on their displays after using the system for a short period of time, and Apple is investigating these reports right now. Any customers experiencing this problem should contact AppleCare." (San Jose Mercury News 31 Oct 2003)

Category 24.8 *MAC OS*

2003-11-24 **Apple OS X security patch vulnerability exploit fix Jaguar**

NIPC/DHS

November 20, Macworld.co.uk — Apple releases security patches.

Apple Computer Inc. has released security updates for Mac OS X Panther 10.3.1 client and server systems and Mac OS X Jaguar 10.2.8 client and server operating systems. The Panther update includes the following updated components: OpenSSLzlib "gzprintf()" function, an update to the open-source lossless compression library used by Darwin, the kernel of Apple's OS. The Jaguar update improves a number of components, including document formatting system, groff; Unix macro processor component, gm4; and Mail w/CRAM-MD5 authentication (used to debug common authentication services). It also improves OpenSSL (a robust, commercial-grade, full-featured, and open-source toolkit with a general-purpose cryptography library that implements the Secure Sockets Layer); Personal File Sharing; QuickTime for Java; and the zlib "gzprintf()" function. Both updates are available for download from Apple's Website:
http://www.info.apple.com/support/downloads.html

Category 24.8 *MAC OS*

2003-12-24 **patch fix flaw vulnerability Apple Mac OS X DHCP Jaguar buffer overflow**

NIPC/DHS

December 22, CNET News.com — Apple issues patch for Mac OS X hole. Apple Computer has issued a security update that, among other fixes, closes a hole in Mac OS X that could have allowed hackers to take control of a computer under particular circumstances. The patch essentially changes the default settings for connecting to a Dynamic Host Communication Protocol (DHCP) server on Mac OS X 10.2.8. (aka "Jaguar"), Mac OS X 10.3.2 (aka "Panther") and the corresponding server versions of these operating systems. A DHCP server assigns a TCP/IP address to a computer and, under the earlier default settings, a Mac running one of the above-listed OSes would accept data from DHCP servers found on a local area network. If a hacker inserted a malicious DHCP server on a local network, he or she could then exploit Apple's earlier default setting to embed malicious software on a computer or use the computer as a drone for coordinated attacks on other systems. Apple's security update also fixes a buffer overflow vulnerability in a file system, plugs another vulnerability in Panther that could cause denial-of-service requests and in general improves the security features of the affected OSes. Additional information available on Apple's Website:
http://docs.info.apple.com/article.html?artnum=61798

Category 24.8 *MAC OS*

2004-03-02 **vulnerability hole flaw patch fix file sharing Mac OS X**

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1540556,00.asp

February 27, eWEEK — File sharing vulnerability discovered in Mac OS X.

A security issue that could result in stolen passwords and data on Friday, February 27, was revealed for Apple Computer Inc.'s Apple Filing Protocol (AFP), a component of Mac OS X 10.3.2. In a posting to the SecurityFocus BUGTRAQ list, Chris Adams, a system administrator, noted that while users could request secure connections, the system will not issue any alert or indication if an SSH connection is unavailable and then defaults to a non-secure connection. The only indication was a negative one--users must be aware that an alert "Opening Secure Connection" did not appear. This could result in users sending unencrypted passwords over an insecure connection. Adams said that any such activity would only come as the result of an active attack. "OS X does warn you before using unencrypted passwords and AFP does prevent passive password collection by encrypting the log-in process to protect the password on its way to the server. This problem allows you to trick it into sending the unencrypted password to you instead of the intended server," he said. Though his BUGTRAQ warning provided workarounds, such as manually configuring a SSH tunnel or using SFTP instead, Adams suggested that SSH should be enabled by default for both client and server and the user interface modified to clearly warn when the system is unable to establish an SSH tunnel. Additional information is available on the SecruityFocus Website:
http://www.securityfocus.com/bid/9763/discussion/

Category 24.8 MAC OS

2004-05-04 **Apple Mac OS X vulnerability patch issued**

DHS IAIP Daily; http://www.esecurityplanet.com/prodser/article.php/3349191

May 04, eSecurityPlanet — Apple issues patch for Mac OS X.

Apple Computer has rolled out a major security update to plug several vulnerabilities in its flagship Mac OS X server and client versions. The patch, which is being described as "highly critical," addresses security issues with the AFP Server, CoreFoundation and IPSec and also integrates a previously issued patch which contained bugs, Apple said. The latest flaws, discovered by researchers at @Stake, could lead to system hijack, security bypass, manipulation of data, privilege escalation, denial-of-service attacks and system access. The most serious flaw was found with AppleFileServer and can be exploited to compromise a vulnerable system. The vulnerability is caused due to a boundary error within the password handling and could allow attackers to cause a buffer overflow by passing an AFP "LoginExt" packet with a string in the "PathName" field. Apple also confirmed the existence of an unspecified vulnerability within the CoreFoundation when handling environment variables. This may potentially be aprivilege escalation vulnerability. Another flaw in RAdmin when handling large requests was also pinpointed. Secunia warned that this issue could potentially lead to system compromise problems. Security update information: http://docs.info.apple.com/article.html?artnum=61798

Category 24.8 MAC OS

2004-05-17 **vulnerability MAC OS X security issue critical update issued**

DHS IAIP Daily;
http://www.techworld.com/security/news/index.cfm?newsid=1574

May 17, Techworld — Mac OS X hit with another serious security issue.

A "highly critical" hole has been found in Apple's Mac OS X operating system, which will allow remote system access by getting someone to visit a malicious Website. Lixlpixel has reported a vulnerability dealing with how basic Internet elements are addressed in the OS' help facility that allow arbitrary local scripts to be executed on a user's machine. It is also possible to place files in a known location on a system by asking users to download a ".dmg" disk image file. A default browser option in Internet Explorer and Safari will mean a single user click is enough to drive the whole process. The combination of the two holes, tested and confirmed by security experts Secunia, can therefore allow system access to be achieved "very simply" according to Secunia CTO Thomas Kristensen. The holes affect Safari 1.x and Explorer 5.x. The solution is to change browser options and rename the help URI handler. More details are 11 available on Secunia's Website: http://secunia.com/advisories/11622

Category 24.8 MAC OS

2004-05-21 **Apple OS X Mac vulnerabilities update issued**

DHS IAIP Daily;
http://www.reuters.com/newsArticle.jhtml?type=technologyNews
&storyID=5224718

May 21, Reuters — Apple says OS X vulnerable to security breach.

Apple Computer Inc. said on Friday, May 21, a security hole in its software leaves users' computers vulnerable to attack. Apple, warning of a rare security hole in the company's OS X operating system for the second time this month, said in a release that a "theoretical vulnerability" in an application used to get help while browsing the Web could expose users to a malicious software code. The specific nature of the security hole, such as whether it makes the computer vulnerable to outsiders or allows virus-like code to enter the operating system, was not made clear. Apple urged users to go to its Website to download a free software update: http://www.apple.com/support/downloads/

Category 24.8 *MAC OS*

2004-05-25 **Apple OS X Mac vulnerabilities run file IM e-mail virus**

DHS IAIP Daily;
http://news.com.com/Mac+OS+fix+fails+to+plug+security+hole/2 100−1002_3 −5220285.html

May 25, CNET News.com — Mac OS fix fails to plug security hole.

A security hole still threatens Mac OS X users after a patch issued by Apple Computer last week failed to fix the underlying problem, security experts say. The security issue could allow an attacker to transfer and then run a malicious program on a Mac, if the Mac's user can be enticed to go to a fake Web page on which the program has been placed. Two other software companies have confirmed the issue. Security information company Secunia raised its rating of the potential risk to "extremely critical" after determining that the vulnerability is more widespread than Apple apparently first thought. The vulnerability actually involves two flaws. One allows a website to place a file on the Mac's hard drive when a user clicks on a uniform resource locator, or URL, specifically designed to bypass Mac OS X's security. The other gives an attacker the ability to run a file on another user's computer, provided the location of the file is known. Used together, the flaws constitute a major security hole that could result in a potential instant-messaging or e-mail virus.

Category 24.8 *MAC OS*

2004-08-10 **Apple Mac OSX 10.3.5 vulnerability PNG phishing attack**

DHS IAIP Daily; http://www.esecurityplanet.com/patches/article.php/3392971

August 10, eSecurity Planet — Apple plugs OS X vulnerabilities.

Apple Computer has rolled out a major security update for its Mac OS X Panther client platform. The patch addresses security flaws that put users at risk of sensitive data leakage, Denial of Service attacks and system access. The Mac OS X 10.3.5 update corrects multiple vulnerabilities in libpng that can be exploited by malicious hackers to compromise a user's system. The U.S. Computer Emergency Readiness Team (US-CERT) has previously issued a warning that bugs in libpng, the reference library that supports the Portable Network Graphics (PNG) image format, could allow a remote attacker to commandeer a vulnerable machine. Also patched are specific vulnerabilities in Apple's Safari Web browser. The upgrade plugs a hole that could open the door to phishing attacks and addresses a flaw that could be used by a malicious Website to steal sensitive information from forms. The original advisory is available here: http://docs.info.apple.com/article.html?artnum=25631

Category 24.8 *MAC OS*

2004-08-16 **Apple Safari Web browser vulnerability Mac OS X HTTP GET POST URL**

DHS IAIP Daily; http://www.kb.cert.org/vuls/id/128414

August 16, US-CERT — Vulnerability Note VU#128414: Apple Safari fails to properly handle form data in HTTP redirects.

Apple Safari is a web browser available for the Mac OS X operating system. A vulnerability exists in the way Safari handles web form data. When a web form is submitted to a server using the POST method and the server returns an HTTP redirect to a GET method URL, Safari may re-POST that data to the GET method URL. It has been reported that this condition occurs when the forward/backward buttons are used. As a result, a user's form data could be disclosed to a remote server. Apple has released a patch to address this vulnerability: http://docs.info.apple.com/article.html?artnum=61798

Category 24.8 *MAC OS*

2004-09-07 **Apple Mac OSX operating system flaws vulnerabilities fixes patch Kerberos authentication Jaguar Safari browser**

DHS IAIP Daily;
http://news.com.com/Apple+fixes+15+flaws+in+Mac+OS+X/2100−10 02_3− 5350010.html?tag=nefd.top

September 07, CNET News.com — Apple fixes 15 flaws in Mac OS X.

Apple Computer released an update to its Mac OS X operating system on Tuesday, September 7, to fix 15 security issues in the software. Many of the problems are flaws in the operating system's underlying open-source software, including a critical flaw in the Kerberos authentication system--software that can act as a gatekeeper for computer networks. The patch is available for Mac OS X 10.3.5 and Mac OS X 10.3.4, and also fixes issues in Mac OS X 10.2, known as "Jaguar." The patch, available through automatic updates or from the company's website, fixes software flaws that could enable an attacker to crash or freeze the Apache 2 Web server, run software by utilizing Apple's Safari Web browser or expose the password store used by the network. Apple's advisory, with details of the update, is available at: http://www.apple.com/support/

Category 24.8 *MAC OS*

2004-10-28 **Apple Remote Desktop privilege escalation vulnerability update issued**

DHS IAIP Daily; http://secunia.com/advisories/11711/

October 28, Secunia — Apple Remote Desktop privilege escalation vulnerability.

A vulnerability has been reported in Apple Remote Desktop, which can be exploited by malicious users to gain root access on a vulnerable system The problem is that a user under certain circumstances during the login process is able to launch applications behind the login window with root privileges. Update to version 2.1 or apply Security Update 2004-10-27 for version 1.x available at: http://www.apple.com/support/downloads

---

Category 24.8 *MAC OS*

2004-11-03 **National Security Agency NSA Mac OSX guidance**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/27799−1.html

November 03, Government Computer News — NSA gives security guidance for Mac OS X.

The National Security Agency (NSA) has posted a 109-page document on its Website (http://www.nsa.gov/snac/os/applemac/osx_client_final_v.1.pd f) telling agencies how to securely install and use Apple Computer Inc.'s Mac OS X Version 10.3.x operating system, code-named Panther. NSA notes that the document is a security guide and "not meant to replace well-structured policy or sound judgment." It warns administrators to test only in a non-production environment as similar as possible to the architecture where the OS will be deployed.

Category 24.8 *MAC OS*

2004-12-10 **Adobe Version Cue Mac OSX privilege escalation vulnerability no update issued**

DHS IAIP Daily; http://secunia.com/advisories/13399/

December 10, Secunia — Adobe Version Cue privilege escalation vulnerability.

A vulnerability in Adobe Version Cue is caused due to an error in the suid root scripts "startserver.sh" and "stopserver.sh". The current directory is not checked properly before executing scripts without an absolute path and can be exploited to gain root privileges by planting a malicious script named "productname.sh" in the current directory. The vulnerability has been reported on Mac OS X 10.3.6. Other versions may also be affected. No vendor solution is currently available.

Category 24.8 *MAC OS*

2004-12-22 **Apple Tiger suit data leakage BitTorrent intellectual property non-disclosure agreement NDA**

NewsScan; http://news.bbc.co.uk/1/hi/technology/4117465.stm

APPLE SUES 'TIGER' TESTERS OVER LEAKS

Apple has sued three members of the Apple Developer Connection for releasing preview versions of its latest Mac OSX, code-named Tiger, onto file-sharing sites. "Members of Apple Development Connection receive advance copies of Apple software under strict confidentiality agreements, which we take very seriously to protect our intellectual property," said Apple in a statement. The Apple Development Connection is a group of software programmers who have access to text versions of Apple software in order to tweak their own applications to work with Apple systems. The Tiger software was apparently leaked onto sites that use BitTorrent technology, which does not actually host the files being shared, but rather hosts a link that points users toward others who have the file sought. Last week, the Motion Picture Association of America launched a legal campaign against such sites, noting that they've been used for illegal sharing of movie files. (BBC News 22 Dec 2004)

Category 24.8 *MAC OS*

2005-01-06 **Apple data leakage confidentiality Thinksecret.com intellectual property lawsuit non-disclosure agreement NDA**

NewsScan;
http://www.reuters.co.uk/newsArticle.jhtml?type=internetNews&storyID=7250030
&section=news&src=rss/uk/internetNews

TO PROTECT ITS "DNA," APPLE SUES THINKSECRET.COM

Apple Computer is suing the Web site thinksecret.com for allegedly distributing Apple trade secrets by leaking details of upcoming products. The suit alleges that Think Secret owner Nick dePlume and other unnamed individuals posted information on thinksecret.com that could only have been obtained by someone who had signed a confidentiality agreement with Apple. A statement from Apple says: "Apple's DNA is innovation, and the protection of our trade secrets is crucial to our success." But dePlume says he's confident that Think Secret's reporting is consistent with the rights and privileges granted by the First Amendment. (Reuters 6 Jan 2005)

Category 24.8 *MAC OS*

2005-04-20 **Apple iSync local buffer overflow vulnerability Mac OS X command execution attack update issued**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/0366

APPLE ISYNC "MROUTER" LOCAL BUFFER OVERFLOW VULNERABILITY

A new vulnerability was identified in Apple Mac OS X, which could be exploited by local attackers to obtain elevated privileges. This flaw is due to a buffer overflow error in the iSync helper tool mRouter when handling specially crafted command line arguments, which can be exploited by a malicious user to execute arbitrary commands with "root" privileges. Security Update 2005-004: http://wsidecar.apple.com/cgi-bin/nph-reg3rdpty1.pl/product= 05661&platform=osx&method=sa/SecUpd2005-004Pan.dmg

---

Category 24.8 *MAC OS*

2005-05-16 **US CERT vulnerability alert Apple Mac OS X**

DHS IAIP Daily; http://www.us−cert.gov/cas/techalerts/TA05−136A.html

APPLE MAC OS X IS AFFECTED BY MULTIPLE VULNERABILITIES

Apple has released Security Update 2005-005 to address multiple vulnerabilities affecting Mac OS X version 10.3.9 (Panther) and Mac OS X Server version 10.3.9. The most serious of these vulnerabilities may allow a remote attacker to execute arbitrary code. Impacts of other vulnerabilities addressed by the update include disclosure of information and denial of service. Apple advisory and updates: http://docs.info.apple.com/article.html?artnum=301528

Category 24.8 *MAC OS*

2005-06-08 **Apple MAC OS X folder permission flaw privilege escalation**

DHS IAIP Daily; http://docs.info.apple.com/article.html?artnum=301742

MAC OS X FOLDER PERMISSION FLAW MAY LET LOCAL USERS GAIN ELEVATED PRIVILEGES

A vulnerability was reported in Mac OS X in the enforcement of folder permissions. A local user may be able to gain elevated privileges. A local user can exploit a race condition in assignment of permissions on files in the system's cache folder and the Dashboard system widgets. A local user may be able to write to files in those directories. See Source link below for updates.

Category 24.8 *MAC OS*

2005-06-09 **Apple MAC OS X fix patch flaw arbitrary command execution denial-of-service privilege escalation**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/0712

APPLE SECURITY UPDATE FIXES MULTIPLE MAC OS X VULNERABILITIES

Apple has released a security patch to correct multiple vulnerabilities affecting Mac OS X. These flaws could be exploited by remote or local attackers to execute arbitrary commands, cause a denial of service, obtain elevated privileges, or disclose sensitive information. Vendor updates are available. Mac OS X 10.3.9 Update (2005-006): http://www.apple.com/support/downloads/securityupdate2005006 macosx1039.html and Mac OS X 10.4.1 Update (2005-006): http://www.apple.com/support/downloads/securityupdate2005006 macosx1041.html

---

Category 24.8 *MAC OS*

2005-08-16 **Apple MAC OS X patches security update**

DHS IAIP Daily; http://www.techtree.com/techtree/jsp/article.jsp?article_id=5484&cat_id=582

APPLE RELEASES OS X PATCHES

Apple has released a security update for Mac OS X, which addresses several potential vulnerabilities in the operating system. The update incorporates patches for AppKit, which prevent malicious users from executing malware stored in carefully crafted, rich-text files. The Bluetooth code is modified, to ensure that devices' requirement for an authenticated connection is reported correctly. The security update also fixes "algorithmic complexity attack" vulnerabilities in the OS' CoreFoundation code. The update includes patches for the Directory Services code as well. Kerberos has been updated to version 5.5.1, which prevents multiple buffer overflows resulting in remote compromise of a KDC or denial of service. The Loginwindow application which handles user accounts, has been repaired to prevent a local user who knows the password for two accounts, from being able to log into a third account without knowing the password. Safari is patched to prevent arbitrary command execution, as also sending of information submitted in a form to the wrong Website. As of now, two updates are available, one for Mac OS X 10.4.2 and the other for 10.3.9. Both are further sub-divided into server and client versions. Apple Website: http://docs.info.apple.com/article.html?artnum=61798

Category 24.8 *MAC OS*

2006-01-26 **Apple Intel microprocessor OS X exploit**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1915923,00.asp 23

APPLE'S SWITCH TO INTEL COULD ALLOW OS X EXPLOITS.

The recent move by Apple Computer to begin shipping Macintosh computers that use microprocessors from Intel could open the door to more attacks against computers running the company's OS X operating system, security experts warn. The change could put more pressure on Apple to build security features into OS X. In an e-mail statement, the company said that the security technologies and processes that have made Mac OS X secure for PowerPC remain the same for Intel-based Macs. However, using the Intel x86 platform pulls Macintosh systems onto the same platform used by Microsoft's Windows computers, a prime target of the hacking community for years. "Attackers have been focused on the [Intel] x86 for over a decade. Macintosh will have a lot more exposure than when it was on PowerPC," said Oliver Friedrichs, a senior manager at Symantec Corp. Security Response. There are many more malicious hackers who understand the x86 architecture in-depth than understand the PowerPC. And attackers have access to hundreds of documents and examples of how to exploit common vulnerabilities on x86, whereas exploits for PowerPC are far fewer, Friedrichs said.

Category 24.8 MAC OS

2006-03-07 **Mac OS X vulnerability patch scrutiny new flaw hole**

DHS IAIP Daily; http://news.com.com/Mac+OS+X+patch+faces+scrutiny/2100 −1002_ 3−6046588.html?tag=cd.top 23

MAC OS X PATCH FACES SCRUTINY.

An Apple Computer patch released last Wednesday, March 1, that doesn't completely fix a high-profile Mac OS X flaw, leaving a toehold for cyber attacks, experts said. The update added a function called "download validation" to the Safari Web browser, Apple Mail client, and iChat instant messaging tool. The function warns people that a download could be malicious when they click on the link. Before that change, clicking on a link could have resulted in the automatic execution of code on a Mac. But Apple failed to address a key part of the problem; the fix should be at a lower, operating system level, experts said. It is now still possible for hackers to construct a file that appears to be a safe file type, such as an image or movie, but is actually an application, they said.

Category 24.8 MAC OS

2006-03-08 **Mac OS X hacking contest shut down too easy**

DHS IAIP Daily; http://www.informationweek.com/security/showArticle.jhtml?ar ticleID=181502078 23

HACK-MY-MAC CHALLENGE LEAVES SYSTEM SHIPSHAPE.

Dave Schroeder, a University of Wisconsin systems engineer who said a Swedish Hack-My-Mac contest was too easy, closed down his own challenge Tuesday, March 7. The machine ran Mac OS X 10.4.5 with the latest security updates and had two local accounts. In addition, Schroeder left both SHH and HTTP open. The mini garnered attention and lots of traffic, said Schroeder, who logged 4,000 attempts. The machine weathered two denial-of-service attacks, various Web exploit scripts, SSH dictionary attacks, and untold probes by scanning tools, he added.

Category 24.8 MAC OS

2006-03-08 **University of Wisconsin-Madison computer hacking contest Mac OS X stopped**

EDUPAGE; http://news.com.com/2100-7349_3-6047735.html 23

WISCONSIN HACKER CONTEST OUT OF BOUNDS

Officials at the University of Wisconsin-Madison have pulled the plug on a Mac OS X hacking contest started by a systems engineer at the university. The engineer, Dave Schroeder, connected a Mac computer to the university's network and invited hackers to try to compromise the machine within five days. Schroeder did not, however, clear the contest with his superiors, and when the institution's CIO learned of it, the computer was removed from the network and the contest was over. Brian Rust, spokesperson for the university, said the contest "was not an activity authorized by the UW-Madison." Rust noted that the institution's "primary concern is for security and network access for UW services," saying that during the time of the contest the university "was able to handle the traffic, and there were no compromises to university systems." Rust said that although Schroeder was "well-meaning," he will have to conduct such experiments in the future on his own, "not using university systems."

Category 24.8 MAC OS

2006-03-14 **multiple vulnerability fixes Mac OS X update**

DHS IAIP Daily; http://secunia.com/advisories/19129/ 23

MAC OS X SECURITY UPDATE FIXES MULTIPLE VULNERABILITIES.

Apple has issued a security update for Mac OS X, which fixes multiple vulnerabilities. Analysis: Under certain circumstances, it is possible for JavaScript to bypass the same origin policy via specially crafted archives. A boundary error in mail can be exploited to cause a buffer overflow via a specially crafted e-mail. This allows execution of arbitrary code on a user's system if a specially crafted attachment is double clicked. An error in Safari/LaunchServices can cause a malicious application to appear as a safe file type. This may cause a malicious file to be executed automatically when visiting a malicious Website. Solution: Apply Security Update 2006-002. Mac OS X 10.4.5 (PPC): http://www.apple.com/support/dow...yupdate2006002macosx1045p pc.html Mac OS X 10.4.5 Client (Intel): http://www.apple.com/support/dow...006002macosx1045clientint el.html Mac OS X 10.3.9 Client: http://www.apple.com/support/dow...rityupdate20060021039clie nt.html Mac OS X 10.3.9 Server: http://www.apple.com/support/dow...rityupdate20060021039server.html

---

Category 24.8 MAC OS

2006-04-06 **Mac threats Windows installation special security issues**

DHS IAIP Daily; 23
http://www.techweb.com/wire/security/184429499;jsessionid=TX
CXZFKVJIOF0QSNDBOCKH0CJUMEKJVN

MAC USERS MAY MEET WINDOWS THREATS.

Users installing Windows XP on Intel-based Macs face some special security issues, a security expert said Thursday. By applying Apple Computer's just-released Boot Camp, Mac owners can now create a dual-boot system that runs either Mac OS X or Windows XP. It's the latter that worries Ken Dunham, the director of the rapid response team at security intelligence firm iDefense. "When a Mac is booted into Windows, it can be attacked by the same [exploits] that threaten any Windows PC," said Dunham. "If you're running an unpatched version of Windows XP on any box, it'll be hacked pretty quickly." But it's not the vulnerability of Windows that concerns Dunham; it's the fact that the Mac will have multiple operating systems on its hard drive. Typically, argued Dunham, people are less diligent about updating their secondary system.

Category 24.8 MAC OS

2006-04-18 **Apple Mac OS X security update J2SE security bypass vulnerabilities solution update**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2006/1398 23

APPLE MAC OS X SECURITY UPDATE FIXES J2SE SECURITY BYPASS VULNERABILITIES.

Apple has released security updates to address multiple vulnerabilities identified in J2SE. These flaws could be exploited by malicious Websites to compromise a vulnerable system. Analysis: A security vulnerability in Java Web Start may allow an untrusted application to elevate its privileges. Due to an issue handling input method events, it is possible that key events intended for a secure field such as a password field may be sent to a normal text field in the same window. This could result in accidental password disclosure to others present when the password is entered. Affected products: Apple Mac OS X version 10.4.5; Apple Mac OS X Server version 10.4.5. Solution: Upgrade to J2SE 5.0 Release 4 (Intel): http://www.apple.com/support/downloads/j2se50release4intel.h tml Or J2SE 5.0 Release 4 (PPC): http://www.apple.com/support/downloads/j2se50release4ppc.html

---

Category 24.8 MAC OS

2006-05-05 **research leap Mac vulnerabilities McAfee Avert Labs**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1958180,00.asp 23

RESEARCHERS CHART LEAP IN MAC VULNERABILITIES.

The volume of security vulnerabilities discovered in Apple's Macintosh platform has increased significantly over the last several years, according to a new report released by McAfee's Avert Labs. The security software maker contends that the number of flaws found in the Mac operating system has increased by 228 percent since 2003. While the researchers said the number of serious vulnerabilities isolated in the latest version of Apple's operating system software, Mac OS X, is dwarfed by the quantity of problems unearthed in Microsoft's rival Windows during the same period, McAfee maintains that as Apple's products have become more popular, a larger number of glitches are being identified. Perhaps even more disturbing, based on how closely Apple can tie its current wave of success to hot-selling consumer multimedia products, McAfee said that many of the reported issues have actually been related to the company's iPod devices and iTunes download service. McAfee Avert Labs whitepaper: http://download.nai.com/products/mcafee-avert/WhitePapers/Ne wAppleofMalwaresEye.pdf

---

Category 24.8 *MAC OS*

2006-05-11 **Apple Mac OS X multiple remote client-side code execution vulnerabilities arbitrary command execution solution update**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2006/1779 23

APPLE MAC OS X MULTIPLE REMOTE AND CLIENT-SIDE CODE EXECUTION VULNERABILITIES.

Apple has released security updates to address thirty-one vulnerabilities identified in Mac OS X. These flaws could be exploited by attackers to execute arbitrary commands, bypass security restrictions, disclose sensitive information, or cause a denial-of-service. Affected products: Apple Mac OS X version 10.4.6 and prior; Apple Mac OS X Server version 10.4.6 and prior; Apple Mac OS X version 10.3.9 and prior; Apple Mac OS X Server version 10.3.9 and prior. Solution: Security Update 2006-003 for Mac OS X 10.4.6 Client (PPC): http://www.apple.com/support/downloads/securityupdate2006003 macosx1046clientppc.html Security Update 2006-003 for Mac OS X 10.4.6 Client (Intel): http://www.apple.com/support/downloads/securityupdate2006003 macosx1046clientintel.html Security Update 2006-003 for Mac OS X 10.3.9 Client: http://www.apple.com/support/downloads/securityupdate2006003 1039client.html Security Update 2006-003 for Mac OS X 10.4.6 Server: http://www.apple.com/support/downloads/securityupdate2006003 1046server.html Security Update 2006-003 for Mac OS X 10.3.9 Server: http://www.apple.com/support/downloads/securityupdate2006003 1039server.html

---

Category 24.8 *MAC OS*

2006-05-12 **US Computer Emergency Readiness Team US CERT alert Apple Mac product multiple vulnerabilities**

DHS IAIP Daily; http://www.uscert.gov/cas/techalerts/TA06−132A.html 23

US-CERT TECHNICAL CYBER SECURITY ALERT TA06-132A: APPLE MAC PRODUCTS AFFECTED BY MULTIPLE VULNERABILITIES.

Apple has released Security Update 2006-003 to correct multiple vulnerabilities affecting Mac OS X, Mac OS X Server, Safari Web browser, Mail, and other products. The most serious of these vulnerabilities may allow a remote attacker to execute arbitrary code. Impacts of other vulnerabilities include bypassing security restrictions and denial of service. Systems affected: Apple Mac OS X version 10.3.9 (Panther) and version 10.4.6 (Tiger); Apple Mac OS X Server version 10.3.9 and version 10.4.6; Apple Safari Web browser; Apple Mail. Previous versions of Mac OS X may also be affected. Please see Apple Security Update 2006-003 for further information. Apple Security Update 2006-003 resolves a number of vulnerabilities affecting Mac OS X, OS X Server, Safari Web browser, Mail, and other products. Further details are available in the individual US-CERT Vulnerability Notes: VULNERABILITY#519473: http://www.kb.cert.org/vuls/id/519473 Solution: Install Apple Security Update 2006-003: http://docs.info.apple.com/article.html?artnum=303737 This and other updates are available via Apple Update: http://docs.info.apple.com/article.html?artnum=303737 For additional protection, disable the option to "Open 'safe' files after downloading," as specified in "Securing Your Web Browser": http://www.us-cert.gov/reading_room/securing_browser/#sgeneral

---

24.9 Peer-to-peer networking

Category 24.9 *Peer-to-peer networking*

1997-03-05 **web hack sabotage vandalism**

NASA

One of the NASA administrators posted part of the text of the NASA Web page hack on the USENET.

Category 24.9 *Peer-to-peer networking*

1997-03-09 **penetration Web hack vandalism hacktivists**

EDUPAGE

Criminal hackers with either a sophomoric sense of humor or truly deluded worldview cracked security on the NASA Web site and posted a childish diatribe against commercial use of the Internet. They also posted threats to destroy corporate America within a month using electronic terrorism. They demanded the release from jail of convicted criminal hackers.

Category 24.9 *Peer-to-peer networking*

1997-03-13 **penetration vandalism Web hack**

EDUPAGE

NCAA site was smeared with racist graffiti. Site managers allege that a 14-year old high school student was responsible and have turned over their evident to the FBI.

Category 24.9 *Peer-to-peer networking*

1997-04-15 **Web insurance**

PR Newswire

The InsureSite insurance policy was announced by the Risk and Insurance Management Society. The policy covers third-party liability for monetary losses due to problems on the covered Web site; personal injury resulting from breach of privacy; and physical damage due to vandalism, viruses and other perils. Clients whose Web sites are certified by the NCSA's Web Certification program are eligible for significant discounts.

Category 24.9 *Peer-to-peer networking*

1997-05-08 **Web hacking penetration**

Polish Radio 1, Reuters

Hackers vandalized the Web page of the Prime Minister of Poland, changing headers to "Hackpublic of Poland" and "Government Disinformation Center." A government spokesperson minimized the threat, saying that the Web system is not linked to other government computers and no confidential information was compromised.

Category 24.9 *Peer-to-peer networking*

1997-05-14 **Web vandalism hacktivism**

RISKS 19 14

According to Martin Minnow, regular contributor to RISKS from Sweden (direct quotation of Mr Minnow's posting),

>The Swedish newspaper *Svenska Dagbladet* reports that the Swedish meat packers, Scan, had their web page replaced by an unknown attacker. The new page looked much like the old, but with changed text, including: "Now we're making our packages EVEN smaller, so that YOU the consumer can buy our meat for even lower prices. Boycott nasty vegetables. Eat more meat, smile, and be happy. And, by the way, you sure don't want to turn your stomach into a composter, right?" [My free translation.]

The page's links take you to the Animal Rights Law Center, McDonalds, and Flashback, a home on the net for a number of underground movements.<

Category 24.9 *Peer-to-peer networking*

1997-05-23 **penetration hacking Web**

Reuters, Newsbytes

Koichi Kubojima (or "Kuboshima"), a 27-year-old computer engineer, was arrested in Tokyo and charged with replacing weather pictures by pornography on the Asahi Broadcasting Co. web pages. He was the first person to be charged under the 1987 anti-hacking law and faces up to five years in jail because of stiff penalties added to the law in 1992. According to Martyn Williams of Newsbytes, "Police tracked down Kuboshima by gaining access to the records of an Internet service provider that he reportedly used to carry out the hack. Local press reports said the account was opened with a false credit card number and name." The site was taken out of service within 10 minutes of the hack at 10:00 and was back on air by 13:00.

Category 24.9 *Peer-to-peer networking*

1997-05-29 **Web hack vandalism penetration**

UPI, OTC

UPI reported that the Los Angeles Police Department Web page was hacked and satirical content substituted for the normal texts. However, investigation by revealed that the tale was itself an error that spread like wildfire through the Net. It seems that someone did post a lampoon of the LAPD's page at a completely separate site <www.dis.org/se7en/hacktrash/lapd/index.html> and it did include disrespectful language. However, no one broke into the real LAPD site.

On the other hand, claims that Universal Studios' Web hack was a deliberate publicity stunt by the Studios were vigorously denied by spokespersons, who pointed out how pointless it would be to put a fraudulent hack up for all of five hours — from 03:00 until 08:00. The key points in the rant published by Glen Lipka were that the graphics were too good and that date stamps on the graphics files preceded the stamps on the original Web page; neither observation leads unavoidably to the conclusion of fraud. Good graphics packages are available to everyone; and date stamps mean nothing when it's PCs that stamp the files.

Category 24.9 *Peer-to-peer networking*

1997-05-31 **Web vandalism**

RISKS 19 20 ff

According to Reuters, >The opening page for the Web site for the film ``The Lost World: Jurassic Park'' wasn't all it was quacked up to be after hackers got through with it Tuesday. In place of the film's trademark dinosaur logo was a profile of a prehistoric-looking duck, accompanied by the title ``The Lost Pond: Jurassic Duck.'< A later item in RISKS pointed out that the correct form of that vandalism was "The Duck World: Jurassic Pond" which is just as silly. Some cynics argued that the hack was likely to be an inside job and maybe a deliberate hoax; no proof, however, of this conjecture.

Category 24.9 *Peer-to-peer networking*

1997-06-03 **Web vandalism hacking**

EDUPAGE

In Delaware, police arrested a teenager accused of defacing the NASA Web site and leaving graffiti describing site administrators as "extremely stupid." The kid's computer was seized as evidence.

Category 24.9 *Peer-to-peer networking*

1997-06-24 **Web hacker vandalism denial of service**

EDUPAGE

Microsoft's Web site was down for about 10 minutes after a cracker exploited a known flaw in the MS server software. MS posted a fix immediately and got its system up with a simple reboot.

Category 24.9 *Peer-to-peer networking*

1997-07-19 **denial of service mail bombing Web infowar**

Reuters

A Web site supporting ETA guerrillas was mailbombed after ETA killed a Spanish politician. The Euskal Herria Journal of New York was pulled off the Web site of the Institute for Global Communications after its servers were brought to their knees by the flood of duplicate messages and huge binary files sent by opponents of ETA.

Category 24.9 *Peer-to-peer networking*

1997-07-25 **Web vandalism**

Polish News Bulletin

For the second time in three months, hackers broke into the Polish government's computer systems and altered its Internet site, Government Information Centre (CIR) officials admitted. A hacker calling himself "Cyberbob" added several new messages to the Polish-language page: "Lech W. for President," "he he he meee meee" and "Al. Zachlapana 1/3 00-583 Pruszkow," also notifying users of a change in the CIR server's address to "www. playboy.com."

Category 24.9 *Peer-to-peer networking*

1997-08-07 **hackers Web vandalism**

UPI

In late July, someone attacked the Web site of the Minnesota Department of Public Safety; an entire day of work was deleted. Ten days later the site was attacked again and all access to public e-mail was shut down.

Category 24.9 *Peer-to-peer networking*

1997-08-14 **hacker Web server vandalism ISPs FBI**

Editor & Publisher 130 26

An official of the San Antonio Express-News revealed in August that his company's Web servers were severely damaged by one or more hackers in mid-April. Eight other regional ISPs were damaged in the attacks. Suspects under investigation by the FBI included a high-school student and more experienced Unix hackers. Logic time-bombs were left on the system that eventually interpreted harmless files commands as instructions to delete files. The servers crashed completely soon after the time-bombs detonated. He estimated that 300,000 pages on his Web site were damaged. The newspaper offered a $25,000 reward for information leading to conviction of the perpetrators and this apparently resulted in many helpful leads for investigators.

Category 24.9 *Peer-to-peer networking*

1997-08-19 **Web vandalism hack password intrusion**

Grand Rapids Press

A poorly-chosen password allowed hackers to vandalize First Michigan Bank Corp's WWW site. The main page was replaced by a solid black background with a few identifying scribbles. Luckily, the bank suffered few damages.

Category 24.9 *Peer-to-peer networking*

1997-09-11 **Web security cracking vandalism**

EDUPAGE

Computer Security Canada Inc. posted a database of Web site security breaches; see <http://www.csci.ca/>.

Category 24.9 *Peer-to-peer networking*

1997-09-30 **Web vandalism hacker**

2600

AirTran Airways (formerly ValuJet) saw its Web site vandalized in September, with gross references to the 1996 crash that killed 110 people.

Category 24.9 *Peer-to-peer networking*

1997-12-09 **Web hack vandalism extortion**

AP

In early December, hackers attacked the Yahoo site, leaving electronic graffiti threatening a massive logic-bomb attack on the planet's networks on Christmas day and a nationwide power-system failure on

---

Category 24.9 *Peer-to-peer networking*

1998-02-11 **criminal hackers Web vandalism penetration**

XINHUA

In Israel, the Knesset's Web site was entered by apparently well-meaning criminal hackers. Instead of the usual pornography and other juvenalia, these criminals simply left a note (in bad English, for some reason) claiming to have plugged 19 security holes that allowed penetration. Funny way of helping. . . .

Category 24.9 *Peer-to-peer networking*

1998-03-13 **hack penetration Web vandalism script attack military**

RISKS 19 63

The Web sites of the Army Air Defense Artillery School, the Army 7th Signal Brigade[*], and the Army Executive Software Systems Directorate were all vandalized on 8 March. The vandals left messages about the recent attacks on Pentagon Web sites.

Category 24.9 *Peer-to-peer networking*

1998-05-30 **penetration Web vandalism attacks**

RISKS 19 77

Steven Slatem, reporting from Prague, reported a continuing two-year onslaught on Czech and Slovak Web sites by a criminal hacker group calling themselves "CzERT" (a reference to the Czech word for devil or demon). These vandals have damaged sites for 28 sites as of May 1998, including "Czech Army, a bank, a Web chat site (hackers posted list of alleged software pirates), a search engine site, a magazine for police, ISPs (little animated e-man sauntered across the screen and pissed on the ISP's logo), a couple of daily news sites, a press agency (delivered their own news story), a computer magazine site, UNICEF's site, software vendors' sites, schools, various ministries and more."

Category 24.9 *Peer-to-peer networking*

1998-05-30 **Web site attack vandalism penetration data diddling**

RISKS 19 77

A criminal hacker used the sheer size of AOL's technical support (6,000 people) to attack the ACLU's Web site. The attacker repeatedly phoned AOL until he found a support technician foolish enough to grant access to the targetted Web site, which was wiped out. AOL promised to change its procedures for training their harried staff.

Category 24.9 *Peer-to-peer networking*

1998-09-15 **attack vandalism Web site hackers criminal political**

EDUPAGE

"Hackers for Girlies" (HFG) vandalized the New York Times Web site. Professor Lance Hoffman of George Washington University commented, "The material posted by the hackers is offensive, childish, threatening and chilling. It's a good example of why we have to bring accountability to the Internet."

Category 24.9 *Peer-to-peer networking*

1998-09-17 **Web vandalism attack DoD vulnerabilities risk**

EDUPAGE

The DoD, alarmed by the increasing frequency of successful attacks on Web sites, ordered a thorough review of its own security precautions for its non-classified Web sites.

Category 24.9 *Peer-to-peer networking*

1998-09-23 **Web attacks vandalism criminal hackers crackers DoD**

RISKS 19 97

According to the nominated Assistant Secretary of Defense for C3I (Command, Control & Communications), Art Money, "Cyberterrorists have hacked into and altered the Defense Department's medical World Wide Web pages that contain information on troops' blood types." Actually, though, the attacks on an incomplete demonstration model of the DoD Defense Blood Standard System and were simulated by official Red Team DoD staff in a tiger team exercise. Furthermore, according to a DoD spokesperson, no data were altered. Finally, the real blood systems are on stand-alone computers that are not connected to the Internet.

Category 24.9 *Peer-to-peer networking*

1998-12-07 **information warfare vandalsim Web defacement hacker trust**

Wall Street Journal / Dow Jones

Don Clark presented an interesting overview of the Web-vandalism phenomenon in the Wall Street Journal in December. He noted the parallel between the filth-strewn language of the Web vandals and the spray-painted obscenities on building walls but then added that vandalism is damaging public perceptions of safetey on the Internet.

Category 24.9 *Peer-to-peer networking*

1999-01-16 **DNS reference pornography hijack URL 404 link**

RISKS 20 17

Daniel Tobias was startled to be criticized by a colleague who complained that his Web page included a link to a pornographic Web site. Indeed, one of Mr Tobias' originally inoffensive links did indeed now go to a porn site. The problem turned out to be a Web URL hijacking: the original owner of a domain either sold its domain to the pornographer or allowed the domain registration to lapse. The new domain owner programmed his Web site to link all references to the original pages at the original domain to point to his home page instead of returning a "404 Not Found" message. [MK comments: Net hygiene dictates that one check one's links regularly.]

Category 24.9 *Peer-to-peer networking*

1999-01-21 **vandalism Web attack damage Trojan Horse**

New York Times

The US Information Agency's Web site was severely damaged in January by vandals who installed Trojan Horse software.

Category 24.9 *Peer-to-peer networking*

1999-02-12 **Web server write-protect switch hardware**

RISKS 20 21

Electrical engineer Ian Cargill asked in RISKS why Web servers couldn't have hardware-based switches to prevent writing on the disks without authorization. It turns out that some hard disks do indeed have a write-protection jumper that could easily and cheaply be wired to an external switch. However, Nigel Rantor replied in the following issue that there were several problems with such a scheme: (1) Most Web sites have dynamic content that resides on the Web server (in part because many Web managers have no idea how to implement a back-end to a database on another server) and must therefore be in write-permit mode all the time; (2) many Web servers are hosted at third-party locations; asking for someone to flip a switch many times a day would be unacceptable. Mr Rantor also pointed out that even if the available methods for write-protection (firewalls, ACLs) are perfectly implemented, there are other ways of harming Web sites, such as denial-of-service attacks.

Category 24.9 *Peer-to-peer networking*

1999-04-01 **information warfare Web vandalism hacktivism April Fool's**

OTC

In a tasteless April Fool's joke (what other kind is there?), radio personality Art Bell's site on the Web claimed to have been hacked. The supposedly damaged site included text reading, "The Yugoslav Citizens' Message To Nato World Criminals" and urged worldwide protests against the NATO bombing campaign. Actually the site was altered by its owners in a stupid display of insensitivity toward people on both sides of a dreadful war.

Category 24.9 *Peer-to-peer networking*

1999-05-12 **criminal hacker Web vandalism**

OTC

The White House Web site was shut down for a day on 1999-05-11 after hackers attacked the server; NBC reported that the intruders left graffiti critical of NATO operations in Kosovo.

Category 24.9 *Peer-to-peer networking*

1999-07-01 **Web penetration vandalism political message criminal hackers**

InternetWeek

Criminal hackers vandalized the Web site of the State of Hawaii, leaving electronic graffiti with political statements on the damaged home page.

Category 24.9 *Peer-to-peer networking*

1999-08-02 **criminal hackers penetration Web vandalism hoax**

Newsbytes, Dow Jones, San Jose Mercury News

The Symantec Inc. Web site was hacked on 1999-08-01 and hoax claims of worm infection of the anti-virus company's products were left on the site. The hack was noticed by Dutch Symantec employees about an hour after the damage occurred. The company immediately notified the FBI.

Category 24.9 *Peer-to-peer networking*

1999-08-03 **criminal hackers penetration Web vandalism**

Newsbytes

A criminal-hacker gang calling itself HFD (Hacking for Drunks) vandalized the Jerry Springer Show Web site. The modified page included text such as, "Drunken hackers: The women who love them and the admins who fear them" and "On the next Jerry Springer... Meet beercan, b33rman, and beerb0ttl3. Three young men who have given there (sic) up their lives to alcohol abuse and computer hacking. They have agreed to come on Jerry to tell there story." Surprisingly, someone actually noticed that the subliterate, error-packed announcement of an ridiculous upcoming show was a hoax.

Category 24.9 *Peer-to-peer networking*

1999-08-06 **criminal hacker Web penetration vandalism**

AP

Someone using an IP address in Russia vandalized the anti-hacker AntiOnline site on 2000-08-05 by taking advantage of an unusual feature of the site. AntiOnline provides links to discussions taking place on other sites. Someone put executable code in a message that allowed the perpetrator to alter some links in the "Eye on the Underground" on the AntiOnline site. While the sabotage was unrepaired (about an hour), visitors clicking on the damaged link were shunted to a Web site showing an eye and the message, "Expensive security systems do not protect from stupidity." It was unclear whether the author of the message was making a self-reference or criticizing John "JP" Vranesevich, who had recently announced his intentions to aid law enforcement authorities in tracking and prosecuting criminal hackers.

Category 24.9 *Peer-to-peer networking*

1999-08-10 **international conflict information warfare INFOWAR hackers vandalism penetration Web sites governments**

Wall Street Journal, Reuters

China and Taiwan extended their conflict over national identity into cyberspace in 1999, with hackers on both sides of the Taiwan Strait attacking each country's Web sites. Mainland hackers attacked Taiwanese Web sites with Chinese and English messages such as "Taiwan is indivisible part of Chinese territory and will always be! The Taiwanese government headed by Lee Teng-hui cannot deny it!" Taiwanese hackers penetrated Web sites of the China Securities Regulatory Commission and a Shaanxi government agency where they posted Taiwan's national flag and national anthem and messages such as "Go to the mainland to fight the Communists."

Category 24.9 *Peer-to-peer networking*

1999-08-11 **criminal hackers Web vandalism penetration**

OTC Newsbytes

The Federal Energy Regulatory Commission (FERC) Web site was vandalized on 1999-08-10 at 04:30 and was repaired by 07:00. The vandals posted a cartoon of a woman holding a whip and the words "Hacked by Sarin."

Category 24.9 *Peer-to-peer networking*

1999-08-27 **criminal hackers hactivists penetration Web site redirection hijack**

DataLounge Weekly News Recap

For a period of two days, the absurdly homophobic site <www.godhatesfags.com> was hijacked so that visitors to the hateful site were shunted to <www.godlovesfags.com>. As one commentator wrote, "While we can't applaud the hijacking of domains, we do appreciate the moral imperative that drove someone to temporarily replace a message of hate with a message of tolerance — and say in all sincerity that it couldn't have happened to a nicer bunch of folks."

Category 24.9 *Peer-to-peer networking*

1999-09-08 **criminal hackers Web vandalism racism government**

Newsbytes

The Level Seven Crew gang of criminal hackers, claiming 39 unauthorized penetrations of computer systems in 1999 alone, vandalized the Web sites of the US embassy in Beijing and the Federal Graphic Data Committee in early September. The embassy site's home page was replaced by a document containing racist comments about China and sneers and both the FBI and at other crmininal hacker groups.

Category 24.9 *Peer-to-peer networking*

1999-09-15 **criminal hackers Web vandalism obscenity government**

Reuters

A criminal hacker gang calling itself "B1nary Outlawz"damaged the Web site of Statistics SA, leaving a page full of obscenities on screen instead of the usual consumer price data. Apparently the penetration occurred because of vulnerabilities in the Web hosting service provided by the SA Internet Exchange (Saix), a subsidiary of South Africa Telekom. There was initial suspicion that the vandalism might have been an inside job, as there was a labor dispute in progress at the time. This suspicion was not borne out by later evidence.

Category 24.9 *Peer-to-peer networking*

1999-09-15 **criminal hackers gang group attack penetration Web site stock exchanges vandalism**

Dow Jones, AP

The United Loan Gunmen criminal hacker gang vandalized the NASDAQ and American Stock Exchange in September. For Hallowe'en, the ULG vandalized the Associated Press Web site, leaving a greeting and a poem by Edgar Allan Poe on the home page.

Category 24.9 *Peer-to-peer networking*

1999-09-15 **criminal hackers Web penetration vandalism**

AP, Reuters, Wall Street Journal

A new criminal hacker gang calling itself "United Loan Gunmen" vandalized Internet gossip-monger Matt Drudge's Web site and then that of C-SPAN cable news network on 1999-09-05, leaving a badly-designed hoax claiming that the US government had conspired to foment conflict in the Middle East in 1983. The farce quoted "the Secretary of War at the State Department," a non-existent post. On the 15th of September, the same group attacked the Web sites of the NASDAQ and the American Stock Exchange. They left cybergraffiti claiming that they could have manipulated stock prices (apparently false) and that they had created e-mail accounts for themselves.

Category 24.9 *Peer-to-peer networking*

1999-10-05 **vandalism Web attack defacement sabotage**

Straits Times (Singapore)

Three Singapore Web sites were defaced in early October by the criminal hacker calling him/herself "Mistuh Clean." The hacker blanked the home pages and left the electronic graffito, "owned…can we say more?" Local authorities wondered how they would proceed legally if the perpetrator turned out to be a foreign national living abroad. One mitigating circumstance is that the criminal may have been responsible for hacking into two US computer systems as well.

Category 24.9 *Peer-to-peer networking*

1999-10-19 **criminal hacker Web site penetration vandalism**

Wired http://www.wired.com/news/print/0,1294,31986,00.html

In October 1999, someone broke into the official Web site for George W. Bush Jr and replaced his picture with a hammer and sickle — the emblem of the Communist movement. To add injury to insult, the intruders placed links to the International Communist League on the vandalized page. The campaign's Web site is hosted on the Illuminati Online hosting service based in Autin, TX. Analysis by external security experts revealed that the Web site was basically unprotected against intrusion.

Category 24.9 *Peer-to-peer networking*

1999-10-26 **criminal hackers vandalism government Web damage Windows NT phreak.nl**

NEWSBYTES NEWS NETWORK

A criminal hacker or hacker group calling itself "phreak.nl" has been attacking US Web sites in the last week of October 1999. According to a Newsbytes article by Bob Woods dated 1999-10-26, the criminals damaged Web sites of NASA's JPL, the US Army's Redstone Arsenal's Program Executive Office and the National Defense University. All these sites were described by a hacker-publicity group, "attrition.org" as running WindowsNT servers. The defacements consisted of the usual puerile sneers and insults in the peculiar spelling affected by the criminal hacker subculture. One common theme was the notion that "phreak.nl" was engaged in "a game ... called hack the planet." In addition to these attacks, "phreak.nl" also damaged sites for All Timeshare, Pet GBets and WPYC. Anyone wishing to see copies of the damaged sites can do so at <http://www.attrition.org> but readers are urged to use caution when visiting any such site. Don't run active content, don't allow cookies and use a firewall on your workstation to preclude unauthorized activity.

Category 24.9 *Peer-to-peer networking*

1999-11-01 **criminal hackers Web vandalism prank satire government ministry**

AP

Criminal hackers penetrated the Web site of the Romanian Finance Ministry. The cybervandals left satirical content introducing taxes on stupidity and laying out an official plan to bribe NATO so that Romania could enter the military alliance quickly. There were no laws in Romania making such unauthorized activities illegal.

Category 24.9 *Peer-to-peer networking*

1999-11-14 **criminal hackers Web site defacement vandalism government**

Newsbytes

Several incidents in November reminded the world of the ongoing problems with hacking in Asia. A HK government website run by the Highways Department was trashed; the Chinese Ministry of Foreign Affairs suffered a similar indignity, with replacement of the home page by a blank screen with a few criminal hacker boasts and obscenities. In a related story, China announced that a former bank employee, Zhao Zhe of Shanghai, was sentenced to three years in prison for breaking into the computers of the Shanghai branch of a Hainan securities firm and altering share prices in a failed stock-manipulation scheme. In Singapore, criminal hackers defaced the Web sites of The Singapore Government Shopfront and the Ministry of Law's Integrated Land Information Service (INLIS) Web site.

Category 24.9 *Peer-to-peer networking*

1999-11-16 **Web vandalism attack penetration defacement court conviction sentencing**

Straits Times (Singapore)

In September 1999, someone calling him/herself "mistuh clean" vandalized the Web site of Mediacity, part of the Television Corporation of Singapore's network. Evidence suggested that the criminal hacker might not be a local but rather a foreigner, possibly a Canadian resident. The criminal contacted Victor Keong, a Canadian security consultant using e-mail to inform him of the vandalism, and Mr Keong called Mediacity to warn them of the tampering.

In November 1999, eighteen-year-old student Edwin Lim Zhaoming admitted having broken into the Television Corporation of Singapore (TCS) website on 15 June with the help of a Burmese confederate aged 15. Among other damage, the vandals renamed the site "Mediashity." The juvenile confederate who told him about an easy user-ID and password to penetrate the site was sentenced to 12 months probation and 100 hours of community service. The attack consisted of replacing the TCS Web site with a page larged with vulagarities and abusing Bill Gates; the company estimated that the site was down for 10 hours, took 80 person-hours and cost S$13,000 to recover .

Category 24.9 *Peer-to-peer networking*

1999-11-18 **Web site government vandalism criminal hacker defacement**

Reuters

In Belgium, (a) criminal hacker(s) vandalized several government Web pages, putting offensive messages about a local libel case onto the welcome pages at the Treasury and for an administrative court. Officials claimed that security on those Web pages was low because the information was public. [Come again?]

Category 24.9 *Peer-to-peer networking*

1999-11-18 **criminal hacker Web penetration vandalism**

Reuters

A criminal hacker penetrated the Web sites of the Belgian Treasury and of an administrative court in mid-November. The intruder put up obscene language referring to the legal case in which fashion designer Ann Demeulemeester succeeded in preventing distribution of a satirical book by Belgian writer Herman Brusselmans in which she was named.

Category 24.9 *Peer-to-peer networking*

1999-11-20 **Web vulnerability criminal hackers vandalism government**

Newsbytes

A rash of exploits using Remote Data Service (RDS) allowed criminal hackers to deface several US government Web sites in November, including the Department of Energy (DoE), Federal Aviation Administration (FAA), the National Institutes of Health (NIH), the National Oceanic and Atmospheric Administration (NOAA) and the US Postal Service (USPS). Damage included graffiti in some cases but wholesale replacement of entire pages in others.

Category 24.9 *Peer-to-peer networking*

1999-12-07 **criminal hacker Web site redirection information warfare lawsuit John Doe**

UPI, OTC

On 1999-10-09, someone breached security on the Staples Web site and redirected browsers to the Web site of Office Depot, the victim's major competitor. On 1999-11-30, Staples announced on that it filed a federal "John Doe" lawsuit against its assailant(s) claiming damages for lost business and for the recovery effort. Staples and Office Depot both said they doubted that Office Depot was in any way responsible for the attack.

Category 24.9 *Peer-to-peer networking*

1999-12-07 **Web vandalism criminal hackers**

Business Day (Johannesburg, RSA) via OTC

The criminal hacker group calling itself "B1nary Outlawz" attacked the Web sites of the South African Police Service and about a dozen other Johannesburg-based Web sites. The vandalism included obscenities directed at the police; the criminals notified the press through e-mail. The same group claimed responsibility for damaging the Web site of the Statistics SA department in September. In an apparently unrelated hack the Statistics department was hacked from a US address in November.

Category 24.9 *Peer-to-peer networking*

1999-12-12 **criminal hackers hactivists political propaganda Web penetration vandalism government**

ITAR-TASS, Reuters

Criminal hacker gangs calling themselvs "The Princes of Darkness" and "The Angels of Freedom" penetrated the Web site of the official Russian ITAR-TASS news agency. The intruders posted verbiage protesting the warn in Chechnya.

Category 24.9 Peer-to-peer networking

2000-02-18 **peer-to-peer networking risks**

KTSL http://www.ktsi.net/whsecurityp2p.html 20 76

"Security Concerns for Peer-to-Peer Software" by Mike Petruzzi <mpetruzzi@ktsi.com>, Rob Sherwood, John Dunnivan, Rob Chavez and Pat Holley of Key Technologies and Security, Inc. reviews the security implications of programs such as Napster, Gnutella and their possible variants.

The following extracts (slightly reordered) from their well-written paper are reprinted with the kind permission of my old friend and colleague, Fred Tompkins, Senior Vice President of KTSI.

Peer-to-peer (hereafter referred to as P2P) communication software allows individual computers to share and swap various types of files. Recently, P2P software has been much in the news due to current and potential lawsuits. Napster, the company that makes software for exchanging MP3s (encoded music files), is being sued for copyright infringement; the recently re-released Gnutella has the potential for exchanging all types of files and may therefore be embroiled in litigation even more quickly than Napster was.

P2P software takes the idea that the Internet is for sharing to new levels. P2P has been described as "an anarchistic threat to the current Internet" (David Streitfeld, The Washington Post, July 18, 2000) and Marc Andreesen has called P2P software the most important thing on the Internet in the last six years (when Netscape was first released) and a "benevolent virus." Ian Clarke, the creator of FreeNet, says, "People should be free to distribute information without restrictions of any form."

Even protected code is not safe. Programs like AOL Instant Messenger, or any other P2P software, can be reverse engineered and released as Open Source software. These programs can then be released for any operating system platform. This also gives malicious hackers the ability to change the software code so that it can be used for other purposes. This requires a great deal of programming knowledge and skill, but can still be done.

The first obvious concern is the liability of copyright infringement. Even though all of the companies that produce and release P2P software issue warnings regarding the illegalities of downloading copyrighted materials, simply releasing the software makes those illegal acts possible. Some P2P software contains security warnings during the installation of the software and enables default settings to protect the naïve consumer and their computer. But armed with some simple knowledge of the Internet and its protocols, even a beginner criminal hacker can cause many security risks to users of this class of software.

More important than any copyright concerns are the potential security concerns for corporations and consumers. For corporations, P2P software threatens:
• bandwidth consumption
• liabilities and acceptable use violations
• undermining of security policies
• Trojan Horse and virus distribution
• disclosure of IP and MAC addresses
• telecommuters.

For individual consumers, P2P software represents:
• disclosure of IP and MAC addresses
• disclosure of connection speed
• file sharing
• Trojan horse and virus distribution.

I hope that readers will go to the KTSI Web site and read the entire article for themselves. The URL is < http://www.ktsi.net/whsecurityp2p.html >.

Category 24.9 *Peer-to-peer networking*

2000-03-07 **intellectual property copyright theft customer relations hostility generation gap**

NewsScan, New York Times
http://www.nytimes.com/library/tech/00/03/biztech/articles/07net.html

The popular Napster software, which enables users to find and copy a wide array of digitized songs as well as share collections with others, is changing the way younger people think about copyrighted music as intellectual property, and the industry fears things may never be the same again. "There's an incredible disconnect out there between what is normal behavior in the physical world versus the online world," says Carey Sherman, general counsel for the Recording Industry Association of America. "There are people who think nothing of downloading entire CD collections on Napster who wouldn't dream of shoplifting from Tower Records. There's just a massive education program that's needed here for people to understand what goes into the creation of music." The RIAA has filed a lawsuit against Napster, which argues that it is not liable for music piracy because it doesn't keep any of the pirated files on its own servers. But punishing the individual consumer is a losing proposition: "One of the fastest ways to turn potential customers off is to say they're all a bunch of thieves," says a copyright expert at UC-Berkeley. "You start hating your customers and your customers are going to start hating you back, and that doesn't bode well for your ability to attract them to buy more stuff from you. It makes them more inclined to infringe rather than buy." (New York Times 7 Mar 2000)

Colleges and universities are split on "the Napster issue." Some are blocking Napster, some are not. Among the ones that are not are Georgia Tech, Michigan, Stanford, Duke, and the University of California at Berkeley. A Georgia Tech official says: "We are an educational institution and we will err on the side of unfettered access to information. Once you start down that road ... well, we could tie up an awful lot of staff people and resources trying to evaluate Web sites' content, and we don't want to get into that." Among the ones that are blocking Napster are Yale, Indiana, Southern California, Texas, Ohio State, Northeastern, and Canisius. The first three in this group made their decisions after being sued by two rock groups and the Recording Industry Association of America; the second two chose to block Napster on the grounds that Napster traffic clogged their computer networks; and the last two cited legal and ethical reasons for rejecting Napster and similar programs. A Canisius official explained: "It's not free for you to steal books from the public library, and it's not free to download music you haven't paid for." (AP/San Jose Mercury News 1 Oct 2000)

Category 24.9 *Peer-to-peer networking*

2000-03-24 **peer-to-peer networking file exchange**

NewsScan, Los Angeles Times
http://www.latimes.com/business/2000324/t000027817.html

Some enterprising computer hackers have come up with a variation on Napster software that helps people search and swap any type of computer file — not just MP3 music files. The variation, dubbed "Wrapster," uses Napster's servers to exchange everything from games and movies to software and spreadsheets by tricking them into thinking the files are in the MP3 format. Napster holds patents on some components of its technology and the company's VP of engineering says it hasn't decided "whether we're going to turn a blind eye to it or actively try to disable it." Napster is currently developing its own systems that would enable other types of files to be traded. (Los Angeles Times 24 Mar 2000)

Category 24.9 *Peer-to-peer networking*

2000-04-25 **intellectual property copyright theft violations marketing publicity e-commerce peer-to-peer**

NewsScan

Criticizing fellow rock artists and who have attacked Napster Inc. for promoting music piracy by allowing people trade and search for files of musical performances downloaded via the Internet and without remunerating artists or record companies, the lead singer of the rock band Limp Bizkit . . . [called] Napster software "an amazing way to market and promote music" and . . . [maintained] that "the Internet is here, anybody trying to fight that, which would be people who are living by certain standards and practices of the record industry ... are the only people who are scared and threatened." The Recording Industry Association of America is suing Napster for piracy and copyright infringement, as is the band Metallica. (Reuters/San Jose Mercury News 25 Apr 2000)

Category 24.9 *Peer-to-peer networking*

2000-04-25 **intellectual property copyright violations theft peer-to-peer lawsuit litigation**

NewsScan, CNet http://news.cnet.com/news/0-1005-200-1760313.html

Rap artist Dr. Dre . . . joined Metallica and the Recording Industry Association of America in suing Napster, whose controversial software, they charge, is responsible for massive copyright violations, primarily by college students who swap tunes using MP3 files. But in a new twist, Dr. Dre's lawsuit targets individual students as well as universities that permit the software to be used on their servers. No individual students or universities are named in the suit filed yesterday, but experts say it's serving as a kind of placeholder, and that five schools and students will be named later. Already, the three universities cited in the Metallica suit have blocked or sharply restricted the use of Napster on their campuses. (News.com 25 Apr 2000)

Category 24.9 *Peer-to-peer networking*

2000-05-09 **intellectual property copyright violation theft lawsuit ruling**

NewsScan, Los Angeles Times
http://www.latimes.com/business/20000509/t000043641.html

The Recording Industry Association of America claimed initial victory in its lawsuit against Napster after U.S. District Court Judge Marilyn Patel rejected Napster's argument that it is a "mere conduit" for pirated music files. The RIAA is hoping for a repeat performance of its recent win over MP3.com. A federal judge in that case ruled that MP3.com violated copyright law with its database that allows users to store music and then access it from any computer connected to the Internet. The RIAA is seeking statutory damages ranging from $500 to $100,000 per sound recording downloaded using Napster's software. Analysts estimated the total could approach hundreds of billions of dollars. (Reuters/Los Angeles Times 9 May 2000)

Category 24.9 *Peer-to-peer networking*

2000-05-30 **intellectual property copyright infringement violation**

NewsScan, http://www.usatoday.com/life/cyber/tech/cth987.htm

Conceptually similar to Napster, the Net software company that makes it easy for users to download and trade copies of songs (either with or without permission of the copyright owners), new sites such as Scour and iMesh have developed software that allows the swapping of photos and videos as well as music. As a result, bootlegged copies of some brand new movies, including the popular "Gladiator," are available free to people willing to spend the time to download them, and willing to ignore copyright laws. Both Scour and iMesh insist they post strict legal notices and they are legitimate entertainment sites, offering authorized "trailers" (movie previews) by arrangement with movie studios such as Miramax. (USA Today 30 May 2000)

Category 24.9 *Peer-to-peer networking*

2000-06-05 **music sharing intellectual property copyright permission legal authorized fair use streaming**

NewsScan

Pointera, a Palo Alto-based startup that launches today, says its service is unique in that it enables portals and users to share files, including digital music files, legally through a standard Web browser. The service is conceptually similar to Napster and Gnutella, but rather than copying the desired files, the user "shares" the file, which remains on the original computer. "We enable the streaming of media files as opposed to people just downloading," says CEO Manish Vij. "What this means is you can just hit play from your hard disk instead of hitting copy. If you're simply playing that's the same as going to someone's house and watching a movie and is still covered by fair use under the copyright laws." The Pointera Search Engine enables portal servers to work directly with individual PCs for file-sharing. "The real issue here is that the technology essentially moves beyond MP3," says Gartner Group's Chris Le Tocq. "The Pointera technology is a business application, which we've never had before. Groups of people can exchange files and work together... The interesting thing here is that this an instant process, it allows for peer to peer architecture. This is very different than the hierarchical architecture found on the Web today." (Internet.com 5 Jun 2000)

Category 24.9 *Peer-to-peer networking*

2000-06-14 **intellectual property peer-to-peer distribution encryption**

NewsScan, New York Times
http://partners.nytimes.com/library/tech/00/06/biztech/articles/14movie.htm

The digital video and music distribution company Sightsound.com is going to use the Gnutella software to transmit movies over the Internet as encrypted files. Giga Information group analyst Rob Enderle says, "We believe that these kinds of distribution schemes will become increasingly common as the music and movie industries realize the kind of threat they are under. SightSound executives are not commenting on the plan because the company is in a "quiet period" before an initial public offering. With Gnutella, the various files shared are stored locally on individual users' machines. The company has said it will use commercially available encryption technology to protect its content. (New York Times 14 Jun 2000

Category 24.9 *Peer-to-peer networking*

2000-06-16 **intellectual property music theft trafficking lawsuit litigation**

NewsScan, San Jose Mercury News
http://www.sjmercury.com/svtech/news/breaking/ap/docs/91264l.htm, New York Times
http://partners.nytimes.com/library/tech/00/06/biztech/articles/16music.htm

[In June,] The Recording Industry Association of America . . . asked a federal judge to grant an injunction preventing Napster, the online service that allows individuals to swap music collections without necessarily observing copyright laws, from "facilitating or assisting others in, the copying, downloading, uploading, transmission or distribution of copyrighted musical works." The request was supported by the Motion Picture Association of America and by MP3.com. MPAA president Jack Valenti . . . [said]: "If Napster can encourage and facilitate the distribution of pirated sound recordings, then what's to stop it from doing the same to movies, software, books, magazines, newspapers, television, photographs or video games?" (AP/San Jose Mercury News 13 Jun 2000)

Defending itself against a copyright lawsuit against the Recording Industry Association of America for making it possible for over 10 million computers users to share copyrighted files, the Internet music distribution company Napster.com . . . [said in June] that it should not be sued just because it is operating on a large scale. Napster's position is that the RIAA would never sue a single individual for copying a song or movie and giving it to a friend, and so it should not be suing Napster just for facilitating such behavior on a large scale. Without conceding that it is lawful for users to share music one-on-one, the recording industry . . . [said] that "there can be no question it is unlawful when done on a large scale, as with Napster." (New York Times 16 Jun 2000)

Category 24.9 *Peer-to-peer networking*

2000-07-12 **wireless communication Internet access e-mail peer-to-peer networking**

NewsScan, New York Times
http://partners.nytimes.com/library/tech/00/07/biztech/articles/12cybiko.html

Seeing "a huge opportunity with 12-16 year olds," the New York start-up company Cybiko is marketing a $129 device with an LCD screen, small keyboard, and the ability to communicate with similar devices within 300 feet. If one device within that range is connected to an Internet-connected PC, other Cybikos can send and receive e-mail, and if the devices are equipped with optional digital music players they will be able to share music downloaded from the Internet as MP3 files. Cybiko's president said, "We want to create a social environment where teens can chat and interact." (AP/New York Times 12 Jul 2000)

[Comment by MK: This P2P technology offers considerable scope for breaches of security. On the face of it, schools and universities will have to ban such devices from examinations much as Palm Pilot and other devices that can exchange information via infrared frequencies have been banned. In addition, the prospect of having wireless access to Internet e-mail should prompt careful examination of potential confidentiality and forgery issues involving such devices.]

Category 24.9 *Peer-to-peer networking*

2000-07-27 **intellectual property IP peer-to-peer lawsuit injunction**

NewsScan, Washington Post http://www.washingtonpost.com/wp-dyn/articles/A50239-2000Jul26.html

A federal judge in San Francisco . . . issued a preliminary injunction ordering Napster.com, which provides free software allowing music-lovers to swap files of music downloaded from the Internet, to shut down its operations. Dismissing arguments that Napster users were merely exercising their First Amendment rights, U.S. District Judge Marilyn Hall Patel concluded that the illegal duplication of copyrighted material "was the whole reason for Napster's existence." The judge hinted that the Recording Industry Association of America, the plaintiffs in the suit, would ultimately prevail against Napster in a full-blown trial: "I find the plaintiffs have established not only a reasonable likelihood of success, but have shown a strong likelihood of success on the merits." (Washington Post 27 Jul 2000)

Category 24.9 *Peer-to-peer networking*

2000-07-31 **intellectual property IP copyright infringement lawsuit negotiation settlement**

NewsScan

Though Napster chief executive Hank Barry . . . [suggested there was] an opportunity to reach an out-of-court settlement in the copyright infringement suit brought against his company by the Recording Industry Association of America (RIAA), one recording company executive . . . [scoffed]: "Napster doesn't even have a business plan. There's really nothing they could offer us in settlement talks except a mailing list of people who want free music." But other record executives think some kind of settlement is inevitable, and one of them explains: "Nobody thinks the technology is going away. The point is to win the suit and keep the venture capitalists away from it." (Reuters/San Jose Mercury News 31 Jul 2000)

Category 24.9 *Peer-to-peer networking*

2000-08-21 **peer-to-peer intellectual property IP culture sociology psychology**

NewsScan

A report from scientists at the Xerox Palo Alto Research Center who studied the Gnutella system, which people can use to "share" music downloaded from the Internet, . . . [said] most users are takers but not givers. See <http://www.parc.xerox.com/istl/groups/iea/papers/gnutella>. The scientists call the lack of true sharing "a tragedy of the digital commons." (New York Times 21 Aug 2000)

Category 24.9 *Peer-to-peer networking*

2001-05-03 **criminal hacker gang group tools civil disobedience censorship peer-to-peer networking**

NIPC Daily Report

A computer hacking group known for creating tools for hijacking computer systems is turning its hand to civil disobedience and plans to release an application that could hinder government and corporate censorship around the world. The tool, to be called Peekabooty, will be based on peer-to-peer network technology. This allows data to be distributed directly between computer systems and has attained fame through the emergence of music-sharing technologies such as Napster and Gnutella. Cult of the Dead Cow is a team of computer hackers best known for producing security tools that exploit weaknesses in Microsoft software. (Infosec News, 3 May)

Category 24.9 *Peer-to-peer networking*

2001-08-01 **peer-to-peer networking exposure risk commerce distributed computing**

NewsScan

PEER-TO-PEER NETWORKING MOVES TO WALL STREET [9 Feb 2001]
Peer-to-peer networks have already proven their popularity for swapping music files, and now the same technology is invading Wall Street, with a number of startups "poised to revolutionize the investment management industry," according to an analyst at research firm TowerGroup. Two types of peer-to-peer models are emerging: one resembles Napster, in which computers share the files directly, and the other pools the resources of lots of computers to maximize the processing power. The first type enables Wall Street brokerages to deliver targeted information to clients and provides a platform for money managers to trade stock among themselves without the use of a broker. Meanwhile, distributed peer-to-peer computing networks can process complex calculations in record speed. The investment community "is a space that does not need religion when it comes to distributed computing," says Datasynapse CEO Peter Lee. "Every one of our clients was already doing it in some way, shape or form" through their own internal networks. (Investor's Business Daily 9 Feb 2001)
http://www.investors.com/editorial/tech01.asp?v=2/9

PEER-TO-PEER MOVES INTO THE MAINSTREAM [13 Jun 2001]
Many people think "Napster" when they hear about "peer-to-peer" computing, but the technology, which enables users to share files and collaborate by linking their computers over the Internet, is moving into corporate America. A variety of companies, including Intel, GlaxoSmithKine, Raytheon, Ernst & Young, and First Union, are finding that peer-to-peer technology allows their workers to do business faster, better and cheaper. Employees can hold online meetings from any location, bypassing the bottleneck of corporate servers, and freelance workers and contractors can join an online group without compromising the company's security system. "The way people get things done is by working together in small or large groups," says a Garner Group research director. "With peer-to-peer, we move from personal to interpersonal computing." Garner estimates that by 2003 nearly one in three corporations will use peer-to-peer technology to distribute files among employees. (New York Times 13 Jun 2001)
http://www.nytimes.com/2001/06/13/technology/13BURT.html

PEER-TO-PEER SCREENSAVERS [1 Aug 2001]
DALiWorld, a new peer-to-peer software program that debuted this week, is one of the first examples of how file-sharing technology is emerging as a foundation for a new generation of online games. "Traditional peer-to-peer software like Napster or Gnutella is just about moving files," says DALi CEO Todd Pappainoannou. "What we're talking about is shared, networked entertainment -- people interacting in the same virtual world from wherever they are." For the moment, DALi's major creation is software that allows you to create a virtual aquarium on your computer housing your own artificially intelligent fish, as well as others created by other users. Users can right-click on any fish swimming by to see where they've come from. Future plans call for evolving DALiWorld into a complex universe where players can create their own creatures, communicate with players from around the world, forage for food and even fiddle with the biochemistry of the virtual environment. (Wired.com 1 Aug 2001)
http://www.wired.com/news/culture/0,1284,45726,00.html

Category 24.9 *Peer-to-peer networking*

2001-08-30 **peer-to-peer distributed network parasitic computing servers**

NewsScan

'PARASITIC' COMPUTING [30 Aug 2001]
Researchers at the University of Notre Dame have demonstrated "parasitic" computing -- using other people's servers to do your own processing. Although several projects have harnessed the power of distributed computing for a common research goal, the difference here is that the Notre Dame researchers didn't ask the other server owners' permission. The methodology exploits technical protocols that ensure reliable communication by, in effect, turning the Internet into a distributed computer. Servers can then be harnessed to perform computations on behalf of an uninvited users, solving complex mathematical problems while engaging in standard communications. (InfoWorld 30 Aug 2001)
http://www.infoworld.com/articles/hn/xml/01/08/30/010830hnparasite.xml

---

Category 24.9 *Peer-to-peer networking*

2002-01-07 **privacy peer-to-peer spyware music swapping tracking Trojan game online gambling quality assurance QUALITY ASSURANCE**

NewsScan

USER WEB HABITS TRACKED BY SOME MUSIC-SWAPPING PROGRAMS
The Web surfing habits of people who used the LimeWire, Grokster and KaZaA music-sharing programs were surreptitiously tracked because those programs were linked to an online sweepstakes game called ClickTillUWin, in which players pick numbers and win cash prizes. The company that operates the sweepstakes game says it told outside distributors to get users' permission before installing the software, but in these cases that action was not taken. The three companies have posted new versions of their software without the tracking component, and LimeWire has issued an apology. (AP/USA Today 4 Jan 2002)
http://www.usatoday.com/life/cyber/tech/2002/01/04/limewire-tracking.htm

---

Category 24.9 *Peer-to-peer networking*

2002-01-24 **unauthorized use prosecution plea-bargain fine probation encryption brute-force distributed computing college**

Security Wire Digest 4 6

SYSADMIN GETS FINE, PROBATION FOR DISTRIBUTED COMPUTING
A computer technician who installed software for a volunteer distributed-computing effort was given probation and a $2,100 fine this week after an agreement was reached with state prosecutors. David McOwen, who worked at DeKalb Technical College in Georgia, was officially charged with one count of computer theft and seven counts of computer trespassing. He could have faced years in prison and hefty fines and restitution for using DeKalb computers to assist in a communal code-breaking challenge, according to published reports.

Category 24.9 *Peer-to-peer networking*

2002-03-25 **distributed computing scientific research search engine**

NewsScan

GOOGLE TACKLES DISTRIBUTED COMPUTING
Google has invited 500 users to try out a new version of its toolbar that enables them to donate their excess processing power to a Stanford University research project aimed at discovering how genetic information is converted into proteins. The Google Compute project follows the lead of other distributed computing endeavors that have sought to find everything from extraterrestrial life to cures for cancer and anthrax. "The main motivations were to try to leverage Google's expertise with large computer systems and to try to give something back to science," says Susan Wojcicki, head of Google Compute. The company likely will expand the program to include other scientific projects in an effort to boost its search business, says Wojcicki, but she doubts it will ever become a source of revenue in itself. "You never want to say never, but the goal now is to contribute something to science. We have enough fish to fry in our current businesses." (CNet News.com 22 Mar 2002)
http://news.com.com/2100-1001-867091.html

Category 24.9 *Peer-to-peer networking*

2002-04-30 **P2P peer-to-peer networks intellectual property file-swapping piracy copyright violations**

NewsScan

PEER-TO-PEER SITES MULTIPLY DESPITE LEGAL PROBLEMS
The number of peer-to-peer Web sites has increased more than five-fold in the past year, according to a study by Websense, despite heightened efforts by record companies, movie studios and software makers to shut them down. According to the survey, the number of file-swapping sites totals nearly 38,000, up 535% in the last year. Meanwhile, the recent surge in file-swapping is beginning to affect the workplace, as employers struggle to deal with the issues surrounding workers who use the speedy corporate networks to download songs and software -- a potentially illegal activity. "Companies that look the other way many have copyright violations occurring in the workplace, and lawsuits are a potential outcome of such activity," says one attorney. (Reuters/CNN.com 29 Apr 2002)
http://www.cnn.com/2002/TECH/internet/04/29/file.swapping.reut/index.html

---

Category 24.9 *Peer-to-peer networking*

2002-06-10 **P2P peer-to-peer networks file sharing vulnerabilities privacy penetration hard drive e-mail financial information compromise honeypot**

RISKS 22 12

Nathan Good of the Information Dynamics Lab at HP Laboratories posted a note in RISKS:

We have just finished a study that shows how user interface design flaws allow users on Kazaa to share their personal files without their knowledge. In a laboratory user study, only 2 out of 12 subjects were able to correctly determine that Kazaa was sharing their entire hard drive. We looked at the current Kazaa network and discovered that many users are sharing personal information such as email and data for financial programs such as Microsoft Money.

To see if other users on Kazaa were aware of this and taking advantage of users ignorance, we ran a Kazaa client for 24 hours with dummy personal files. During this time, files named "Inbox.dbx" and "Credit Cards.xls" where downloaded from our client by several unique users.

The tech report can be accessed here:
http://www.hpl.hp.com/shl/papers/kazaa/KazaaUsability.pdf
or from our lab web page at
http://www.hpl.hp.com/shl/

Category 24.9 *Peer-to-peer networking*

2003-03-29 **US military peer-to-peer P2P technology battlefield Iraq**

NewsScan

P2P GOES TO WAR
The U.S. military is using peer-to-peer technology to plan battlefield operations in Iraq and coordinate humanitarian aid to that country. Microsoft's NetMeeting software and programs from Groove Networks and Appian Corp. are part of the Defense Department's shift away from massive central computer servers toward more flexible systems that enable users to work on joint projects and share information. For instance, commanders in the Persian Gulf use collaboration software to chart their progress, drawing on one another's maps during videoconferences several times a day, says J.P. Angelone, who heads the enterprise capabilities center at the Defense Information Systems Agency. One advantage is that data are kept on individuals' computers — when a participant disconnects from the network, he can keep working on his personal version of the material. Logging in again automatically sends the updated material to other participants. "It's helpful because you reduce the physical distance to connect. If you've got a command or a tactical unit in the area of responsibility, there's no sense coming all the way back to tap into a server," says Angelone. The Defense Information Systems Agency has installed basic collaboration tools at more than 63 sites worldwide, and the trend toward P2P use likely will continue because such systems are more resistant to attack and can be faster and easier to use than traditional, server-based systems. (Los Angeles Times 29 Mar 2003)

Category 24.9 *Peer-to-peer networking*

2003-06-01 **Altnet KaZaA peer-to-peer p2p users networking authorized sharing awards**

NewsScan

ALTNET AND KAZAA PUSH LEGIT P2P NETWORK
Sharman Networks' Kazaa and Brilliant Digital Entertainment's Altnet are teaming up to launch a new phase of peer-to-peer networking, harnessing the capacity of tens of millions PCs to swap authorized copies of games, songs and movies. Giving people an incentive to trade in legitimate files could create a powerful new business model for the entertainment industry and reduce file-swapping networks' role as hubs of online piracy, says Altnet CEO Kevin Bermeister. "The minute you begin shifting unauthorized files out of people's shared folders, the peer-to-peer networks (as sources of copyright infringement) begin to disappear. Lawsuits are the stick approach. This is the carrot." Customers who sign up for the new service will agree to install high-security file-swapping software and host files that are authorized for distribution through the network. "Peer Points" will be awarded each time someone uploads a file, with the points redeemable for a variety of bonuses ranging from free access to paid content to sweepstakes entries for big-ticket items such as cars or cash. The new Altnet service and a revamped version of the regular Kazaa file-swapping software are expected to be released in test form later this week. (CNet News.com 1 Jun 2003)

Category 24.9 *Peer-to-peer networking*

2003-10-10 **P2P peer-to-peer networking Simson Garfinkel MIT technology copyright infringement**

NewsScan

P2P: SALVATION OR SCOURGE?
Internet gadgeteer and author Simson Garfinkel says peer-to-peer technology may have gained a bad name in recent years, but it could solve many of the current Internet's traffic congestion and security problems. "Peer-to-peer could overcome many of the fundamental problems that are facing the Internet today — problems of centralized control, vulnerable servers, and the difficulty that most organizations have scaling. On the other hand, peer-to-peer could also make the Internet's security problems worse, by allowing hackers to create large-scale attack networks. Peer-to-peer could be a boon for the artists and the recording industry, giving them a way of publicizing and distributing their intellectual property for far less than they do now. Yet better peer-to-peer systems could further hurt the recording companies — and not just through copyright violations... The real threat that peer-to-peer poses to the record labels is that it could make them obsolete. At the end of the day, peer-to-peer technology is about increasing the reliability and the redundancy of Internet-based systems. That's why the recording industry is afraid of it — because peer-to-peer can be used to create networks that the industry can't shut down. But peer-to-peer can also be used to create networks that earthquakes, wars and terrorists can't shut down. Ultimately, I think that we're better off trying to strengthen the Internet rather than trying to make it weaker." (MIT Technology Review/Wall Street Journal 10 Oct 2003)

Category 24.9 *Peer-to-peer networking*

2003-12-09 **hackers pirates theft Trojan horses peer-to-peer P2P Kazaa**

NIPC/DHS

December 08, New York Times — Hackers steal from pirates, to no good end.

Rogue programs known as "Trojan horses" are used by hackers to mask their identities by using unwitting people's computers as relay stations. It had been assumed that investigators could ultimately shut down a system by identifying the server computer used as the initial launching pad. But computer expert Joe Stewart has said that a program called Backdoor.Sinit uses the commandeered machines to form a peer-to-peer network like the Kazaa program used to trade music files. Each machine on the network can share resources and provide information to the others without being controlled by a central server machine. When there is no central machine, "these tactics make it impossible to shut down," he said. Rings of infected computers have been used to send spam, present online advertisements for pornographic Websites, or trick people into giving up information like credit card numbers. "Sinit appears to have been created as a money-making endeavor," Stewart said. "This Trojan is also further evidence that money, not notoriety, is now the major driving force behind the spread of malware these days." On Websites frequented by hackers, spammers and people who identify themselves as practitioners of credit card fraud, the remote-access networks, or "radmins," are offered openly.

Category 24.9 *Peer-to-peer networking*

2004-01-22 **virus threat peer-to-peer network P2P file music sharing**

NIPC/DHS; http://news.bbc.co.uk/1/hi/technology/3409187.stm

January 20, BBC News — Viruses turn to peer-to-peer nets.

Virus writers are setting up peer-to-peer networks to help their malicious creations spread. The networks are being used to control thousands of innocent PCs that some virus programs have infected. The tactic is being used because peer-to-peer networks are hard to disrupt, making viruses using this technique hard to stop spreading. One of the first viruses to set up a peer-to-peer network to help it spread was the Slapper worm that was aimed at the Linux operating system. A Windows virus called Sinit appeared in late 2003 that turned every machine infected by the malicious program into a member of a peer-to-peer network. It was expected that Sinit's creator would issue commands to infected computers via this network. In the past some creators of Trojan programs, that open up a backdoor into an infected PC, have used net chat channels as a way to issue commands. Often thousands of computers were enrolled in these remote controlled networks that have been dubbed "bot nets." Finding and shutting down the chat channels would effectively cut a virus writer off from his network of slave machines. But shutting down a distributed network would be much more difficult because no one machine is in charge. It also is much more difficult to trace where commands were being inserted and find the network's controller.

Category 24.9 *Peer-to-peer networking*

2004-02-02 **peer-to-peer P2P music file sharing intellectual property rights lawsuit Grokster Morpheus**

NewsScan

P2P CASE HEADS BACK TO COURT

A federal appeals court in California will review a lower court ruling made last spring that held distributing P2P software tools such as Grokster and Morpheus was legal and absolved the parent companies of responsibility for copyright infringement occurring on those networks. That ruling was a surprise setback for the entertainment industry, which had prevailed in previous efforts to shut down Napster and other file-swapping sites. In his decision last April, Judge Stephen Wilson wrote: "Defendants distribute and support software, the users of which can and do choose to employ it for both lawful and unlawful ends. Grokster and Streamcast are not significantly different from companies that sell home video recorders or copy machines, both of which can be and are used to infringe copyrights." In its appeal, the recording industry will argue that Wilson's analysis was flawed, citing earlier decisions in the Napster case, in which judges said that the VCR analogy (known as "substantial noninfringing use" in legal circles) does not apply if a company knows its products are being used for illegitimate purposes. "We believe (Grokster and Streamcast) are operating just like Napster and fall under the Napster ruling that the court handed down three years ago," says an attorney for the Motion Picture Association of America. "They do have one thing Napster lacked, and that is a good business model. They are making millions of dollars off of content that is not theirs." (CNet News.com 2 Feb 2004)

Category 24.9 *Peer-to-peer networking*

2004-07-07 **file-sharing peer-to-peer music sharing service colleges academia copyright infringement intellectual property rights**

NewsScan

FILE-SWAPPING AT A NEW LEVEL: I2HUB

A new file-swapping service called i2hub works only at universities with access to Internet2 -- a superfast version of the Internet created for academic use. One student who uses i2hub says: "People in legal trouble aren't aware of what they're doing or they are laughing in the face of authorities by deciding to share a ridiculous number of files. I make a minimal number of downloads from the Internet." (Wall Street Journal 7 Jul 2004) (sub req'd)

Category 24.9 *Peer-to-peer networking*

2004-10-06 **peer-to-peer P2P Morpheus Neonet search accelerator hops network intellectual property piracy theft music video files**

NewsScan; http://news.com.com/Super-powered+peer+to+peer/2100-1032_3-5397784.html

P2P GETS A BOOST

Streamcast Networks, owner of the Morpheus file-swapping software, is releasing an updated version that incorporates technology called Neonet to speed up the search process on peer-to-peer networks. Neonet, authored by a pair of former Harvard students, uses "distributed hash tables," which are essentially a way of taking a snapshot of where every file on the network is at a given moment and scattering bits of that information around the entire network. To find a specific file, a user's search request bounces from computer to computer across the P2P network, with each hop revealing a little more information about where the file can be found. Usually just three or four hops are necessary before the file is located for downloading. "The main benefit is that it allows you to search the entire network instead of just a local area," says Jed McCaleb, chief programmer for eDonkey, which also uses Neonet technology. "It's probably faster than the way Gnutella works, and it's definitely technically superior." Neonet creators Ben Wilkin and Francis Crick say the technology also holds promise for newer applications such as Net calling. "It can be used for all sorts of distributed computing tools, and that's where we're going to go with it," says Wilkin. "It really eliminates the need to have any centralized infrastructure."

Category 24.9 *Peer-to-peer networking*

2004-11-22 **P2P peer-to-peer Weed music legal use**

NewsScan; <http://www.wired.com/news/digiwood/0,1412,65774,00.html>

P2P GROWING LIKE A WEED

Peer-to-peer file-sharing networks, the scourge of the music industry, can also be used to promote music through software programs like Weed, which allows fans to download a song and play it three times before they're prompted to pay for it. Songs cost about a dollar and can be burned to an unlimited number of CDs, passed around on file-sharing networks and posted to Web pages. "We're trying to take the problem of unauthorized music sharing and turn it into an opportunity for everyone to participate in the music business," says John Beezer, president of Shared Music Licensing, which markets the Weed software and channels payments to the artists and distributors. Weed also encourages sharing by offering a commission to users who pass a song onto a friend who then buys it. Under the distribution scheme, the copyright owner gets 50%, Weed gets 15%, and the fan who passes the music along gets 20%. [Note: The article failed to mention where the other 15% goes.] Weed is also a participant in the P2P Revenue Engine project sponsored by the Distributed Computing Industry Association, which seeks to demonstrate to entertainment firms how they can use P2P services to make money. (Wired.com 22 Nov 2004)

Category 24.9 *Peer-to-peer networking*

2004-11-29 **Kazaa music Australia peer-to-peer file sharing P2P**

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/10295215.htm

RECORDING INDUSTRY SUES KAZAA

Australia's recording industry has filed a lawsuit to shut down the Kazaa file-swapping network, which it calls "an engine of copyright piracy to a degree of magnitude never before seen" because it allows users to freely exchange songs, movies and TV programs without paying royalties to the copyright owners. Sharman Networks Ltd., which owns Kazaa, will argue that it not only warns users not to commit music piracy but also that it has no control over what people actually do with the "peer-to-peer" software it provides. But the recording industry points out that Sharman provide software that helps users filter pornography and viruses -- yet don't provide software to filter out files containing copyrighted material. (San Jose Mercury News 29 Nov 2004)

Category 24.9 *Peer-to-peer networking*

2004-12-06 **peer-to-peer P2P Napster Shawn Fanning Snocap**

NewsScan; http://www.zdnet.com.au/insight/software/0

NAPSTER FOUNDER SINGING A NEW TUNE

Shawn Fanning, of Napster fame, is launching a new venture called Snocap that offers technology to identify songs as they are moved around on the Net and prompt users for payment before they listen. The idea is to transform peer-to-peer music sharing into a profit-making venture for the artists and record labels through a comprehensive content registry and "fingerprinting" technology. "We're trying to build something that facilitates a high-quality service. Respecting rights holders is important, but it's all working under the assumption that everyone is trying to make as much content available as possible. The business is built on the premise that a peer-to-peer service ought to be able to launch a successful authorized system and have the breadth of content that they had available previously, or close to that," says Fanning, who adds that his technology could also be used to police file-sharing of video games, software, movies and other P2P network content. "The fingerprint technology is music specific, but fingerprinting can apply to video, etc. The rule-sets are specific to music, but those are also very easily adaptable. So our system in a general sense is very extensible, and we believe that once the music space begins to adopt the Snocap system, there will be a demand for this kind of architecture to provide content in other forms." (ZDNet 6 Dec 2004)

Category 24.9 *Peer-to-peer networking*

2005-01-11 **file sharing BitTorrent RSS P2P peer-to-peer Vidora**

NewsScan; http://www.wired.com/news/digiwood/0

NEW SOFTWARE FINDS VIDEO IN A SNAP

A 20-year-old student at Carleton University in Ottawa, Canada, has developed a software application that combines P2P file sharing software BitTorrent with RSS (Really Simple Syndication) software used for blogging. While other software that does the same thing exists, Sajeeth Cherian notes that his Videora application is less complicated and doesn't "demand computer enthusiasts' knowledge." Once a user downloads Videora, the program automatically installs BitTorrent and downloads the RSS feeds. Users just type in a title or keyword, such as "amateur tsunami videos," and the program will automatically create a list of possibilities, any of which can be downloaded by double-clicking on the file. "We extract the BitTorrent link from the RSS feed, and if the title matches what you are looking for, we start downloading the BitTorrent file from the RSS link," says Cherian. The Videora software is available free or users can pay $23 for a version with additional features. (Wired.com 11 Jan 2005)

Category 24.9 *Peer-to-peer networking*

2005-01-21 **P2P peer-to-peer BBC Hollywood music video control business models**

NewsScan; http://news.bbc.co.uk/1/hi/technology/4191581.stm

THE FUTURE OF P2P

While Hollywood and the music industry has spent the last few years demonizing peerto- peer networks, big business is eyeing the technology's potential for "commoditization" (translation: $$$). "Old media always tries to stop new media. When they can't stop it, they try to control it. Then they figure out how to make money and they always make a lot of money," says StreamCast Networks president Michael Weiss. P2P networks can be used to share any type of file -- photos, software, licensed music and other digital content. The BBC has already embraced the technology, and will be using P2P to offer most of its programs for download this year. Even some commercial entertainment companies are working on business models that would enable them to make money off of it, such as paid-for-pass-along, in which firms receive money each time a file is shared. (BBC News 21 Jan 2005)

Category 24.9 *Peer-to-peer networking*

2005-01-25 **music piracy artists P2P peer-to-peer Supreme Court**

NewsScan; http://www.usatoday.com/tech/news/2005-01-25-riaa-wed-usat_x.htm

ARTISTS AGAINST MUSIC PIRACY

The U.S. Attorney General and the state attorneys general will have some celebrity allies in their effort to convince the U.S. Supreme Court to overturn a lower-court Internet file-sharing decision. Music stars rallying against file-sharing software's threat to copyright include the Eagles, the Dixie Chicks, Bonnie Raitt, Sheryl Crow, Stevie Nicks, Tom Jones and Beach Boys founder Brian Wilson. Don Henley of the Eagles says, "There is no more important case for the future of our business. These systems promote copyright violations on an unprecedented scale." But Fred von Lohmann, a lawyer representing the Grokster file-sharing service, says: "All the prominent movie stars of the day talked about how the VCR was the death of Hollywood. The court wasn't fooled then by the parochial interests of one industry, and it won't be now." (USA Today 25 Jan 2005)

Category 24.9 *Peer-to-peer networking*

2005-03-15 **LimeWire Gnutella client peer-to-peer P2P vulnerabilities file disclosure privilege escalation attack**

DHS IAIP Daily; http://www.securityfocus.com/archive/1/393146?ref=rss

LIMEWIRE GNUTELLA CLIENT TWO VULNERABILITIES

LimeWire client contains two vulnerabilities that allow a remote user access to many or all files on a users machine. These vulnerabilities result from inappropriate handling of "resource get" requests and "magnet" requests. Gnutella "push style" requests are not vulnerable, so a firewall that blocks access to the magnet port blocks the attack. The files accessible to a remote attacker include all of the user's private, local files, and any file on the machine if the user has administrator privileges. Upgrade to LimeWire version 4.8.0: http://www.limewire.com/english/content/home.shtml

---

Category 24.9 *Peer-to-peer networking*

2005-06-16 **peer-to-peer P2P file music movie software illegal downloading BitTorrent spyware adware infection threat**

EDUPAGE; http://news.com.com/2100-7349_3-5750601.html

BITTORRENT THE NEW SOURCE FOR SYPWARE AND ADWARE

BitTorrent downloads have become widely infected with adware and spyware, according to observers. Although functionally different from P2P services, BitTorrent has become a popular tool for locating and downloading music, video, and computer game files. Chris Boyd, operator of the Vital Security Web site, said he has uncovered many instances both of adware and of spyware being included in BitTorrent downloads. In most cases, users were prompted to download the software with instructions implying that the desired download file would not function without the extra software. Alex Eckelberry, president of Sunbelt Software, maker of antispyware software, called the BitTorrent situation "one of the most egregious spyware infestations that we have seen." He said the programs being installed on users' computers will flood them with unwanted pop-up ads and could result in overall system instability. CNET, 16 June 2005

24.A Secure processors

Category 24.A *Secure processors*

2002-06-25 **operating system security monitor kernel hardware**

NewsScan; http://apnews.excite.com/article/20020625/D7KC66M01.html

MICROSOFT CREATES VIRTUAL 'VAULT'
Microsoft, bowing to pressure to make its Windows operating software more secure, is developing a new security feature called "Palladium" that acts as a virtual "vault" for conducting electronic transactions and storing sensitive information. In order to use the new feature, consumers will have to buy new computers equipped with ultra-secure computer chips from Intel, Advanced Micro Devices, among others. Microsoft says the new technology won't be available for at least 18 months, and company officials have said they don't expect to see Palladium-enabled products hit the mainstream market for at least five years. Supporters of the technology say it will be capable of weeding out viruses and other malicious computer code and that personal information such as financial or medical records will be encrypted and inaccessible, even from other software running on the computer. Critics say Palladium could end up being just one more means for Microsoft to dominate the world's software markets, and that using the software will require changes to video and keyboard technologies requiring billions of dollars in new equipment upgrades by consumers, corporations and governments. (AP 25 Jun 2002)

Category 24.A *Secure processors*

2002-09-10 **secure microprocessor chips partitions operating systems**

NewsScan

INTEL'S 'LEGRANDE' VISION FOR SECURE CHIPS
Intel is planning to build security features into its microprocessors next year, in a move aimed at thwarting computer viruses and malicious hackers. The technology, dubbed LeGrande, initially will be included in Prescott, the code name for a new Pentium chip due out the second half of 2003. The idea of using secure chips, in addition to software, isn't new, but gained wider attention this summer when Microsoft announced its Palladium security initiative, which it hopes to develop in conjunction with Intel and chip rival Advanced Micro Devices. Unlike Palladium, however, the LeGrande technology will work with operating systems other than Microsoft Windows. The technology works by partitioning off areas of the computer's hard drive into protected areas called "vaults," and protecting the pathways between the vaults and keyboards, monitors and other peripherals. (Wall Street Journal 10 Sep 2002)

Category 24.A *Secure processors*

2002-11-04 **trusted computing hardware chips processors**

NewsScan

IT'S YOUR DATA; WHOM DO YOU TRUST WITH IT?
The major information technology companies, including Microsoft, Intel, IBM, Hewlett-Packard and 170 others, are developing an approach to data security called "trusted computing," which hardwires security into silicon chips and related software, rather than relying strictly on software to achieve security. Intel software manager Narendar Sahgal says, "This is a fundamentally new approach as opposed to taking a software-only approach." (At Intel trusted computing is called LaGrande; at Microsoft it's called Palladium.) In the trusted computing approach, each communication transaction (such as an e-mail message or an online purchase) is required to interact with secure and uniquely identified hardware through "trusted agents." Not all technologists are happy with the trend. Cambridge University security researcher Ross Anderson says, "I don't think the kind of trustworthiness they seek to deliver is at all desirable. It's not security for me. It's security for them." (AP/San Jose Mercury News 3 Nov 2002)

Category 24.A *Secure processors*

2003-10-11 **laptop crash protection IBM ThinkPad freefall crash chip**

NewsScan

IBM TOUTS LAPTOP CRASH PROTECTION
Two of IBM's new ThinkPad laptop models come with a chip designed to detect when a laptop is in freefall (if it's been knocked off a table for instance), and automatically stops the hard drive from reading or writing data — activities that IBM says make it especially vulnerable to crashing completely. The crash chips are included in the ThinkPad R50 and T41 models, which start at $1,529 and $1,649 respectively. (AP 11 Oct 2003)

Category 24.A *Secure processors*

2004-02-22 **buffer overflow hardware microprocessor fix chip manufacturers**

NewsScan

CHIPMAKERS RACE TO PLUG THE BUFFER OVERFLOW PROBLEM

The next generation of microprocessors will plug the gaps that have resulted in "buffer overflow" vulnerabilities, causing Microsoft to issue repeated "critical security alerts." The buffer section of computer memory stores a finite amount of data. To exploit the flaw, hackers cause more data to be sent to the buffer than it can hold, forcing it to overflow into the next chunk of buffer memory, where they then deposit their malicious code. This leaves the computer open to attack, as demonstrated by the devastating Slammer and Blaster worm invasions in 2003. "Buffer overflows are the largest class of software vulnerabilities that lead to security flaws," says the head of one security company. The new chips will be designed to block this avenue of attack, although security experts predict that determined hackers will find other ways to insert computer viruses — for example, by making a program jump to a subsection of its own code at the wrong time, perhaps to open a data port to a hacker. (New Scientist 22 Feb 2004)

Category 24.A *Secure processors*

2004-04-12 **portable computers cell phones encryption security firmware chip**

NewsScan

INTEL CHIPS WILL INCLUDE HARD-WIRED SECURITY

Intel's PXA27x processors — that company's next generation of chips for cell phones and handheld computers — will include hard-wired security by means of a security "engine" placed on the same piece of silicon but separated from the area where general processing takes place. Intel wireless security manager Dave Rogers says, "Carriers want to be able to identify the handset on the network. They want to make sure nobody is doing anything malicious with that handset." Some industry-watchers remain skeptical. Gartner research analyst Michael King says of Intel's wireless plans: "They're at an early place in this marketplace. Being able to dictate standards requires that you have a commanding position and I don't think they're there yet." (AP/Los Angeles Times 12 Apr 2004)

24.B Robust systems (hw / sw)

Category 24.B *Robust systems (hw / sw)*

2005-04-29 **computer keyboard equipment dirty filthy infected bacteria culture sanitize disinfect**

RISKS 23 87

COMPUTER KEYBOARDS A VECTOR FOR BACTERIAL INFECTION IN HOSPITALS

Ken Knowlton reported on new findings about a different sort of infection risk in computer equipment:

"Computers are making hospitals more dangerous, new research suggests. Computer keyboards fester with colonies of bacteria, which can easily spread from the medical personnel who use them to the patients they treat. Some hospitals now have computers in every patient room, creating even more opportunities for contamination. Researchers at Northwestern Memorial Hospital in Chicago found that the types of bacteria commonly found in hospitals -- some resistant to antibiotics -- could survive on a keyboard for 24 hours. Simply cleaning the computers with soap and water didn't make a difference. Using a strong disinfectant did kill the germs -- but it also damaged the computers. 'The difficulty with keyboards is you can't pour bleach on them,' Dr. Allison McGreer of Toronto's Mount Sinai Hospital tells The Canadian Press. 'They don't work so well when you do that.' Because it's nearly impossible to keep keyboards sterile, researchers say, the onus is on doctors and nurses to wash their hands vigorously and often." [Excerpted from *The Week*, 29 May 2005]

[MK notes that there is a tremendous market here for an enterprising company to manufacture sterilizable computer equipment, much as some manufacturers make military-grade field equipment. Sterilization could involve special materials in combination with special disinfectants especially chosen to be safe both for people and for the computer gear.]

Category 24.B *Robust systems (hw / sw)*

2005-08-09 **software quality assurance QA system design robust resistance fraud ethics third-world intellectual property rights open-source proprietary code design**

RISKS; http://www.spectrum.ieee.org/aug05/1699 24 01

ROBUST SYSTEMS DESIGN FOR THIRD-WORLD APPLICATIONS

There is an interesting article in the August 2005 issue of _IEEE Spectrum_ [by G. Pascal Zachary] on the above subject. [Hermann] Chinery-Hesse runs a very successful software business in Ghana. Some of the high points:

* Software that is lean and efficient, so it runs well on old PCs such as 386/486. These are affordable in Ghana.
* Software design for robustness under third-world conditions. For example, frequent writes to disk to minimize work lost of the power goes off, as it frequently does.
* Rather extreme measures to protect proprietary software, such as updates installed in personal visits by software company employees. This to cope with conditions in a country where any sense of ethics is practically nonexistent.
* Shunning of open source software, on the grounds that having the source makes it too easy for unscrupulous users to modify the code so as to line their own pockets.

This last item could well be criticized as security through obscurity. Surely the incentives are there for users to make a considerable effort to tamper with closed source proprietary software. One could argue that open source software would be easier to audit for unauthorized modifications. But then who audits the auditors? And how can they be sure that the code actually running in the machine is accurately represented by the source code they can see.

This suggests a larger research topic: how can we make computer systems that are guaranteed to "work right" when they are to be installed in a den of thieves? Seems like this has applicability to the problem of electronic voting systems in the U.S.

[Abstract and comments by J. H. Haynes]

---

25 Computer remote control & disruption

Category 25 *Computer remote control & disruption*

1997-01-24 **RFI**

RISKS 18 79

High altitude flights may subject modern computers to enough cosmic rays to cause single-bit errors at a rate of about once per hour on typical PCs.

Category 25 *Computer remote control & disruption*

1997-03-12 **infowar HERF EMP TEMPEST information warfare RFI**

RISKS 18 90

New work on hardening systems against high-energy electromagnetic pulses was published on <http://www.infowar.com/class_3/harden.html-ssi> by Carlo Kopp, and Australian defense analyst.

Category 25 *Computer remote control & disruption*

1997-04-16 **RFI cancer cell phone**

AP, AAP; RISKS 19 39

Medical experts at a conference in Sydney, Australia presented epidemiological evidence that electromagnetic radiation from cellular phones is associated with cancer and a number of other diseases. In separate research, a few hundred specially-bred mice highly susceptible to spontaneous lymphoma were exposed to cell-phone radiation for 18 months. Cancer rates doubled. It is not yet known if these results can be extrapolated to normal mice and to other species. The results were published in the journal _Radiation Research_ in May. Not incidentally, the results were announced with much hoopla at a press conference held by Microshield, a manufacturer of a phone cover claimed to reduce radiation from the devices. Motorola, a major manufacturer of cell phones, responded by threatening a lawsuit if the claims by Microshield were not withdrawn.

Category 25 *Computer remote control & disruption*

1997-04-28 **RFI**

RISKS 19 11

A couple of British victims of technology gone mad won a £4,000 judgment for damages because their motorized beds behaved like props from a movie comedy in response to what is assumed to be radio-frequency interference. Instead of providing soothing vibrations, the beds would go off at random, with much buzzing, pounding like jack-hammers, and abrupt changes of head and food tilt angles.

Category 25 *Computer remote control & disruption*

1997-05-02 **RFI lawsuit libel**

RISKS 19 12

In response to widespread concern about the putative cancer-causing radiation from cell phones, Motorola Australia suggested that it would sue people spreading such claims. Now _there's_ a constructive response to public fear. . . .

Category 25 *Computer remote control & disruption*

1997-07-22 **HERF guns EMP urban myths debunking**

Netly News

Cyber-historian and gadfly George Smith debunked stories of HERF (high-energy radio-frequency) weapons and EMP (electromagnetic pulse) bombs in an article published in July. He presented persuasive arguments that these stories are urban myths devoid of factual evidence.

Category 25 *Computer remote control & disruption*

1997-08-25 **RFI cancel mobile cellular phones brain tumors**

Reuters

A research project led by Dr Luc Verschaeve and sponsored by Belgacom, main owner of Belgium's largest mobile phone network, found no harm to human blood cells from exposure to emissions from their cellular phones. From this work the cellular phone company spokesperson concluded that there ought not to be any association between cell phone emissions and brain or bone cancer. [I think there ought not to be any either, but I'm not sure that looking at erythrocytes is the way to go.]

Category 25 *Computer remote control & disruption*

1997-09-17 **EMI RFI electromagnetic intererence radio-frequency**

RISKS 19 38

In a court case in September, expert witnesses demonstrated that some GM cruise control systems are susceptible to electromagnetic interference that can cause sudden acceleration. Demonstrations included goosing the cruise control by running a power drill near the car. See <http://bluecoat.eurocontrol.fr> for more details on RFI shielding requirements.

Category 25 *Computer remote control & disruption*

1997-10-01 **RFI radio frequency interference**

RISKS 19 40

In the Netherlands, a bus using an electronic linkage between the accelerator pedal and the throttle mechanism suddenly accelerated and crashed into the restaurant at Eindhoven Central Station, injuring nine people. The bus manufacturer acknowledged that radio-frequency interference from "communications equipment, the 2-way radio, the mobile telephone and/or the little box which operates traffic lights." was thought to account for the rash of such accelerations. Of the 178 busses with the electronic accelerator pedal, 22 have been taken out of service.

Category 25 *Computer remote control & disruption*

1998-01-05 **RFI EMI emissions cellular phone mobile cancer brain tumor**

Reuters

Dr Andrew Davidson, an Australian oncologist, published a letter in the Medical Journal of Australia suggesting that the 50% increase in brain tumors between 1982 and 1992 in Western Australia paralleled the increase in cellular (mobile) phone usage. This conjecture was criticized by the phone companies (no surprise).

Category 25 *Computer remote control & disruption*

1998-01-10 **information warfare RFI EMI jamming radio-frequency GPS**

RISKS 19 54

Aviaconversia, a Russian company, offered a GPS jamming device for $4,000 at the Moscow Air show in September 1997. The company claimed their jammer could interfere with civilian aircraft over a 200 km radius. The respected French publication _Intelligence_ debunked their claims (no. 76 p. 6).

Category 25 *Computer remote control & disruption*

1998-01-18 **RFI EMI radio-frequency interference avionics**

RISKS 19 55

The Australian Bureau of Air Safety recorded 30 incidents in which the use of handheld electronic equipment was thought to have been responsible for disturbances of avionics systems; however, the Bureau found no "connectivity" between the events and the devices. According to an article in the _Sydney Morning Herald_, aircraft captains are authorized (presumablyl by the BAS) to order these devices turned off. However, notes RISKS correspondent Ben Low, many devices today are in fact never powered off — "off" just means the screen is off.

Category 25 *Computer remote control & disruption*

1998-03-05 **RFI EMI radio-frequency interference**

EDUPAGE

Mercedes Benz warned that cell phones can interfere with several computer-controlled features of its cars, including the Babysmart toddler restraint seat that normally disables the passenger-side airbag when there's a child in the front seat. Cell phones can also interfere with anti-lock brakes, according to other automobile manufacturers.

Category 25 *Computer remote control & disruption*

1998-03-09 **RFI EMI radio-frequency interference medical heart monitors**

RISKS 19 62

When the Dallas station WFAA-TV switched on its new digital high-definition television broadcast, they instantly halted 12 heart monitors in the Baylor University Medical Center heart-surgery recovery room.

Category 25 *Computer remote control & disruption*

1998-04-01 **RFI EMI radio-frequency interference**

RISKS 19 64

In a long and detailed article published in the _New York Review of Books_ and available at <http://jya.com/twa800-emi.htm>, writer and Harvard Professor of Philosphy Elaine Scarry analyzed the possibility of electromagnetic interference as a precipitating cause in the crash of Flight TWA 800 in 1997. However, a subsequent commentator in RISKS 19.65 described the study as "far from a rational, scientific review of the evidence." Peter Ladkin debunked Scarry's arguments in a scathing attack published in RISKS 19.66. [So with a bow to Dr Neumann's penchant for punning, we can conclude that this scary story by Scarry has been scarified by experts.]

Category 25 *Computer remote control & disruption*

1998-04-16 **RFI EMI radio-frequency interference jamming cell phones**

RISKS 19 68

Steven Slatem, writing from Prague, reported that many gas stations in the Czech republics now bar the use of cellular phones because of reported interference with data transfers for checking credit cards. Another correspondent noted that in the UK, mobile phones must not be used near petrol stations because of the risk of sparking an explosion.

Category 25 *Computer remote control & disruption*

1998-04-23 **cell phone availability information warfare blocking jamming**

EDUPAGE, RISKS

Everyone knows about the problem caused by cell phones in public places such as concert halls, lectures, hospitals, and places of worship. This problem is particularly bad in Israel, where the military had to ban cell phone use by soldiers on active duty because the chatterboxes were inadvertently revealing sensitive military data. In my own synagogue in Montreal (writes editor Mich Kabay) our congregation was startled when a shrill tweedling interrupted the rabbi's Dvar Torah (sermon) in the middle of a service. Well, Israeli company Netline Technologies announced C-Guard, a system for suppressing unwanted cell phone calls in any given area by low-power jamming of communications with local base stations. Yasher koach (go in strength), as we say in Hebrew.

Category 25 *Computer remote control & disruption*

1998-04-28 **RFI EMI jamming quality assurance QA testing**

RISKS 19 70

The Newport, NY facility of the US Air Force Research Lab Information Directorate started a brief test of antenna emission patterns on 30 Dec 1997; the test involved 5-watt broadcasts at many Global Positioning Satellite frequencies. Unfortunately, the tests did not stop at the end of the automatic sequence, causing disruption of GPS signals used by commercial aircraft in a 300 km diameter zone defined by the FAA. The problem was not discovered until 12 January, when AF staff happened to notice complaints about GPS signal failures. [The tale of the Sorceror's Apprentice often comes to mind when I read about such cases of unplanned continuation of what were supposed to be temporary processes.]

Category 25 *Computer remote control & disruption*

1998-10-21 **RFI EMI radio-frequency interference certification**

RISKS 20 4

The casual assignment of electromagnetic frequencies is becoming perilous, wrote Peter Neumann in RISKS. "Patriot defenses and Predator unmanned aerial vehicles reportedly cannot work properly in certain foreign countries (Germany, Japan, South Korea and Bahrain are particular instances) because of frequency clashes. For example, Patriot missile system radios, radars, and data-link terminals clash with Korean cellular phones; U.S. force pages clash with Japanese aeronautical systems; crib monitors used on U.S. bases clash with German telephone service. In Bahrain, SPS-40 and SPS-49 radars are unusable because of interference from the national telecommunications services."

Category 25 *Computer remote control & disruption*

1999-01-29 **denial of service cellular phone signals control channel**

RISKS 20 18

In Crystal River, FL an innocent user unknowingly blocked all other cellular calls in his area whenever he used his new cell phone. The outages lasted 10 days while GTE tracked the problem down to his phone, which they replaced. [This case illustrates the vulnerability of the highly computer-dependent cellular-phone system to disruption — accidental in this case but possibly deliberate in an information warfare attack.]

Category 25 *Computer remote control & disruption*

1999-03-01 **electromagnetic radiation interference HERF medical**

RISKS 20 23

A new digital TV station in Melbourne, Australia was assigned the same frequency as that used for heart monitors at the nearby Epworth Hospital. Specialists worried that the signals would interfere with output from the cardiac devices.

Category 25 *Computer remote control & disruption*

1999-04-16 **RFI radio frequency interference crosstalk**

Wired

Automatic garage doors in a six-mile (10 km) radius of the port at Hobart, Australia were shut down by the USS Carl Vinson's powerful 310-320 MHz communications transmitters — which happen to override the short-range electronic communications channel allocated by the Australian regulatory bodies for such devices as garage-door openers. In addition, one poor soul was unable to move his car when the transmissions overrode his car security system, locking the vehicle down until the huge ship left.

Category 25 *Computer remote control & disruption*

1999-10-22 **criminal hacker radio frequency interference RFI**

APB News

Someone drove around Boone County, KY setting off the warning sirens intended to alert the population to dangerous weather conditions. Although the sirens are supposed to sound for only a few minutes, attempts to shut them off met with resistance from the unknown prankster, who forced the racket to continue for up to 20 minutes. Since the sirens were to be used in cases of real danger such as approaching tornados, the prank could easily turn deadly.

Category 25 *Computer remote control & disruption*

1999-11-30 **electromagnetic radiation microwave cell phone memory brain**

RISKS, New Scientist, ABC News 20 23

Reports surfaced in March that cellular phone usage could be causing memory loss in mobile-phone users. Commentators expressed doubts about the veracity of this story from the London _Daily Mail_ because of sketchy details. However, a study with rats at the University of Washington (see <http://www.washington.edu/newsroom/news/1999archive/11-99archive/k113099a.html>) suggested memory loss for those critters in after exposure to cell phones radiation. A good review of the situation by David Concar appeared in the New Scientist on 1999-04-10 <http://www.newscientist.com/nsplus/insight/phones/mobilephones.html>. For more on this subject, see the following Web sites (links listed by Lycos):
<http://www.howstuffworks.com/cell-phone.htm>
<http://www.mcw.edu/gcrc/cop/cell-phone-health-FAQ/toc.html>
<http://www.drkoop.com/news/focus/july/cell_phones.html>
<http://www.goaskalice.columbia.edu/1428.html>
<http://www.electric-words.com/radiation/rindex.html>
<http://www.ecomall.com/greenshopping/magnet.htm>
<http://www.nrpb.org.uk/Nir-is4.htm>
<http://www.health.gov.au/arl/is_phone.htm>
<http://www.tassie.net.au/emfacts/mobiles/index.html>.

Category 25 *Computer remote control & disruption*

2000-01-06 **RFI radio frequency interference jamming hijacking**

BBC http://news.bbc.co.uk/hi/english/sci/tech/newsid_592000/592972.stm

Some car radios in Britain are equipped with circuits that automatically switch to specific frequencies so that drivers can hear emergency road reports. Unfortunately, pirate radio-station operators have discovered how to misuse the Radio Data System (RDS) to their own advantage. They constantly transmit the data signal, forcing the radios to stay tuned to the pirate frequencies until the cars leave the local transmission area or the driver disables the RDS feature. Authorities were hunting the pirates.

25.1 Remote control, RATs, reprogramming, auto-updates

Category 25.1 *Remote control, RATs, reprogramming, auto-updates*

1997-08-21 **medical informatics remote sensing telemedicine**

EDUPAGE

MediVIEW and Medically Oriented Operating Network (MOON) from Sabratek Corp. allow intensive remote medical intervention such as alterations of automated flow control devices for drug administration. The initial press releases included no sign that anyone was concerned about security issues in this system. [The risks of system error and hacking now become life-threatening.]

Category 25.1 *Remote control, RATs, reprogramming, auto-updates*

1998-07-17 **Windows vulnerability probe remote administrationTrojan RAT criminal hacker**

Cult of the Dead Cow, news wires, RISKS

The Cult of the Dead Cow (cDc) announced Back Orifice, a tool for analyzing and compromising MS-Windows security (such as it be). The author, a hacker with the L0PHT group, described the software as follows: "The main legitimate purposes for BO are remote tech support aid, employee monitoring and remote administering [of a Windows network]." However, added the cDc press release, "Wink. Not that Back Orifice won't be used by overworked sysadmins, but hey, we're all adults here. Back Orifice is going to be made available to anyone who takes the time to download it [read, a lot of bored teenagers]." The product featured image and data capture from any Windows system on a compromised network, an HTTP server allowing unrestricted I/O to and from workstations, a packet sniffer, a keystroke monitor, and software for easy manipulations of the victims' Internet connections. BO's description qualified it as a Trojan that allowed infection of other applications and used stealth techniques to erase its own visibility once loaded into memory. Security experts pointed out that the key vulnerability allowing BO to contaminate a network was the initial step — running a corrupted application that would load the parasitic code into memory. Users should not download software from unknown sites or execute attachments to e-mail without assurance of their legitimacy. All the major firms offering anti-malicious-code software issued additions to their signature files to identify the Trojan code.

Apparently 15,000 copies of Back Orifice were distributed to Internet Relay Chat users by a malefactor who touted a "useful" file ("nfo.zip")that was actually a Trojan infected by Back Orifice.

Category 25.1 *Remote control, RATs, reprogramming, auto-updates*

1999-07-12 **criminal hacker remote control penetration Trojan tools**

Canberra Times (Australia)

David Hellaby of the Canberra Times (Australia) published a good review of remote-control software used by criminal hackers. Some of the dangerous applications are BackOrifice, BackOrifice 2000, DeepThroat 1, 2 and 3, EvilFTP, ExploreZip.worm, GateCrasher 1.2, GirlFriend 1.3, Hack'a'Tack, NetSphere 1.30,phAse Zero, Portal of Doom, and SubSeven (aka BackDoor-G). These programs are usually integrated into otherwise harmless and useful vector programs to create Trojans that are downloaded from the Net or shared among hapless victims. Symptoms of remote control sound like a nightmare from a paranoid schizophrenic's worst crisis: "your CD draw begins opening and closing, your web browser starts on its own, strange messages appear on your screen, and your PC seems to be haunted." The author warned his readers to be very careful about opening attachments to e-mail messages.

Category 25.1 *Remote control, RATs, reprogramming, auto-updates*

1999-07-12 **criminal hacker penetration tool Trojan version WindowsNT**

AP

The Cult of the Dead Cow released BackOrifice 2K (B02K), the newest version of its 1998 penetration tool, BackOrifice (named as a lampoon of the BackOffice product of Microsoft). BO2K, usually installed illegally on victim machines through a contaminated vector program that has been thereby transformed into a Trojan horse, allows complete remote control and monitoring of the infected PCs. BO2K was noteworthy because it attacks WindowsNT workstations and servers and thus has even more serious implications for INFOSEC. Anti-virus companies worked feverishly immediately after the release of the tool to update their virus-signature files. A criminal hacker calling himself Deth Veggie insisted that the CDC is involved in guerilla quality assurance — their penetration tools, he argued, would force Microsoft to repair the "fundamentally broken" Windows operating systems. Jason Garms, lead product manager for Windows NT security, disagreed strongly: "I certainly categorize what they're trying to do as being malicious. This program they have created has absolutely no purpose except to damage users." He added, "You can't walk down the street and pick up a rock and throw it through someone's window. You'd be arrested. But there are people on the Internet that would argue that it's good behavior because that window should have been stronger. In the real world you can't say 'You should have bulletproof glass on your windows."

Category 25.1 *Remote control, RATs, reprogramming, auto-updates*

2000-05-31 **remote control radio frequency interference RFI hacking vulnerability risk design**

RISKS 20 90

The General Motors OnStar system will allow not only geographical positioning data, local information, and outbound signaling in case of accidents: it will also allow inbound remote control of features such as door locks, headlights, the horn and so on — all presumably useful in emergencies. However, Armando Fox commented in RISKS,
>If I were a cell phone data services hacker, I'd know what my next project would be. I asked the OnStar speaker what security mechanisms were in place to prevent your car being hacked. He assured me that the mechanisms in place were "very secure". I asked whether he could describe them, but he could not because they were also "very proprietary". *Sigh*<

Category 25.1 *Remote control, RATs, reprogramming, auto-updates*

2000-08-17 **information warfare battlespace remote-control armament police law enforcement equipment robot Internet vulnerability risk**

RISKS 21 02

Anatole Shaw reported in RISKS on a dreadful new development in mobile attack weapons: "The Thailand Research Fund has unveiled a new robot, resembling a giant ladybug with a couple of extra limbs. The unit is equipped with visible-spectrum and thermal vision, and a gun. According to Prof. Pitikhet Suraksa, its shooting habits can be automated, or controlled `from anywhere through the Internet' with a password. The risks of both modes are obvious, but the latter is new to this arena. Police robots of this ilk have been around for a long time, but are generally radio-controlled. The apparent goal here is to make remote firepower available on-the-spot from around the Internet, which means insecure clients everywhere. How long will it take for one of these passwords to be leaked via a keyboard capture, or a browser bug? Slowly, we're bringing the risks of online banking to projectile weaponry."

Category 25.1 *Remote control, RATs, reprogramming, auto-updates*

2000-08-25 **remote control cellular telephones wireless mobile active content**

RISKS 21

Several hundred users of new Japanese programmable wireless phones were harassed when someone remotely ordered their devices to dial the emergency services. Kevin Connolly commented in RISKS, "The risk is that people designing new mobile phone functions do not learn from the mistakes in the MS Word macro `virus enabling' feature."

Category 25.1 *Remote control, RATs, reprogramming, auto-updates*

2000-10-20 **remote control laboratory equipment Internet hacking**

RISKS 21 10

A gateway sold by National Instruments allows instruments equipped with the standard IEEE-488 bus to be connected to the Internet — completely without any security provisions — and thus controlled remotely by total strangers. The usual dangers to the electronic equipment are exacerbated, wrote Stephen D. Holland in RISKS, because laboratory equipment is often used to control mechanical devices.

Category 25.1 *Remote control, RATs, reprogramming, auto-updates*

2000-12-22 **remote control reconfiguration firmware upgrade automatic modification control integrity error QA quality assurance design**

RISKS 21 17

In the early 1990s, certain tape drives were criticized for allowing uncontrollable automatic firmware upgrades if a "firmware-configuration tape" was recognized. The problems occurred when the tape drive "recognized" a tape as such even if it wasn't. A decade later, the same type of feature — and problem — has been noted in Dolby digital sound processors for the audio tracks of 35mm film: any time anything looking like a firmware-reconfiguration data stream is encountered, the device attempts to reconfigure itself, regardless of validity of the data stream or the wishes of the operator. A German contributor to a discussion group about movie projectors noted (translation by Marc Roessler), "The trailer of "Billy Elliott" has got some nasty bug: If the trailer is being cut right behind start mark three, the CP500 will do a software reset with data upload as the trailer runs through the machine. Either Dolby Digital crashes completely or the Cat 673 is set to factory default, which means setting the digital soundhead delay to 500 perforations, i.e. the digital sound lags 5.5 seconds behind the picture. . . ."

Category 25.1 *Remote control, RATs, reprogramming, auto-updates*

2000-12-27 **remote control upload update firmware device**

RISKS 21 18

Andrew Klossner noted in RISKS that home electronics such as DVDs are being reprogrammed using automatic firmware upgrades from media (e.g., DVDs). The correspondent writes, "When the authoritarian software forbids me to skip past a twenty-second copyright notice, it makes me nostalgic for the old 12-inch laser disks."

[MK notes: This poses additional sources of troublesome problems when the software doesn't work right. Even if it isn't broke, someone at a distance may try to fix it anyway.]

Category 25.1 *Remote control, RATs, reprogramming, auto-updates*

2001-01-12 **automated firing computer control weapons system military aircraft quality assurance**

RISKS 21 20

Daniel P. B. Smith reported in RISKS that a new airborne laser is being designed to shoot down missiles. Smith quotes an article at < http://www.cnn.com/2001/US/01/12/airborne.laser/index.html> as follows:

>No trigger man
>
>No human finger will actually pull a trigger. Onboard computers will decide when to fire the beam.
>
>Machinery will be programmed to fire because human beings may not be fast enough to determine whether a situation warrants the laser's use, said Col. Lynn Wills of U.S. Air Force Air Combat Command, who is to oversee the battle management suite. The nose-cone turret is still under construction
>
>"This all has to happen much too fast," Wills said. "We will give the computer its rules of engagement before the mission, and it will have orders to fire when the conditions call for it."
>
>The laser has about only an 18-second "kill window" in which to lock on and destroy a rising missile, said Wills.
>
>"We not only have to be fast, we have to be very careful about where we shoot," said Wills, who noted that the firing system will have a manual override. "The last thing we want to do is lase an F-22 (fighter jet)."

[MK: Readers are invited to decide if, given the current state of software quality assurance worldwide, they would be willing to entrust the safety of their family to an automobile equipped with analogous control systems.]

Category 25.1 *Remote control, RATs, reprogramming, auto-updates*

2001-01-19 **remote control automobile speed governor**

RISKS 21 22

Steve Loughran noted in RISKS that the British government has sponsored tests of computer-controlled speed governors for automobiles; the system would rely on a GPS to locate the vehicle and an on-board database of speed limits. Loughran commented, "Just think how much fun you'll be able to have by a UK motorway in five years time from jamming the GPS signals. Or how much a 'chipped' database or speed limiter will be worth. A more rigorous trial would be to place the speed limited vehicles in the hands of well known violators of the speed laws to see how much effort it takes to disable -- the UK home secretary himself, for example." In addition, the prospect of being unable to take evasive action in an emergency should cause grave concern. Furthermore, given the dismal state of software quality assurance, few RISKS readers would be happy with such a system.

Category 25.1 *Remote control, RATs, reprogramming, auto-updates*

2001-01-26 **remote control reprogramming smart cards access token**

RISKS 21 22

Jeremy Epstein wrote an interesting report for RISKS on remote reprogramming: "DirecTV has the capability to remotely reprogram the smart cards used to access their service, and also to reprogram the settop box. To make a long story short, they were able to trick hackers into accepting updates to the smart cards a few bytes at a time. Once a complete update was installed on the smart cards, they sent out a command that caused all counterfeit cards to go into an infinite loop, thus rendering them useless."

Category 25.1 *Remote control, RATs, reprogramming, auto-updates*

2001-03-30 **QA quality assurance automatic upgrade remote control ISP Internet service provider long-distance modem database loss data corruption**

RISKS 21 32

Microsoft Networks (MSN) upgraded its dialup lists automatically for users in the Research Triangle, NC area -- and wiped out several local access node numbers. Outraged users found out (too late) that their modems had switched to dialing access nodes in areas reached through long distance calls. About a month later, MSN reimbursed its customers for the long-distance calls their modems had placed due to MSN's errors.

Category 25.1 *Remote control, RATs, reprogramming, auto-updates*

2001-04-09 **home appliance hacking remote control wireless**

RISKS 21 35

Appliance hacking has been a subject of speculation for years, but more and more manufacturers are interested in controlling their domestic appliances at a distance. According to a report in RISKS, "IBM and Carrier, an air-conditioning manufacturer, said they plan to offer Web-enabled air conditioners in Europe this summer that can be controlled wirelessly. Financial terms of the collaboration were not disclosed. Owners of the newfangled air conditioners will be able to set temperatures or switch the units on or off wirelessly using a website called Myappliance.com < http://www.wired.com/news/business/0,1367,42918,00.html >. The press release quoted in RISKS indicates that the system will log information about device utilization and allow remote maintenance operations.

Category 25.1 *Remote control, RATs, reprogramming, auto-updates*

2001-04-10 **remote control thermostat TCP/IP Internet access vulnerability risk**

NewsScan

INTERNET THERMOSTAT
IBM and the Carrier Corp., which makes heating and air conditioning systems, is planning a pilot program this summer in Britain, Greece and Italy to test an Internet-based system that would allow people to use a Web site, myappliance.com, to control their home air conditioners from work or elsewhere. The system will allow troubleshooting to be done remotely and will make it easier to conserve electricity during peak demand periods. (AP/New York Times 9 Apr 2001)
http://www.nytimes.com/aponline/business/AP-Internet-Thermostat.html

---

Category 25.1 *Remote control, RATs, reprogramming, auto-updates*

2001-09-06 **remote control encryption Windows PC access authorization**

NewsScan

NEW SERVICE OFFERS REMOTE CONTROL OF YOUR PC
A new Web-based service called GoToMyPC enables users to control their desktop PCs in their homes or offices using any other Windows PC anywhere in the world that has Internet access. The service, a brainchild of Expertcity Inc., costs $10 a month. Instead of lugging a laptop along on a trip, a user could sit down at an Internet café PC and access all files, e-mail, etc. on his or her PC at home. Alternatively, if a worker found that the file he or she needed over the weekend was on the computer at work, it could be retrieved using the service. The company says the system is highly secure and requires two passwords -- one to log onto the service and another to gain access to each target PC. All of the data exchanged in each remote-control session is encrypted and Expertcity says the service will operate through many corporate firewalls. (Wall Street Journal 6 Sep 2001)
http://interactive.wsj.com/archive/retrieve.cgi?id=SB999723847321875907.djm (sub req'd)

Category 25.1 *Remote control, RATs, reprogramming, auto-updates*

2001-10-01 **remote control airliners airplanes interception impersonation**

RISKS 21 68

Steve Bellovin contributed an item to RISKS about remote control of airplanes:

"The Associated Press reported on a test of a remotely-piloted 727. The utility of such a scheme is clear, in the wake of the recent attacks; to the reporter's credit, the article spent most of its space discussing whether or not this would actually be an improvement. The major focus of the doubters was on security:

But other experts suggested privately that they would be more concerned about terrorists' ability to gain control of planes from the ground than to hijack them in the air.

I'm sure RISKS readers can think of many other concerns, including the accuracy of the GPS system the tested scheme used for navigation (the vulnerabilities of GPS were discussed recently in RISKS), and the reliability of the computer programs that would manage such remote control."

Category 25.1 *Remote control, RATs, reprogramming, auto-updates*

2001-12-20 **remote control telemedicine telesurgery hacking vulnerability interception disruption availability interruption**

NewsScan

TELESURGERY REVOLUTION, PART III [20 Dec 2001]
In a discussion of "the telesurgery revolution" in The Futurist magazine, surgeon Jacques Marescau, a professor at the European Institute of Telesurgery, offers the following description of the success of the remotely performed surgical procedure as the beginning of a "third revolution" in surgery within the last decade: "The first was the arrival of minimally invasive surgery, enabling procedures to be performed with guidance by a camera, meaning that the abdomen and thorax do not have to be opened. The second was the introduction of computer-assisted surgery, where sophisticated software algorithms enhance the safety of the surgeon's movements during a procedure, rendering them more accurate, while introducing the concept of distance between the surgeon and the patient. It was thus a natural extrapolation to imagine that this distance--currently several meters in the operating room--could potentially be up to several thousand kilometers." A high-speed fiber optic connection between New York and France makes it possible to achieve an average time delay of only 150 milliseconds. "I felt as comfortable operating on my patient as if I had been in the room," says Marescaux. (The Futurist Jan/Feb 2002)
http://www.futurist.com

Category 25.1 *Remote control, RATs, reprogramming, auto-updates*

2002-01-08 **remote control FPGA field-programmable logic array firmware**

RISKS 21 87

J. P. Gilliver noted an alarming development in remote reprogramming -- an easy way to modify firmware: ". . . For example, IRL (Internet Reconfigurable Logic) means that a new design can be sent to an FPGA in any system based on its IP address." (From Robert Green, Strategic Solutions Marketing with Xilinx Ltd., in "Electronic Product Design" December 2001. Xilinx is a big manufacturer of FPGAs.) For those unfamiliar with the term, FPGA stands for field-programmable logic array: many modern designs are built using these devices, which replace tens or hundreds of thousands of gates of hard-wired logic.

The RISKs involved are left as an exercise to the readers."

Category 25.1 *Remote control, RATs, reprogramming, auto-updates*

2002-01-16 **theft deterrent remote control explosion destruction tampering interception data diddling man-in-the-middle attacks criminal hackers vulnerability potential**

NewsScan

EXPLODING CHIPS COULD FOIL THIEVES
Researchers at the University of California in San Diego have developed a way to blow up silicon chips using an electric signal -- an innovation that could be used to fry electronic circuitry in devices after they're stolen or fall into the wrong hands. The American spy plane that was impounded in China last year is an example where such technology would have proven handy in destroying its secret electronics systems. Similarly, if a cell phone were stolen, the owner could alert the wireless carrier, which would send a signal to trigger a small explosion in the phone's chip, rendering it useless. The techniques uses a small amount of the oxidizing chemical gadolinium nitrate applied to a porous silicon wafer. (New Scientist 16 Jan 2002)
http://www.newscientist.com/news/news.jsp?id=ns99991795

Category 25.1 *Remote control, RATs, reprogramming, auto-updates*

2002-01-25 **remote control firmware reprogramming update configuration change SMS**

RISKS 21 89

In Switzerland, the mobile phone company Swisscom admitted that it reconfigured its customers' phones using a program embedded in a SMS (short message service) transmission. The message deleted roaming information. S. Llabres reported in RISKS, ". . . [I]nsiders believe that the modification of the roaming information was to direct traffic to networks owned by Vodafone -- which acquired a 25% share of Swisscom [in April] last year." Llabres commented astutely, "It would be interesting:
* If there is any security mechanism protecting anyone from sending such "special" messages.
* Which setting[s] on the mobile phone can be changed (or probably retrieved from the phone) without knowledge to the customer.
* If the network provider must implement such features, I do not understand why this must happen unperceived by the customer. Why not send a message telling people what will happen?"

Category 25.1 *Remote control, RATs, reprogramming, auto-updates*

2002-02-20 **auto-update firewall Trojan trust**

RISKS 21 92

Scott Schram published a paper at < http://schram.net/articles/updaterisk.html > that pointed out the security risks of all auto-update programs (e.g., self-updating antivirus products, MS Internet Explorer, MS-Windows Update, and so on). Once the firewall has been set to trust their activity, there is absolutely no further control possible over what these programs do. If any of them should ever be compromised, the results on trusting systems would be potentially catastrophic.

Category 25.1 *Remote control, RATs, reprogramming, auto-updates*

2002-03-14 **automated aircraft collision detection avoidance robots**

RISKS 21 96

In March 2002, tests on unmanned remote-control aircraft studied the effectiveness of automated collision-avoidance systems. Look for exciting developments in security-engineering failures in years to come.

Category 25.1 *Remote control, RATs, reprogramming, auto-updates*

2002-03-18 **automated automobile highway monitoring detection surveillance**

RISKS 22

In Boston, city engineers described plans for a new highway-traffic monitoring system called the Integrated Project Control System (IPCS). Using magnetic loops embedded in the pavement, the system would sense traffic speed and instantly report sudden slowdowns or stoppages as well as simply keeping track of total volume and speed for statistical purposes.

Category 25.1 *Remote control, RATs, reprogramming, auto-updates*

2002-04-22 **critical infrastructure security wireless interception hijacking vulnerabilities**

RISKS 22 04

John McPherson noted in RISKS:

"... The Matamata wireless link replaced an expensive frame relay service as well as providing a 1Mbs Internet service to several outlying sites including a library and remote management of water supplies. As the water facilities are computer controlled, they are able to manipulate them remotely rather than sending someone 20 miles down the road just to turn a valve." ... From *The New Zealand Herald* (Talking about 802.11b)
http://www.nzherald.co.nz/storydisplay.cfm?storyID=1392336&thesection=technology&thesubsection=general

He added: "Now I don't know if this technology is mature enough to be trusted for this type of thing - I guess I'll wait for the comments to come flooding in. I sincerely hope they've thought through the encryption and security issues here."

Category 25.1 *Remote control, RATs, reprogramming, auto-updates*

2002-04-26 **anti-collision technology automobiles crash lidar smart roadways**

NewsScan

'SMART CAR' FEATURES BEGINNING TO SHOW UP IN LUXURY CARS

The widespread use of "adaptive cruise technologies" to prevent automobile collisions is still well in the future, but some luxury cars such as Infinti, Lexus, and Mercedes-Benz are now being offered with expensive options designed to allow moving vehicles to communicate with each and to detect sensors embedded in the pavement that detect the vehicle ahead either by radar or lidar (the laser-based equivalent of radar). Steven Schladover of the California Partners for Advanced Transit and Highways says: "It feels like you're in a train -- a train of cars. You don't see any separation between the vehicles, and, after a minute of feeling strange, most people relax and say, 'Oh, this is pretty nice!'" A lidar package for the Infiniti Q45 will require purchase of a $10,000 optional equipment package. (San Jose Mercury News 26 Apr 2002)
http://www.siliconvalley.com/mld/siliconvalley/3143626.htm

Category 25.1 *Remote control, RATs, reprogramming, auto-updates*

2002-06-21 **credit card keystroke capture Trojan Horse investigation law enforcement evidence forensics university**

Edupage; http://chronicle.com/free/2002/06/2002062001t.htm

ASU PCS SEIZED IN INVESTIGATION
State police have confiscated desktop computers and hard drives at Arizona State University on the suspicion that unknown third parties installed keystroke-capture software on the computers with the goal of recording credit-card numbers and other personal data. Most of the affected systems were in open-use kiosks, according to campus representatives. The U.S. Secret Service is leading the investigation, with help from Arizona State Police. Computer systems at other colleges may also be involved. Speculation targets the Russian mafia as the perpetrators. Chronicle of Higher Education, 20 June 2002

Category 25.1 *Remote control, RATs, reprogramming, auto-updates*

2003-03-10 **Windows root kit remote administration back door penetration stealth exploit**

NIPC/DHS

March 05, SecurityFocus — Windows root kits a stealthy threat.

A Windows root kit called "ierk8243.sys" was discovered on the network of Ontario University last January. It has since been dubbed "Slanret", "IERK," and "Backdoor-ALI." A root kit is an assembly of programs that subverts the Windows operating system at the lowest levels, and, once in place, cannot be detected by conventional means. Also known as "kernel mode Trojans," root kits are far more sophisticated than the usual batch of Windows backdoor programs. Greg Hoglund, a California computer security consultant, believes intruders have been using Windows root kits covertly for years. He says the paucity of kits captured in the wild is a reflection of their effectiveness — not slow adoption by hackers. Once Slanret is installed on a hacked machine, anti-virus software won't pick it up in a normal disk scan. That said, the program is not an exploit — intruders have to gain access to the computer through some other means before planting the program. Despite their increasingly sophisticated design, the current crop of Windows root kits are generally not completely undetectable, and Slanret is no exception. Because it relies on a device driver, booting in "safe mode" will disable its cloaking mechanism, rendering its files visible. And in what appears to be an oversight by the kit's author, the device driver "ierk8243.sys" is visible on the list of installed drivers under Windows 2000 and XP, according to anti-virus company Symantec Security Response. Hoglund says future Windows root kits won't suffer from Slanret's limitations. And while he says the risk can be reduced with smart security policies — accept only digitally-signed device drivers, for one — ultimately, he worries the technique may find its way into self-propagating malicious code.

Category 25.1 *Remote control, RATs, reprogramming, auto-updates*

2004-01-14 **Microsoft security bulletin patch flaw vulnerability fix buffer overflow overrun remote control**

DHS/IAIP Update

MICROSOFT SECURITY BULLETIN MS04-003: BUFFER OVERRUN IN MDAC FUNCTION COULD ALLOW CODE EXECUTION (832483).

Microsoft Data Access Components (MDAC) is a collection of components that provides the underlying functionality for a number of database operations. When a client system on a network tries to see a list of computers that are running SQL Server and that reside on the network, it sends a broadcast request to all the devices that are on the network. Because of a vulnerability in a specific MDAC component, an attacker could respond to this request with a specially-crafted packet that could cause a buffer overflow. An attacker who successfully exploited this vulnerability could gain the same level of privileges over the system as the program that initiated the broadcast request. For an attack to be successful an attacker would have to simulate a SQL server that is on the same IP subnet as the target system. A target system must initiate such a broadcast request to be vulnerable to an attack. An attacker would have no way of launching this first step but would have to wait for anyone to enumerate computers that are running SQL Server on the same subnet. Also, a system is not vulnerable by having these SQL management tools installed. Code executed on the client system would only run under the privileges of the client program that made the broadcast request. Microsoft has assigned a severity rating of "Important" to this issue.

Category 25.1 *Remote control, RATs, reprogramming, auto-updates*

2004-01-14 **Microsoft security bulletin patch flaw vulnerability fix remote control buffer overflow**

DHS/IAIP Update

MICROSOFT SECURITY BULLETIN MS04-001: VULNERABILITY IN MICROSOFT INTERNET SECURITY AND ACCELERATION SERVER 2000 H.323 FILTER CAN ALLOW REMOTE CODE EXECUTION.

A security vulnerability exists in the H.323 filter for Microsoft Internet Security and Acceleration Server 2000 that could allow an attacker to overflow a buffer in the Microsoft Firewall Service in Microsoft Internet Security and Acceleration Server 2000. An attacker who successfully exploited this vulnerability could try to run code of their choice in the security context of the Microsoft Firewall Service. This would give the attacker complete control over the system. The H.323 filter is enabled by default on servers running ISA Server 2000 computers that are installed in integrated or firewall mode. ISA Servers running in cache mode are not vulnerable because the Microsoft Firewall Service is disabled by default. Users can prevent the risk of attack by disabling the H.323 filter. Microsoft has assigned a severity rating of "Critical" to this issue.

Category 25.1 *Remote control, RATs, reprogramming, auto-updates*

2004-07-26 **WiFi wireless sensor machinery construction manufacturing application**

NewsScan

WIRELESS CYBERCONTROL

The use of wireless networks of sensors and machinery has been expanding rapidly in such applications as the management of lighting systems and the detection of construction defects. Recent examples include a wireless communications system to tell precisely when to irrigate and
harvest grapes to produce premium wine and a system to monitor stresses on aging bridges to help states decide maintenance priorities. Hans Mulder, associate director for research at Intel, says that systems such as these "will be pervasive in 20 years." Tom Reidel of Millenial Net comments: "The
range of potential market applications is a function of how many beers you've had," but adds: "There's a whole ecosystem of hardware, software and service guys springing up." (New York Times 26 Jul 2004)

Category 25.1 *Remote control, RATs, reprogramming, auto-updates*

2005-01-20 **cellphone phone future remote-control multi-function devices**

NewsScan; http://www.latimes.com/technology/ats-ap_technology12jan20

BE MASTER OF THE UNIVERSE (FROM YOUR CELLPHONE)

Toshiba has developed software that will make it possible for people to edit documents, send e-mail, and reboot their PCs remotely from their cellphones, allowing them to work anywhere. Toshiba will begin offering the service in Japan by the end of March through CDMA1X mobile phones offered by KDDI Corp. Toshiba is initially targeting the corporate work force, but says individuals can use it to record TV shows, work security cameras and control air conditioners tied to home networks. (AP/Los Angeles Times 20 Jan 2005)

25.2 Jamming

Category 25.2 Jamming

2001-11-21 **RFI radio frequency interference jamming cellular mobile phones hospital medical electronics**

RISKS 21 78

Russell Stewart caught what appeared to be an interesting paradox about attempts to stop people from using mobile phones in hospitals: seems a Hong Kong company is offering radio-frequency jamming devices. As Mr Steward pointed out, "Hospitals? Now, I admit I know very little about jamming technology, but I know that, at the very least, it requires transmitting radio energy on the same frequency as the signal you are trying to jam. Presumably, it involves transmitting at a considerably higher power than that of the target signal. Now, as I understand it, hospitals' no-cellphone policy is based on the fear that the phones' radio transmissions might interfere with hospital equipment. Are we to understand, then, that they intend to combat the problem by installing a device that, by definition, must transmit on the same frequencies at the same or considerably greater power?"

However, Markus Kuhn immediately responded to the list explaining that mobile-phone jamming does _not_ send a signal that competes with the phone-to-base-station signal; instead, one james cellular phones by competing with the base-station-to-phone signal, which is orders of magnitude weaker. In addition, wrote Mr Kuhn, "The no-cellphone policies in hospitals are today mostly based on the fear that clueless phone users might operate phones in the immediate vicinity (with a couple of centimeters) of critical equipment. As soon as the mobile phone is a few meters away, field strength will drop well bejond the 3 V/m levels against which medical equipment has to be EMC immunity tested by the manufacturers (EN 50082, IEC 601-1-2)."

Category 25.2 Jamming

2003-09-11 **jamming phone cameras iceberg systems safe have technology picture cell picture imaging capabilities**

NewsScan

TECHNOLOGY JAMS CELL PHONE CAMERAS
A new product from Iceberg Systems, dubbed Safe Haven, is designed to block a camera cell phone's ability to snap pictures. The imaging system is then reactivated when the cell phone leaves the Safe Haven-protected area. The product uses hardware transmitters with a small piece of control software loaded into a camera phone handset to disable the imaging capability, and Iceberg Systems managing director Patrick Snow says his company is in talks with handset manufacturers interested in testing the technology. Safe Haven could prove popular with businesses that operate secure sites — Samsung and LG Electronics have already barred employees from using camera phones in research and manufacturing facilities for fear sensitive data could be stolen. Snow says the system could also be tweaked to eliminate other annoying cell phone intrusions, such as loud ringtones in a theater or text-messaging in school. Meanwhile, analysts predict there will be some 1 billion camera phones in use within five years. (CNet News.com 11 Sep 2003)

Category 25.2 Jamming

2004-05-17 **Wi-Fi wireless PDA jamming PDA denial of service DoS**

DHS IAIP Daily; http://www.newscientist.com/news/news.jsp?id=ns99995000

May 17, New Scientist — Wi-Fi networks can be jammed from PDAs.

Wi-Fi networks can be jammed using nothing more sophisticated than a PDA and an off-the-shelf wireless networking card, the Australian Computer Emergency Response Team (AusCERT) has warned. Wi-Fi networks are becoming common in workplaces and elsewhere and it was known that they are vulnerable to jamming. It was thought that this would require the use of large, powerful and expensive equipment, but students at the Queensland University of Technology have now proved this wrong. AusCERT says attacks will be hard to foil because the problem exploited is inherent in the Wi-Fi protocol. However, such an attack can only deny access to the network--it will not enable hackers to access user's data or computers. The problem stems from how the Wi-Fi networks allocate transmission channels. As in many other networks, Wi-Fi nodes check to see if other devices are transmitting on the same frequency band before they begin sending data, to avoid "collisions" that occur when two or more devices talk simultaneously. Like a conversation among a group of people, this works well as long as all devices are well-behaved. But it breaks down if one person or one device insists on talking loudly and continually. In essence, the Wi-Fi jamming is a denial of service attack.

Category 25.2 *Jamming*

2004-05-18 **attack spy camera wireless vulnerability PDA Quennsland University**

NewsScan

ATTACK JAMS SPY CAMERAS

An electronic invisibility cloak generated by nothing more than an off-the-shelf PDA would allow intruders to elude wireless security cameras using vulnerabilities in the most common wireless technologies. There is no defense against such a Mission Impossible-style attack, which can be used to knock out wireless networks and possibly transfer unwitting users to a spoofed wireless network. Accidentally discovered last year by PhD students at the Queensland University of Technology's Information Security Research Centre, the exploit presents obvious applications for terrorism and espionage. The vulnerability is "trivial" to exploit and only took 30 minutes to master, says Associate Professor Mark Looi. "It just uses off-the-shelf hardware and you don't need to write specific software, you just need to know the correct commands to use with the software that's supplied. On a difficulty rating of 1 to 10, it's probably a 2." (The Age 18 May 2004) Rec'd from John Lamp, Deakin Univ.

Category 25.2 *Jamming*

2004-10-11 **France jamming cell phones movie theaters regulations law Europe denial-of-service DoS suppression**

NewsScan; http://apnews.excite.com/article/20041012/D85LIBC80.html

FRANCE APPROVES CELL PHONE-JAMMING IN THEATERS

Tired of chatty theater-goers disturbing your entertainment enjoyment? France Industry Minister Patrick Devedijian has approved a decision by the country's Telecommunications Regulation Authority to allow cinemas, concert halls and theaters to install cell phone jammers that would prevent patrons from making or receiving calls during performances. Devedijian stipulated that emergency calls and calls made outside theaters and other performance spaces must not be affected, however. The move comes in response to "a long-standing request" from cinemas, says Jean Labbe, president of the National Federation of French Cinemas, noting that movie theaters had invested heavily to improve comfort and that "the authorization of jammers is the cherry on the cake." (

Category 25.2 *Jamming*

2004-10-19 **TV remote control jamming denial-of-service DoS brute-force cryptanalysis**

NewsScan; http://www.wired.com/news/culture/0,1284,65392,00.html

TV-B-GONE ZAPS INTRUSIVE BROADCASTS

Inventor Mitch Altman has the answer for people in airports, doctors' offices, restaurants and bars that feature blaring television sets as part of the ambiance. The TV-B-Gone is a universal remote disguised as a tiny keychain fob that works on most televisions and comes in two models geared toward European TV sets or Asian- American ones. When activated by pressing a button, the device runs through about 200 different codes that turn off various TV models, starting with the most popular brands and then moving to the more obscure. One TV-B-Gone enthusiast notes, "You've heard about the battle for eyeballs. They're your eyeballs. You should not have your consciousness constantly invaded. Television people are getting better and better at finding ways of roping us into TV where we can't get away." Altman says friends who've heard about the device have approached him about other uses, such as one that could jam cell phones or shut down vehicle subwoofers and car alarms.

Category 25.2 *Jamming*

2004-11-04 **Ireland cell phone jamming theaters regulation law denial-of-service DoS**

NewsScan; http://theage.com.au/articles/2004/11/04/1099362260997.html

IRELAND TO SILENCE MOBILES IN CINEMAS, THEATERS

Ireland's cinemas and theatres have been given the go-ahead by the country's communications watchdog to permit the use of mobile phone interceptors. Interceptors will allow the creation of "quiet zones" where the mobile phones will not ring but where calls can still be made to emergency services or to lists of approved numbers, the Communications Regulator said on Wednesday. (The Age 4 Nov 2004)

Category 25.2 Jamming

2005-11-04 **radio frequency interference RFI controls garage-door openers military**

RISKS; http://tinyurl.com/7mva3 24 09

RADIO SIGNAL KEEPS OTTAWA GATES AND GARAGE DOORS CLOSED

Apparently garage doors and embassy gates are refusing to work because something in Ottawa is broadcasting on their radio controlled opener devices' frequencies and swamping them. No one seems to know who/what is doing it and some fingers point to the military use of that same frequency…. This is, of course, a common problem as we run out of available radio bandwidth and try to cram more and more users into limited space. There is a possibility that the U.S. Embassy or the U.S. Military stationed at the Embassy is responsible. Time will eventually tell.

[Abstract by R. S. Heuman]

[MK adds:] The CBC article has additional details of interest (all quotations):

* It affects a 25-mile radius.

* Two companies that have plotted the reported problems on maps say they appear to cluster in the Byward Market area just east of Parliament Hill, and a corridor leading southeast from there.

* The Door Doctor has received more than 100 calls from irate customers who can't operate their doors using the usual remotes.

* The signal is transmitted on the 390-megahertz band, which is used by virtually all garage door openers on the continent. That's the same frequency used by the U.S. Military's new state-of-the-art Land Mobile Radio System.

* …[O]perators have already been warned of this phenomenon by service updates from U.S. manufacturers, who started seeing the same problem around military bases last summer. The strong radio signals on the 390-megahertz band simply overpower the garage door openers.

25.3 RFI, HERF, EMP/T

Category 25.3 *RFI, HERF, EMP/T*

2000-05-29 **radio frequency interference RFI avionics cellular phones mobile**

RISKS; New Scientist 20 89
http://www.newscientist.com/nsplus/insight/phones/dangersignals.html

According to a study in Britain's New Scientist magazine, cellular (mobile) phones do in fact exceed radio-frequency interference tolerances for avionics in older airplanes.

Category 25.3 *RFI, HERF, EMP/T*

2000-06-06 **RFI radio frequency interference control systems electrical**

RISKS, Canadian Broadcasting Corporation 20 91
http://cbc.ca/consumers/market/recalls/reclfull/2000/06jun2000b.html

According to an article on the CBC Web site, Ford Explorers are subject to radio-frequency interference with their central computer, resulting in non-responsive on/off switches. Alex Wiebe wrote in RISKS, "the result is anything ON will stay ON, anything OFF will stay OFF." Wiebe noted that the headline for this article referred to air-bags whereas the body did not; if air bags were affected by electronic noise, the danger to drivers and passengers could be severe.

Category 25.3 *RFI, HERF, EMP/T*

2000-09-06 **RFI radio frequency interference avionics crash theory**

RISKS, NY Review of Books 21 04
http://www.nybooks.com/nyrev/WWWfeatdisplay.cgi?20000921092F

A report in the New York Review of Books by Elaine Scarry entitled "Swissair 111, TWA 800, and Electromagnetic Interference" suggested that two flights that took off from JFK airport at the same time on Wednesday nights and then crashed may have been affected by strong radio-frequency interference from military installations nearby. However, Professors Peter Ladkin and Willi Schepper of the University of Bielefeld, Germany, published a strong refutation of Scarry's speculations in a paper published on their Web site at < http://www.rvs.uni-bielefeld.de/publications/Papers/Scarry-refutation.pdf >. These scientists pointed out that the radio-frequency flux would have to be at least 6.8M times greater than anything available in order to trigger explosions inside the plane. Instead, their analysis leads them to focus on the possibility of defective wiring in both planes.

Category 25.3 *RFI, HERF, EMP/T*

2000-12-26 **RFI radio frequency interference avionics navigation**

RISKS, The Times of London http://www.thetimes.co.uk/article/0,,2-58265,00.html 21 17

David Kennedy summarized a case of radio-frequency interference for RISKS (quoting his summary verbatim):

ROYAL AIR FORCE pilots will stop using a bad-weather navigation system from January 1 because new commercial radio frequencies have made it unreliable, the Ministry of Defence said yesterday. Pilots of military planes and helicopters fitted with the Instrument Landing System (ILS) will not be allowed to use it to land in poor weather in the new year. Instead they will have to ask air traffic controllers to talk down their flights.
* Commercial FM growth cited as cause.

* Commercial ILS on different frequencies has not been affected.

* Affected aircraft are Nimrod reconnaissance and search and rescue helicopters. RAF transport a/c have already been upgraded and tactical aircraft do not use ILS.

"There is no operational impact whatsoever," a ministry of Defense spokeswoman said. "It is a worldwide problem which affects all countries." "New landing assistance systems use more reliable technology, such as global positioning satellites, which are not affected by radio frequencies. ILS can also be disrupted by signals from mobile telephones."

Category 25.3 *RFI, HERF, EMP/T*

2001-01-09 **avionics failure RFI radio frequency interference cellular phone**

RISKS 21 20

A cellular (mobile) phone that had been left on in baggage stowed on a Slovenian Adria Airways plane disrupted the avionics and forced an emergency landing.

Category 25.3 *RFI, HERF, EMP/T*

2002-07-24 **spectrum wireless shortage dearth competition overlap**

NewsScan

FCC STEPS UP SEARCH FOR MORE SPECTRUM
A shortage of airwaves is hampering the U.S. wireless industry, and analysts say a major spectrum expansion is critical if the industry is to avert an erosion in the quality of cell phone service or a financial meltdown in the next two years. Although wireless companies are spending nearly $10 billion this year to expand calling capacity and provide new high-speed data services, revenue per minute has dropped to 14 cents, down from 52 cents in 1992. "There's a basic rule of economics: If you sell something for $1 that costs you $1.05, you can't make money," says one telecom consultant. In an effort to alleviate the problem, the FCC announced last week it would auction 740 wireless licenses beginning next month, but those licenses are for spectrum now in use by television broadcasters, and some wireless operators have opposed the auction because carriers would be forced to spend hundreds of millions of dollars on spectrum that's not immediately available. "The wireless revolution is becoming a victim of its own success," says FCC wireless bureau chief Thomas Sugrue. "The simple truth is that as our society grows increasingly dependent on wireless technology and services, spectrum demand is stressing that supply, and that has made spectrum management difficult for government." (Los Angeles Times 5 Jul 2002)
http://www.latimes.com/technology/la-fi-wireless5jul05

PLAN SHIFTS SPECTRUM FROM GOVERNMENT TO WIRELESS USE
The National Telecommunications and Information Administration has unveiled a plan to shift 90 megahertz of spectrum from government to commercial use in an effort to provide the additional airwaves the wireless industry says it needs for so-called third-generation (3G) wireless services. At least half the spectrum will come from the military, with the remainder coming from airwaves controlled by the Federal Communications Commission. Congress is expected to introduce legislation that would transfer the revenue from the auctioned spectrum to the military to cover the costs of buying new equipment and transitioning to different airwaves. Wireless companies could bid on the new spectrum as early as 2004, but wouldn't be able to use it until 2008, which is the earliest the military was willing to make the move. Analysts cautioned that the proposal is not entirely good news for the wireless industry, which has long complained it needs more spectrum to deliver advanced services. The 90 megahertz is less than half the 200 megahertz sought by the industry, and the two chunks are not contiguous, which will make it more expensive to use them. There's also the risk that the military might renege on the agreement down the road, arguing it needs the spectrum for national security requirements. (Wall Street Journal 24 Jul 2002)

Category 25.3 *RFI, HERF, EMP/T*

2002-11-08 **wireless keyboard data leakage confidentiality eavedropping**

NewsScan

TYPE ONCE, READ MANY PLACES
Two men in Norway recently made headlines when they discovered that the text one of them was typing on his Hewlett-Packard cordless keyboard was also appearing on a neighbor's computer in another building at least 150 meters away. They have since had their equipment replaced, but the problem persists and HP Norway product manager Tore A. Särelind says the firm is taking it "deadly seriously," and has mobilized forces to correct the situation. "Among other things we will check the suitability of the frequency we use. It is a so-called walkie-talkie frequency with a radius that can be difficult to limit," says Särelind. "We would also like to do an 'on-site' test in the area where Helle and Evjeberg live to see if there are special circumstances there which might influence the reach of the keyboards." Over 65,000 of the keyboards have been sold in Europe. (Aftenposten 6 Nov 2002)
http://www.aftenposten.no/english/local/article.jhtml

Category 25.3 *RFI, HERF, EMP/T*

2003-02-04 **Wi-Fi wireless radio-frequency interference RFI radio frequency interference jamming radar military national security spectrum**

NewsScan

PENTAGON AND INDUSTRY IN TUG-OF-WAR OVER RADIO SPECTRUM
The U.S. Defense Department, citing national security reasons, is seeking new limits on wireless Internet technology such as the Wi-Fi systems increasingly found in airports, homes and offices, and places like Starbucks. The Pentagon says that the low-power radio emissions may jam as many as ten types of military radar systems. Industry powerhouses such as Intel and Microsoft insist, however, that military and civilian uses of wireless communications technology can coexist peacefully, and that in Europe there are smart wireless Internet devices that can sense the nearby use of military radar and automatically yield the right of way. Wireless industry executive Rich Redelfs of Atheros says: "The idea is to get the world on a single page, and Europe is way ahead of the U.S. in understanding these interference issues." However, Defense Department officials consider the technology unproven and want the Federal Communications Commission to delay releasing for civilian use additional radio frequencies in the 5-gigahertz range. (New York Times 17 Dec 2002)

PACT PREVENTS WIRELESS INTERFERENCE WITH MILITARY CHANNELS
The U.S. Defense Department and a group of high-tech manufacturers have struck a deal aimed at preventing future interference with military radar from next-generation wireless devices. Under the compromise, wireless device makers will build in technology to detect and actively avoid military radars that operate on similar frequencies. In return, Defense officials will support proposals to nearly double the amount of wireless spectrum available, particularly that used for "Wi-Fi" computing. Ed Thomas, chief engineer for the Federal Communications Commission, called the pact "good for the Department of Defense and good for the industry." (Wired.com 3 Feb 2003)
http://www.wired.com/news/wireless/0,1382,57528,00.html

Category 25.3 *RFI, HERF, EMP/T*

2003-08-27 **RSA RFID block information collection tags**

NewsScan

RSA SECURITY's PLANS FOR RFID BLOCKING TECHNOLOGY
RSA Security has developed a blocking technique that disrupts the transmission of information contained in RFID tags and prohibits data collection. The technique is still in the drawing board stage, but the company plans to make prototype chips and see if any manufacturing groups are interested in making the processors, according to chief RSA researcher Ari Juels. Juels says the RSA technology would enable the RFID tags to be used, but that the blocking feature would allay the privacy concerns that have derailed recent deployment plans. "This is not meant to be a hostile tool. It balances consumer privacy and retail use in a profitable way. Tags are too useful to completely disable them." (CNet News.com 27 Aug 2003)

Category 25.3 *RFI, HERF, EMP/T*

2004-04-20 **pacemakers electrical interference**

NYT
http://www.nytimes.com/2004/04/20/health/policy/20PACE.html?th=&pagewanted=print&position=

RFI CAUSES TROUBLE FOR PACEMAKERS

Users of cardiac pacemakers are finding an increasing number of devices at work and at home that interfere with their artificial heart-rate controls. The culprit is generally electrical; examples include electrical nerve stimulators (PENS) and "alternative medicine" devices such as the Zapper, which sends electrical shocks through the victim, er, patient for no obvious reason.

Category 25.3 *RFI, HERF, EMP/T*

2006-04-20 **electromagnetic pulse EMP information warfare RFID radio-frequency identification tag sabotage destruction inactivation criminal hackers**

RISKS; Chaos Computer Club https://events.ccc.de/congress/2005/wiki/RFID-Zapper(EN) 24 26

RFID ZAPPERS

The Chaos Computer Club of Germany had a discussion of RFID Zappers at its 22nd Chaos Communication Congress in December 2005 in Berlin. Al Mac provided a summary:

…[S]ome hobbyist has come up with what it takes for a paranoid person to obliterate any RFID tags that might be on consumer merchandise, or where not expected or wanted….

I imagine that there will be a consumer market for this.

People who want one but do not have the personal what it takes to build stuff in their garage with assurance the contraption works right, and that they not injure themselves before getting it completed. Call this a niche industry that will attract a lot of imitators. To be profitable it needs mass production like on a circuit board assembly line.

* Then the next market needed will be some way to assure purchasers that the RFID Zapper that THEY got really works.
* Then the next society development will be that objects where RFID was inserted for purposes of identification, like in ID cards, Passports etc. Will malfunction because someone had used the RFID Zapper on them, rendering those people's ID unusable for the intended purposes.
* Then stores, and other institutions, will have to institute rules that people are not allowed to enter their premises carrying an RFID Zapper, so as to prevent unauthorized usage on the store merchandise.
* Then the next result might be that RFID Zappers will get declared to be illegal … although I expect this will be a few years away … the effort to illegalze RFID Zappers may get a lot more attention from the general public than the usual illegalization of technology tools.

There have been several problems with RFID deployment so far.
* There is the mass public panic over conspiracy theories, leading to a ton of Urban Legends, of which there is a glimmer of validity at the fringes. There are in fact some risks of abuse, but they are relatively small risks compared to the frenzy of claims out there.
* There's recent threads on the notion that el cheapo implementation can lead to security holes, where RFID is no exception to that risk, such as susceptibility to malware.
* Spread of the RFID Zapper into society and its effects will become problem area # 3.

Al Mac also pointed to the CAUTION section, which he described as" = ROFL." That section follows, idiosyncratic spelling and all.

>Caution

(This part of this article probably will be longer than the equivalent part in the german article, since english-speaking peoble seem to be more concerned with safety matters and less careful with electric devices ;-)

* Poldi kindly informed us, that having a RFID-Zapper with you when checking in to a plane might cause trouble or even get you arrested (he almost was). RFID-Zappers are basically some kind of pocket-EMP. Although we doubt that it has the capacity to cause any trouble aboard an airplane, we seriously recommend against testing it, for reasons of your own health as well as that of others.

* RFID-Zappers don't comply with the FCC-rules.

* Modifying a single-use-camera into a RFID-Zapper isn't completely free of risks. If the capacitor is still charged fully or partly, you might catch yourself an electric shock. If you are a healthy, young person, this is probably only going to hurt a lot, but if you should have any kind of problems with your heart and/or circulation, you definetly want to properly decharge the capacitor first. If you use a bigger capacitor, the risk increases.

* Soldering irons are known to be unpleasantly hot at the tip.

* We also recommend against using the RFID-Zapper on RFID-Tags found within electrical devices, for these are likely to suffer damage too. You also shouldn't use RFID-Zappers too near to electric devices, especially if they are expensive. You also shouldn't use it near any magnetic data storage, like floppy disc, MCs, hard discs, credit cards, streamer-cartridges and so on. And don't try it near your grandpa's pacemaker or other sensitive medical equipment either!

* We don't think that the RFID-Zapper is a strong source of what is known in Germany as Elektrosmog, which means some kind of smog caused by electromagnetic fields. But if you are concerned about it, you might want to be careful. Unfortunately we can't tell you wether wearing a hat of aluminium helps or not.

* The RFID-Zapper might cause you to feel armed against companies or governments trying to compromise your privacy. You might even experience euphoria, especially when destroying RFID-Tags. This could lead to dangerous behavior, like speaking your mind, using freedom of speech, fighting for your rights, all of which are bound to ultimately lead to the communist world revolution ;-)
* Shoplifting: No. This tool was not constructed as a burgular tool and is not to be used as. Besides, shops do not use RFID-Chips for eletronic theft prevention. However, it may be considered as such as a result of unknowledge.<

Category 25.3 *RFI, HERF, EMP/T*

2006-04-26 **electromagnetic inteference EMI personal electronic devices PEDs cell mobile phones aircraft control systems avionics fly-by-wire interference real-time control systems**

RISKS 24 26

PERSONAL ELECTRONIC DEVICES ON COMMERCIAL AIRCRAFT

Prof Peter Ladkin summarized the current state of knowledge about personal electronic devices (PEDs) on aircraft in a report for RISKS. He began with a summary of the problem:

"There has been plenty of discussion of the risks of operating personal electronic devices (PEDs) such as mobile telephones, gameboys and computers on board commercial transport aircraft. In the U.S., the use of mobile telephones on board flying aircraft is forbidden by the Federal Communications Commission, inter alia because such a phone would be within receiving range of many cells simultaneously and the technology is neither designed nor implemented to accommodate such cases. However, there is also the possibility of interference with the aircraft avionics."

His review of the literature strongly supports the aviation industry's concerns about electromagnetic interference (EMI) with avionics and points to widespread ignorance on the part of passengers about why PEDs are to be turned off during flight.

---

26 Health effects of electronic equipment (phones, screens, etc.)

Category 26 *Health effects of electronic equipment (phones, screens, etc.)*

2000-12-08 **RFI radio frequency interference emissions irradiation health hazards danger cellular phones mobile**

NewsScan, San Jose Mercury News
http://www0.mercurycenter.com/svtech/news/breaking/reuters/docs/723127l.htm

The British government will invest $10 million in a research program designed to investigate potential health hazards of cell phones and to mount a public information campaign advising cell phone owners that they should keep their calls short to minimize their exposure to radio waves, and that they should discourage cell phone use by children. Presenting its action as essentially a precautionary step, the government acknowledged that there is no irrefutable medical evidence that cell phones pose health risks.

Category 26 *Health effects of electronic equipment (phones, screens, etc.)*

2000-12-19 **RFI radio frequency interference emissions irradiation health hazards danger cellular phones mobile**

NewsScan

A study of 891 people who used cell phones for up to three years has found no evidence that cell phone use causes brain cancer. The study, which was funded by the industry group Wireless Technology Research and the National Cancer Institute, has been criticized by some scientists for being premature and inconclusive. Professor Henry Lai of the University of Washington says: "Since most solid tumors take 10 to 15 years to develop, it is probably too soon to see an effect." (AP/USA Today 19 Dec 2000)

Category 26 *Health effects of electronic equipment (phones, screens, etc.)*

2001-01-16 **cellular phone mobile cancer research**

NewsScan

STUDY LINKING CELL PHONE USE TO EYE CANCER CRITICIZED
An Essen (Germany) University Clinic study of 118 patients with uveal melanoma, a type of eye cancer, found that those cancer patients used cell phones and other such devices more often than 475 healthy individuals. Michael Foerster of the Free University in Berlin is one of the study's harshest critics: "The problem with the study is that it did not measure how much radiation the studied people had. With such a detailed energetic study, such results are biostatistical garbage." (Reuters/New York Times 15 Jan 2001)
http://partners.nytimes.com/reuters/technology/tech-germany-cellphon.html

---

Category 26 *Health effects of electronic equipment (phones, screens, etc.)*

2001-05-23 **cell phone safety radiation**

NewsScan

GAO AND CONGRESS CONSIDER CELL PHONE SAFETY
The U.S. General Accounting Office says that federal agencies such as the Federal Communications and the Food and Drug Administration have not been doing enough to make people understand that the safety of cell phones has not yet been conclusively determined. "It will likely be many more years before a definitive conclusion can be reached on whether mobile phone emissions pose any risk to human health." In another development, Congress is considering variations on legislation that would ban or restrict the use of a cell phone while driving an automobile. (AP/New York Times 23 May 2001)
http://www.nytimes.com/aponline/national/AP-Cell-Phone-Safety.html

---

Category 26 *Health effects of electronic equipment (phones, screens, etc.)*

2002-02-20 **RFI radio frequency interference emissions wireless communications health danger fraud lawsuit regulation**

NewsScan

FTC SUES SELLERS OF CELL PHONE "RADIO SHIELD" [20 Feb 2002]
The Federal Trade Commission is suing two companies for selling devices purporting, without good evidence, to shield people from harmful radiation emitted by their cell phones. The small metallic devices were sold under such names as WaveShield 1000, NoDanger, and SafeTShield. The FTC said that by claiming that their products could "block up to 97% to 99%" of electromagnetic radiation," the companies were actually "using a shield of misrepresentation to block consumers from the facts." Among the facts missing in company sales materials is any mention of a 2001 General Accounting Office report indicating that "scientific research to date does not demonstrate that the radio frequency energy emitted from mobile phones has adverse health effects, but the findings of some studies have raised questions indicating the need for further investigation." (Newsbytes/Washington Post 20 Feb 2002)
http://www.washtech.com/news/telecom/15264-1.html

Category 26 *Health effects of electronic equipment (phones, screens, etc.)*

2002-04-18 **toxic matrials hazardous waste disposal recycling**

NewsScan

LANDFILLS REJECT COMPUTER JUNK
What to do with old computers? Most landfills are refusing to accept them, because computer monitors and TV screens contain lead, mercury, cadmium and other hazardous materials that seep into soil and groundwater when they're crushed or burned. Well, can you give them to charitable organizations? Maybe, maybe not. Many refuse to accept them, because they can't afford to pay the disposal fees. One solution would be to use "pay-as-you-throw" programs offered by companies such as Hewlett-Packard and IBM, which charge $13 to $34 to pick up old computers. (San Jose Mercury News 17 Apr 2002)
http://www.siliconvalley.com/mld/siliconvalley/3085767.htm

26.1 Radiation

Category 26.1 *Radiation*

2002-05-24 **wireless cellular phone radiation standards health ergonomics legislation regulations limits**

NewsScan

WORLD'S STRICTEST CELL PHONE RADIATION LAW? IN CHINA!
China, which is below international norms for most environmental standards, is considering strict new regulations that would cut cell phone radiation emissions by half of what they are overseas. The cost to cell phone makers would be enormous, because China represents such a huge market for cell phones and because manufacturers would have to redesign their entire operations, from R&D to production. Scientific studies have so far failed to find any evidence that cell phone emissions cause brain cancer, but the World Health Organization (WHO) has also said that further research is necessary before ruling out that possibility. (Reuters/USA Today 24 May 2002)
http://www.usatoday.com/life/cyber/tech/2002/05/24/china-cell-radiation.htm

---

Category 26.1 *Radiation*

2003-09-30 **3G wireless signals sick headache nausea**

NewsScan

3G WIRELESS SIGNALS COULD MAKE YOU SICK
Radio signals used for next-generation (3G) wireless services can cause headaches and nausea, according to a study conducted on behalf of the Netherlands ministries for Economic Affairs, Health and Telecommunications. The study compared the impact of radiation from base stations used for current wireless services with those for new 3G networks, which transfer data at a faster rate. "If the test group was exposed to third-generation base station signals there was a significant impact. They felt tingling sensations, got headaches and felt nauseous," says a spokeswoman for the Dutch Economics Ministry. The Dutch government said follow-up research was needed. Previous research on health effects of mobile phones, primarily second-generation, has been inconclusive, but a long-term study conducted by the International Agency on Research on Cancer is expected to yield results next year. (Reuters 30 Sep 2003)

Category 26.1 *Radiation*

2004-11-16 **glaucoma computer screens sight blindness**

NewsScan; http://www.msnbc.msn.com/id/6493299/

HEAVY COMPUTER USE LINKED TO GLAUCOMA

Researchers at the Toho University School of Medicine in Tokyo have found that long hours spent in front of a computer screen may increase the risk of glaucoma in nearsighted people. Glaucoma, which is caused by damage to the optic nerve, results in blind spots or visual impairments that can lead to blindness. The research is based on a study of 10,000 workers in Japan who were tested for the disease, with results correlated to data on how many hours were spent on the computer and also preexisting visual problems, such as myopia. Scientists said they believe the optic nerve in myopic people might be more vulnerable to computer-caused stress than in normal eyes. "Computer stress is reaching higher levels than have ever been experienced before. In the next decade, therefore, it might be important for public health professionals to show more concern about myopia and visual field abnormalities in heavy computer users," says the report published in the British Journal of Ophthalmology. (Reuters/MSNBC 16 Nov 2004)

Category 26.1 *Radiation*

2005-07-29 **magnetic resonance imaging MRI systems failure harm patients radiation burns reporting control systems flaws**

RISKS 23 95

HITACHI MAGNETIC RESONANCE IMAGING SYSTEMS MAY BE FLAWED

The U.S. Food and Drug Administration warned Hitachi Medical Systems America Inc. That it failed to properly report burns, hearing losses, and other injuries to patients using its magnetic resonance imaging (MRI) systems. The FDA suggested that this "may be symptomatic of serious problems in your firm's manufacturing and quality assurance systems. You must promptly initiate permanent corrective and preventive action. The FDA described one unreported case in which a woman complained she was "shocked and burned on the top of her head while being scanned" by a Hitachi MRI system, and another in which an MRI device caught fire.

[Source: A Reuters item, 26 Jul 2005; abstract by Peter G. Neumann]

26.2 Toxic materials

Category 26.2 *Toxic materials*

2002-05-10 **ergonomics health hazards microbes germs workstations computers**

NewsScan

EEWWW! WORKSTATIONS ARE 'DIRTIER THAN TOILETS'
A study by University of Arizona microbiologist Chuck Gerba has revealed a "bacterial nightmare" lurking on the keyboards of the average computer workstation. Gerba's study, which swabbed keyboards, telephones and office lavatories and compared the bacterial count on each, showed the telephone as the worst offender, followed by the workstation, which had 400 times more bacteria than the average toilet. Unlike bathrooms, most workstations are rarely cleaned, says Gerba, leaving them the repositories for "millions of bacteria that could potentially cause illness." (vnunet.com 9 May 2002)
http://www.vnunet.com/News/1131608

Category 26.2 *Toxic materials*

2002-09-27 **toxic waste international shipping dumping**

NewsScan

CHINA REFUSES TO ACCEPT U.S. ELECTRONIC JUNK
Customs officials in China's Zhejiang province have said they will not accept receipt of 400 tons of electronic trash — scrap computer monitors, keyboards, copiers and color TV sets — that arrived two weeks ago and has sat unclaimed. The 22 containers, each 40 feet long, were marked "electronic products." "As the address and telephone number on the shipping bills are fake, we believe this is most likely a deliberate move to transfer electronic garbage," said one official. Such items are banned under Chinese law from entering the country, and the containers will be returned to where they came from, said the official. (AP 26 Sep 2002)
http://apnews.excite.com/article/20020926/D7M9K5BO0.htm

Category 26.2 *Toxic materials*

2002-10-28 **toxic materials recycling**

NewsScan

PHONE RECYCLING GETS A BOOST
With more than 128 million cell phone users in the U.S. upgrading their handsets every 18 months on average, a record number of obsolete devices are hitting incinerators and landfills. That has environmentalists concerned because the phones contain toxins such as lead, cadmium and mercury that "accumulate in the environment and can cause damage to the ecosystem," says Eric Most, director of INFORM's Solid Waste Prevention Program. By 2005, INFORM predicts that 130 million cell phones weighing about 65,000 tons will be "retired" annually in the U.S. But now users have the option of donating their old phones to nonprofit groups or developing nations, or sending them off to be recycled in environmentally safe ways. "The simple act of recycling your cell phone can have profound ramifications," says Seth Heine, president of Collective Good (www.collectivegood.com), which runs a cell phone collection program. "The money can be used for immunization to keep a child from dying from a disease, or you can save 1,000 square feet of rain forest forever." People can also donate phones through www.donateaphone.com, operated by the Cellular Telecommunications and Internet Association's Wireless Foundation. Phones can be dropped off at Radio Shack, The Body Shop and Sprint PCS stores. (Reuters 26 Oct 2002)
http://makeashorterlink.com/?V2D631342

Category 26.2 *Toxic materials*

2002-11-11 **software disks waste toxic materials marketing protest**

NewsScan

DISK WAR
Two California men have been organizing a massive but polite attack on AOL for that company's distribution of promotional disks; they've established a Web site to encourage people to send them unwanted disks offering trial subscriptions to AOL's service, and when they have collected a million of the disks they'll haul them to the company's Virginia headquarters: "Basically, we'll enlist the help of volunteers who are willing to take a pickup load and drive back to AOL headquarters with us." Their hope is that the publicity stunt will demonstrate to the company that people consider its disk-distribution practices a waste of resources and a detriment to the environment. (AP/CNN Money 11 Nov 2002)
http://money.cnn.com/2002/11/11/news/aol_cds.ap/

Category 26.2 *Toxic materials*

2003-01-10 **recycling toxic materials**

NewsScan

U.S. TECH COMPANIES RANK LOW IN RECYCLING EFFORTS
The Silicon Valley Toxics Coalition (SVTC) has released its annual Computer Report Card comparing the environmental records of 28 high-tech firms, and reports that most U.S. companies lag behind their Japanese competitors when it comes to recycling equipment and safe disposal of hazardous substances used in the manufacturing process. Of the companies surveyed, only Fujitsu received a passing grade. It's one of a handful of Japanese companies that has sought to eliminate toxic chemicals by developing and using lead-free products. "The leadership continues to be by and large the Japanese companies, and the U.S. companies tend to be far behind," says SVTC founder Ted Smith. "A lot of (U.S. manufacturers') initiatives are piecemeal and not really designed to address the vast majority of consumer concerns. There is still an enormous amount of computer waste being exported to China." The Computer Report Card notes that some U.S. companies use a double standard when it comes to recycling. Divisions located in Europe and Japan, where safe recycling is mandated by law, have implemented programs but their U.S. operations have not. Meanwhile, Congressman Mike Thompson (D-Calif.) has introduced a bill that would require the EPA to create grants for private and governmental organizations to develop computer recycling programs and the National Electronics Product Stewardship Initiative is working on a nationwide plan for recycling obsolete electronic devices. (Wired.com 10 Jan 2003)

Category 26.2 *Toxic materials*

2003-02-06 **computer recycling waste toxic materials**

NewsScan

HP OFFERS CONSUMER INCENTIVES FOR COMPUTER RECYCLING
Hewlett-Packard will offer e-coupons exchangeable for HP products when users recycle old computer hardware through the company. The coupons will range from $20 to $50 in value, depending on the amount a consumer spends on recycling services, which cost from $17 to $30 depending on the size of the equipment to be recycled. An HP executive said: "This is a way to learn what our customers want. Do they even want an incentive? Or do they just want to fill out a form and leave a box on their doorstep? We know that waste is a growing problem in the industry, but no one has really studied what consumers want to do to get rid of their computers." (AP/San Jose Mercury News 6 Feb 2003)

Category 26.2 *Toxic materials*

2003-02-26 **high technology computer waste toxic materials recycling**

NewsScan

E-WASTE RECYCLERS UNITE!
A group of 16 electronics recycling firms has signed an "Electronics Recycler's Pledge of True Stewardship," vowing to uphold stricter standards for processing electronic waste, including old computers, cell phones, TV sets and monitors, which contain hazardous materials such as lead and mercury. "We hope the pledge will really set the standard for how electronics recyclers operate their business," says David Wood, organizational director of the Computer TakeBack Campaign. "We hope that attention around it will raise the performance of other companies that are not presently signers." The companies have pledged not to dump discarded electronics into landfills, and to prevent their export to foreign countries. They also say they'll stop using prison labor to dismantle and recycle or refurbish old electronic devices. The group's actions come in response to startling results reported last year in a study, "Exporting Harm: The High-Tech Trashing of Asia." That study, produced by the Silicon Valley Toxics Coalition and the Basel Action Network, found that 50% to 80% of e-waste collected in the U.S. is shipped to developing countries like China, India and Pakistan. (Wired.com 26 Feb 2003)

Category 26.2 *Toxic materials*

2003-03-05 **toxic materials recycling waste**

NewsScan

'REVERSE PRODUCTION' SYSTEM RECYCLES ALL
A study underway at Georgia Tech could offer a model for responsible recycling of electronic waste. Researchers have developed a "reverse production" system that enables every raw material contained in e-waste — metals such as lead, copper, aluminum and gold, as well as plastics, glass and wire — to be recovered and reused. Scientists say such "closed loop" manufacturing offers a win-win situation for manufacturers and consumers, and the project is generating buzz abroad, with officials in Taiwan and Belgium expressing interest in the system. Key to the process is chemical engineer Matthew Realff's design for a means to separate metals, as well as different qualities of plastics from crushed, ground-up components. From this work, new industries could be created to recover value not only from e-waste, but also from automobiles and other durable goods, says Realff. (Science Daily 4 Mar 2003)

Category 26.2 *Toxic materials*

2004-06-04 **toxic dust processors monitors reproductive neurological disorders**

NewsScan

TOXIC DUST

A survey by environment groups called the Silicon Valley Toxics Coalition says that "toxic dust" found on computer processors and monitors contains chemicals linked to reproductive and neurological disorders. Coalition director Ted Smith says, "This will be a great surprise to everyone who uses a computer. The chemical industry is subjecting us all to what amounts to chemical trespass by putting these substances into use in commerce. They continue to use their chemicals in ways that are affecting humans and other species." However, physician Gina Solomon of the Natural Resources Defense Council says: "The levels in the dust are enough to raise a red flag, but not enough to create a crisis. I have an old computer monitor in front of me now, and I'm not about to throw it away. But when I get a new one, it darn well will be free of these chemicals." A Dell spokesman says, "People can be very confident about their new computer purchase. We've worked a lot with suppliers, and we require audits and material data sheets on all our products." (AP/Los Angeles Times 4 Jun 2004

Category 26.2 *Toxic materials*

2004-11-11 **nanotech EPA environment risks threats dangers biology medicine nanotubes**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A43763-2004Nov11.html

STUDYING NANOTECH RISKS

The Environmental Protection Agency has awarded $4 million in grants to a dozen universities to study the biological and medical implications of nanotechnology, which has already yielded such products as carbon "nanotube" electrical wires; cages of atoms that can capture pollutants in water and soil; and catalysts that reduce manufacturers' dependence upon caustic chemicals. Recognizing that these materials are small enough to enter the lungs (and perhaps even be absorbed through the skin and travel to the brain and other organs), EPA official Paul Gilman explained: "This emerging field has the potential to transform environmental protection, but at the same time we must understand whether nanomaterials in the environment can have an adverse impact." Barbara Karn of the EPA's Office of Research and Development says the projects funded by the new grants will do "infinitely more" on nanotech safety than has ever been done previously. (Washington Post 11 Nov 2004)

Category 26.2 *Toxic materials*

2005-01-07 **recycling Intel eBay toxic electronics disposal heavy metals cadmium mercury chrome**

NewsScan; http://apnews.excite.com/article/20050107/D87F998O2.html

RECYCLING ELECTRONIC GADGETS

EBay and Intel have developed a recycling program that encourages Americans to safely dispose of their discarded computers and other electronic devices. Gartner, the marketing research firm, estimates that U.S. consumers decommission 133,000 personal computers every day, and eBay chief executive Meg Whitman says that the user's quandary is, "You don't want to throw them out, and you don't know what to do with them." If not properly disposed of, discarded electronic devices can leak lead, cadmium, chromium, mercury and other toxins into the environment. The new eBay- Intel "Rethink" recycling program will only endorse recyclers who promise not to dump machines in landfills in developing nations. (AP 7 Jan 2005)

Category 26.2 Toxic materials

2005-01-21 **toxic waste electronics China US international Basel Convention treaty**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A24672-2005Jan20.html

E-WASTE IS PILING UP

Consumers' penchant for constant upgrades -- new cell phones, a sleeker laptop -- is causing havoc in the environment, and with technology products now accounting for as much as 40% of the lead in U.S. landfills, e-waste has become one of the fastestgrowing sectors of the U.S. solid waste stream. The International Association of Electronics Recyclers estimates that Americans dispose of 2 million tons of electronic products a year -- including 50 million computers and 130 million cell phones -- and China, which has served for years as the final resting place for Americans' unwanted TVs and computers, is becoming overwhelmed by the volume. Some high-tech companies are taking matters into their own hands -- Hewlett Packard and Dell job out their e-waste handling to environmentally sensitive recyclers such as RetroBox -- but such efforts are still quite limited and unable to cope with a problem that's reaching crisis proportions. Meanwhile, the U.S. is the only developed country not to have ratified the 1992 Basel Convention, the international treaty that controls the export of hazardous waste. "There's a real electronics-waste crisis," says Basel Action Network coordinator Jim Puckett. "The U.S. just looks the other way as we use these cheap and dirty dumping grounds." (Washington Post 21 Jan 2005)

26.3 Heat

Category 26.3 *Heat*

2004-06-28 **mobile phone health risk sperm count decrease**

NewsScan

MOBILE PHONES CUT SPERM COUNT

Men who regularly carry a mobile phone could have their sperm count reduced by as much as 30% according to a new study by Hungarian researchers. Those who place their phone near their groin, on a belt or in a pocket, are at greatest risk. The research findings are the first to suggest that male fertility could be affected by the radiation emitted by mobile phones, also long suspected of causing cancer. The study found the sperm that did survive exposure to mobile phone radiation showed abnormal movements, further reducing fertility. But experts are advising men not to panic yet. (The Australian 28 Jun 2004) Rec'd from John Lamp, Deakin University

26.4 Distraction

Category 26.4 Distraction

2006-02-10 **mobile cell phone driving risks dangers distraction concentration automobile**

The Straight Dope http://www.straightdope.com/columns/060210.html

DON'T DRIVE WHILE USING CELL PHONES

Cecil Adams, author of the popular "THE STRAIGHT DOPE" column, summarized the case against driving while talking on cell phones as follows:

Accumulating evidence suggests gabbing on the phone while driving is definitely dangerous, probably more so than other distractions. What's more, hands-free phones don't solve the problem. What gets you into trouble, it seems, isn't so much fumbling with the phone (though that doesn't help) as the apparent fact that driving and conducting a conversation at the same time consumes more mental processing power than most people can spare. A few data points:

Cell phones are involved in a lot of crashes. Best evidence: investigations of actual incidents. One study of 456 accidents in Australia requiring a hospital visit (McEvoy et al, BMJ, 2005) found that in nine percent of cases (40 crashes) the driver had been talking on a cell phone during the ten minutes prior to the accident, based on phone records. The authors conclude, "A person using a mobile phone when driving is four times more likely to have a crash that will result in hospital attendance." A 1997 study of 699 accidents in Toronto (Redelmeier and Tibshirani, New England Journal of Medicine) came to a comparable conclusion.

In another study, researchers at the Virginia Tech Transportation Institute installed cameras, sensors, and data recording equipment in 100 cars, then watched what happened over the ensuing 12 to 13 months. They recorded 69 crashes, 761 near crashes, and 8,295 lesser close calls. Of driver distractions that may have contributed to these incidents, use of cell phones was by far the most common, occurring in close to 700 cases. The distant runner-up was passenger-related activities, presumably including conversation, with fewer than 400 instances. Of the cell-phone-related distractions, 87 involved dialing a handheld phone and 466 talking or listening.

Hands-free phones don't help much. Although laws restricting cell phone use in cars typically make an exception for the hands-free variety, numerous studies show such phones aren't markedly safer. Dialing does make you take your eyes off the road, but as suggested above most cell-phone-related accidents seem to happen while the driver is merely conversing.

Drivers using cell phones have slower reaction times and miss important visual cues. Studies using driving simulators have found that drivers brake slower, fail to see pedestrians and traffic signals, and otherwise pay less attention to the road while on the phone. Some experts compare driving while phoning to driving while drunk, but a study by folks at the University of Utah (Strayer et al, 2004) suggests that in certain respects drunks actually do better behind the wheel than phone users--they seem to stay closer to the speed limit and brake faster in response to braking vehicles ahead. All in all, there's solid evidence that talking on the phone is among the more dangerous things you can do while driving.

. . . .

27.1 Vulnerability assessment

Category 27.1 *Vulnerability assessment*

1997-01-06 **SATAN**

RISKS 18 74

Dan Farmer's complete unauthorized Internet security survey was made available on < http://www.infowar.com >. The study showed widespread occurrences of well-known vulnerabilities in the majority of systems scanned, including especially financial systems.

Category 27.1 *Vulnerability assessment*

1997-01-21 **SATAN**

EDUPAGE

Dan Farmer's Internet security scan using his SATAN program continued making belated news in the business press. About 68% of the 660 banks studies by Farmer had inadequate security by his standards. Farmer said that system administrators are underfunded and under pressure "just to keep things running — not necessarily secure."

Category 27.1 *Vulnerability assessment*

1997-02-11 **biometrics fingerprint**

EDUPAGE

A biometric authentication device costing $500 and easy to attach to PCs and other computers is being marketed by Oracle Corporation in conjunction with a company called Identix, from Sunnyvale, CA. The device can distinguish a live finger from a model or dead finger using a number of sensors.

Category 27.1 *Vulnerability assessment*

1997-07-05 **computer forensics**

Financial Post (Canada)

The new Geographic Profiling System called Orion (available from Environmental Criminology Research in Vancouver, BC) helps police narrow down the likely residence of serial criminals. Working in conjunction with the RCMP's ViCLAS (Violent Crime Linkage Analysis System) program, Orion helps law enforcement officers enlist the help of local residents where criminals are likely to live.

Category 27.1 *Vulnerability assessment*

1997-07-24 **computer forensics evidence recovery**

Reuter

In Britain, a new firm called Computer Forensic Investigations launched a new data-recovery kit for police officers to salvage data from suspects' computers in the field. The "portable evidence recovery unit" (PERU) has already been widely used by forces in the UK in cases of fraud, murder, blackmail, counterfeiting and child pornography.

Category 27.1 *Vulnerability assessment*

1997-07-24 **computer forensics fraud data mining**

Computing (UK)

British Telecom and MCI have been using data mining techniques to identify patterns of phone-card number theft. The joint project, dubbed "Sheriff", applies statistical pattern recognition algorithms for real-time analysis of phone traffic to spot stolen cards.

Category 27.1 *Vulnerability assessment*

1999-02-01 **criminal hacker attack challenge revenge credit records**

RISKS 20 19

ICSA.net. has long warned vendors not to stage hacking challenges. These purported tests of security software are uncontrolled and teach little or nothing about the effectiveness of security systems. In January, Gen Technology, the maker of Access Denied network security software challenged hackers to break their system. Unfortunately, a criminal hacker who had boasted that he'd be able to crack the system within five minutes failed to break in at all. Enraged, the criminal then damaged the credit rating of Paul Smith, one of the software engineers on the development team, so badly that Mr Smith was precluded from receiving a home loan.

Category 27.1 *Vulnerability assessment*

1999-04-21 **war dialer tiger teams commercial product vulnerability**

Business Wire

Sandstrom Enterprises Inc. of Cambridge, MA announced its commercial-grade war dialer, PhoneSweep. War dialers scan large numbers of phones for unauthorized modems; however, free hacker tools always pose a problem of quality and safety, since there's no guarantee that a criminal hacker has not inserted Trojan horse code in the software. See <http://www.phonesweep.com> for details.

Category 27.1 *Vulnerability assessment*

1999-11-20 **scanner vulnerability audit tool WindowsNT firewalls intrusion detection**

InternetWeek

BindView Corp. and Network Associates announced their latest vulnerability scanning tools in November. Bindview's Hackshield 2.- and NAI's CyberCop Scanner 5.5 both announced new features such as better reporting and automatic repair of vulnerabilities.

Category 27.1 *Vulnerability assessment*

1999-12-01 **password crack guess tool sniffer detection intrusion criminal hacker**

PC Magazine

The people at the L0pht announced two anti-hacking tools for modest fees. L0phtCrack provides efficient brute-force and dictionary-based analysis of network passwords; AntiSniff detects workstations that are configured in promiscuous mode to trap all network traffic in violation of normal security rules.

Prospective clients should be aware of L0pht's history. Their FAQ states that they are, "Just a bunch of hackers who got together and started working on projects together. One of the projects turned out to be L0pht.com. There are remnants of different groups that make up L0pht such as RDT, cDc, RL, etc. We didn't start this thing off to make money. We did this, and still do, out of a love we have for technology and making it do things that it might not have originally been meant to."

Their Web site features a FREE KEVIN logo and advertises an archive of files "especially useful to all Network Administrators, Hackers, Computer Security Professionals, Phreakers, Computer Teachers, Crackers, Lab Monitors, Virus Writers, Communication Specialists, and anyone else that wishes to have a copy of this unique archive collection for their personal use."

The members of L0pht continue to present themselves using their hacker handles; examples include "Mudge," "Weld Pond" and "Space Rogue."

Personally and professionally, I would no more run any of L0pht's products on a production system or a system connected to a trusted network or to the Internet than I would install BackOrifice written by cDc, the Cult of the Dead Cow) on such a system.

Caveat emptor.

Category 27.1 *Vulnerability assessment*

1999-12-03 **vulnerability assessment scanner new version summary statistics**

InternetWeek

Axent Technologies announced release of its newest version of NetRecon (v. 3.0) with improved analytical tools and efficient, prioritized summaries of vulnerabilities.

Category 27.1 *Vulnerability assessment*

2000-02-21 **QA quality assurance source code scanner database**

RISKS, http://www.rstcorp.com/its4/ 20 81

John Viega announced release of an open-source vulnerability scanner for C and C++ source code. ITS4 uses a database of vulnerabilities and is open to refinements by its users to identify increasingly subtle security flaws in code. The Web site described the product as follows:

"ITS4 Software Security Tool

The Software Security Group at Cigital designs, analyzes and tests security-critical software. We developed ITS4 to help automate source code review for security. ITS4 is a simple tool that statically scans C and C++ source code for potential security vulnerabilities. It is a command-line tool that works across Unix and Windows platforms.

ITS4 scans source code, looking for function calls that are potentially dangerous. For some calls, ITS4 tries to perform some code analysis to determine how risky the call is. In each case, ITS4 provides a problem report, including a short description of the potential problem and suggestions on how to fix the code.

ITS4 and its source code are provided here to the security community for any use that does not compete with Cigital's consulting practice."

Category 27.1 *Vulnerability assessment*

2002-01-22 **financial security services outsourcing management**

NewsScan; http://news.ft.com/news/industries/infotechnology

IBM AND VERISIGN INK SECURITY ALLIANCE
IBM and VeriSign have established a global alliance to provide Internet security services to large corporations in a move that could generate more than $1 billion over the next three years. VeriSign will use IBM's computer systems to run its future digital security services. Previously, VeriSign had used servers from Sun Microsystems. (Financial Times 22 Jan 2002)

Category 27.1 *Vulnerability assessment*

2002-01-24 **security industry collaboration communications encryption services e-commerce**

Security Wire Digest, http://www.ibm.com/news/us/2002/01/22.html 4 6

In January 2002, IBM and VeriSign announced a partnership to support a wide range of security services including "secure messaging, secure extranets, intranets and e-commerce sites, as well as secure document management." According to an article by Shawna McAlearney writing in Security Wire Digest, industry analysts saw the move as an aggressive push to take advantage of the two companies relative areas of expertise in support and in security technology to increase their market share in the security arena.

Category 27.1 *Vulnerability assessment*

2002-04-25 **vulnerability analysis software quality assurance QA patches false positives**

Security Wire Digest 4 32

The Microsoft Baseline Security Analyzer (MBSA) was released in early April 2002; by the end of the month, widespread reports indicated that the product was prone to excessive false positives, with many installed patches displayed as missing. Microsoft responded that they were aware of the problems.

Category 27.1 *Vulnerability assessment*

2003-09-12 **vulnerability scada systems grid electric hacker shut down North America back doors**

NewsScan

VULNERABILITY OF ELECTRIC GRID SYSTEM
Researchers say that "back doors" in the digital relays and control room technology managing direct electricity flow in North America is vulnerable to computer viruses and hackers. Cybersecurity researcher Eric Byres of the British Columbian Institute of Technology in Vancouver says: "I know enough about where the holes are. My team and I could shut down the grid. Not the whole North American grid, but a state, sure." He's frustrated because he's contacted a well-known manufacturer — whom he declined to name for security reasons — and urged that the weakness be fixed before hackers found it. Gary Seifert, a researcher with the Energy Department's Idaho National Engineering and Environmental Laboratory, defines the problem this way: "We have a plethora of intelligent electrical devices going into substations and power stations all over the United States. What's to keep somebody from accessing those devices and changing the settings?... We're still going to have back doors no matter how hard we try. You can't keep them out but you hope to slow them down." (AP/USA Today 12 Sep 2003)

Category 27.1 *Vulnerability assessment*

2003-12-23 **port scanning vulnerability assessment reliability network computer ISP block erratic unpredictable erroneous false information**

RISKS 23 10

Reliability of external port vulnerability testing is decreasing due to erratic ISP port blocking

RISKS contributor Charles Preston notes that some ISPs are unannouncedly blocking some ports for their clients' Internet access. When ISPs are asked which ports they were blocking, Preston say, "they are incorrectly stating that they are not blocking any ports, and they are making changes without any notification to customers." In addition, no given ports are guaranteed to be blocked on an ISP's network. As a result, testing one's firewalls using external testing services may not reveal vulnerabilities of ports that are temporarily protected by ISP blocks but that will become open to attack at unpredictable times in the future.

Category 27.1 *Vulnerability assessment*

2005-04-14 **rootkits security problem antivirus vendor warning malicious actions lack of statistics information**

DHS IAIP Daily;
http://informationweek.com/story/showArticle.jhtml?articleID=160900692

ROOTKITS COULD POSE A SERIOUS SECURITY PROBLEM

The hacker equivalent of a cloak of invisibility may cause serious problems for users and anti-virus vendors, a security expert said Thursday, April 14. Rootkits are tools used by hackers to cover their tracks. Rootkits can hide the existence of other malware on a computer by modifying file data, Windows registry keys, or active processes, all of which are used by malicious code detection software to spot worms, viruses, and spyware that's been installed on a PC. They're commonly used by spyware writers, but they're now gaining popularity among virus writers, say some security analysts. According to Panda Software's research director, rootkits for Windows are proliferating. "Even though they're not new, rootkits have re-emerged as a kind of malware that could let hackers discreetly carry out numerous malicious actions," said Luis Corrons. "We've seen that they're being used in combination with backdoors to take remote control of computers." But Ken Dunham, the director of malicious code research for iDefense, is not as convinced as others that rootkits for Windows are that big of a deal. "I think it's a growing trend, but it's really hard to identify [the scope]. There just aren't a lot of stats."

Category 27.1 *Vulnerability assessment*

2005-06-28 **SecurityFocus Sun Solaris Runtime linker vulnerability systems variables setuid setgid binaries privileges**

DHS IAIP Daily; http://www.securityfocus.com/bid/14074/discuss

SUN SOLARIS RUNTIME LINKER LD_AUDIT PRIVILEGE ESCALATION VULNERABILITY

Runtime linkers in most operating systems are designed to ignore LD_* environment variables when executing setuid or setgid binaries. The manual page describing ld.so for Sun Solaris also states that certain precautions are taken when setuid or setgid binaries are executed. Reportedly these precautions are not properly followed when LD_AUDIT is utilized. This vulnerability allows local attackers to gain superuser privileges on affected computers. 11 Sun has released Interim Diagnostic Relief fixes to address this issue: http://sunsolve.sun.com/tpatches

---

Category 27.1 *Vulnerability assessment*

2005-07-01 **vulnerability US-CERT compromises fix Santy worm phpBB**

DHS IAIP Daily; http://www.us−cert.gov/current/current_activity.html#phpBB_v ul

EXPLOIT FOR VULNERABILITY IN PHPBB

US-CERT is aware of a public exploit for a vulnerability in phpBB's "viewtopic.php" script. There are reports of attempts at exploitation, but no confirmed evidence of successful system compromises. A fix for this vulnerability was addressed in version 2.0.11, but did not adequately resolve the issue. In 2004, this vulnerability lead to the propagation of the Santy worm. The phpBB Development Team has released phpBB version 2.0.16 to fully correct this issue. US-CERT encourages administrators to apply the appropriate fixes as soon as possible. More information about this vulnerability can be found in the following US-CERT Vulnerability Note VU#497400: http://www.kb.cert.org/vuls/id/497400 phpBB version 2.0.16: http://www.phpbb.com/downloads.php

---

Category 27.1 *Vulnerability assessment*

2005-07-02 **Exploit vulnerability Microsofts JVIEW Profiler Microsoft Java Virtual Machine HTML COM**

DHS IAIP Daily; http://www.us−cert.gov/current/current_activity.html#jview

EXPLOIT FOR VULNERABILITY IN MICROSOFT'S JVIEW PROFILER (JAVAPRXY.DLL)

US-CERT is aware of a working public exploit for a vulnerability in the Microsoft JVIEW Profiler (javaprxy.dll) component, an interface to the Microsoft Java Virtual Machine. This vulnerability can be exploited when a user attempts to view an HTML document (e.g., a web page or an HTML email message) that attempts to instantiate the JVIEW Profiler COM object in a certain way. Successful exploitation could allow an attacker to execute arbitrary code on the user's system with privileges of the user. Microsoft has published a Security Advisory about this issue and is continuing to investigate the problem. Until a patch is available to address this vulnerability, US-CERT strongly encourages users to review the workarounds section of Vulnerability Note VU#939605. VU#939605: http://www.kb.cert.org/vuls/id/939605 Microsoft Security Advisory (903144): http://www.microsoft.com/technet/security/advisory/903144.ms px

---

Category 27.1 *Vulnerability assessment*

2005-07-04 **Secunia Cacti shell injection vulnerabilities security overwrite structures filtering privileges SQL attacks shell**

DHS IAIP Daily; http://secunia.com/advisories/15908/

CACTI SECURITY BYPASS AND SHELL COMMAND INJECTION

Two vulnerabilities have been reported in Cacti, which can be exploited by malicious people to bypass certain security restrictions and compromise a vulnerable system. 1) Input passed to the "no_http_headers" parameter isn't properly verified before being used. This can be exploited to overwrite session structures and bypass certain filtering mechanisms. Successful exploitation allows people to gain administrative privileges and perform various SQL injection attacks, but requires that "register_globals" is enabled. 2) An error in the administrative interface can be exploited to inject arbitrary shell commands by manipulating the path to "rrdtool". Successful exploitation requires administrative privileges. The vulnerabilities have been reported in version 0.8.6e and prior. Users should update to version 0.8.6f: http://www.cacti.net/download_cacti.php

---

Category 27.1 *Vulnerability assessment*

2005-07-04 **Sun JDS vulnerability Linux Websites flaw error applets**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/

SUN JAVA DESKTOP SYSTEM (JDS) APPLET SECURITY BYPASS VULNERABILITY

A vulnerability was identified in Sun Java Desktop System (JDS) for Linux, which could be exploited by malicious Websites to compromise a vulnerable system. This flaw is due to an unspecified error when handling specially crafted applets, which may be exploited, via a malicious Webpage, to bypass the default security policy and read/write arbitrary files on a vulnerable system or execute local applications with the privileges of the user running the untrusted applet. Users should upgrade to Sun Java Desktop System (JDS) Release 2 with the updated RPMs patch 118752-02. Sun advisory 101799: http://sunsolve.sun.com/search/document.do?assetkey=1-26-101 799-1

Category 27.1 *Vulnerability assessment*

2005-07-05 **Buffer overflow vulnerability Adobe Reader exploitation PDF email link Linux Solaris**

DHS IAIP Daily; http://www.adobe.com/support/techdocs/329083.html

BUFFER OVERFLOW VULNERABILITY IN ADOBE READER

A vulnerability within Adobe Reader has been identified within the Adobe Reader control. If exploited, it could allow the execution of arbitrary code under the privileges of the local user. Remote exploitation is possible if the malicious PDF document is sent as an email attachment or if the PDF document is accessed via a web link. Linux or Solaris users: download Adobe Reader 7.0 at http://www.adobe.com/products/acrobat/readstep2.html. IBM-AIX or HP-UX: download Adobe Reader 5.0.11 at http://www.adobe.com/products/acrobat/readstep2.html.

Category 27.1 *Vulnerability assessment*

2005-07-05 **EasyPHPCalendar inclusion vulnerability compromise include files**

DHS IAIP Daily; http://secunia.com/advisories/15893/

EASYPHPCALENDAR "SERVERPATH" FILE INCLUSION VULNERABILITY

A vulnerability has been reported in EasyPHPCalendar which can be exploited by malicious people to compromise a vulnerable system. Input passed to the "serverPath" parameter isn't properly verified, before it is used to include files. This can be exploited to include arbitrary files from external and local resources. Successful exploitation requires that "register_globals" is enabled. The vulnerability has been reported in version 6.1.5 and prior. Other versions may also be affected.

Category 27.1 *Vulnerability assessment*

2005-07-06 **McAfee IntrusShield Security Management System vulnerabilities sanitize data HTML**

DHS IAIP Daily; http://www.securityfocus.com/bid/14167/exploit

MCAFEE INTRUSHIELD SECURITY MANAGEMENT SYSTEM MULTIPLE VULNERABILITIES

McAfee IntruShield Security Management System is susceptible to multiple vulnerabilities. The first two issues are cross-site scripting vulnerabilities in the 'intruvert/jsp/systemHealth/SystemEvent.jsp' script. These issues are due to a failure of the application to properly sanitize user-supplied data prior to utilizing it in dynamically generated HTML. The next two issues are authorization bypass vulnerabilities leading to information disclosure and the ability to acknowledge, de-acknowledge, and delete security alerts. These vulnerabilities require a valid user account in the affected application. Users of affected packages should contact the vendor for further information on obtaining fixes.

Category 27.1 *Vulnerability assessment*

2005-07-06 **PHPWebsite SQL Injectrion Cross site vulnerabilities scripting directory input validation error**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/0993

PHPWEBSITE SQL INJECTION AND CROSS SITE SCRIPTING VULNERABILITIES

Multiple vulnerabilities were identified in PHPWebSite, which could be exploited by malicious users to conduct SQL injection, cross site scripting and directory traversal attacks. These flaws are due to an input validation error in the search module that does not properly filter a specially crafted "mod" parameter, which could be exploited by remote attackers to conduct SQL injection, cross site scripting and directory traversal attacks. PHPWebSite version 0.10.1 and prior are affected. Users should apply the patch: http://phpwebsite.appstate.edu/downloads/security/phpwebsite _security_patch_20050705.2.tgz

---

Category 27.1 *Vulnerability assessment*

2005-07-06 **IBM Lotus Notes HTML vulnerability email JavaScript sanitised**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/0995

IBM LOTUS NOTES HTML ATTACHMENTS SCRIPT EXECUTION VULNERABILITY

A vulnerability was identified in IBM Lotus Notes email client, which could be exploited to conduct cross site scripting attacks. The problem is that JavaScript code included in HTML attachments is not properly sanitised before being displayed, which may be exploited by attackers to cause arbitrary scripting code to be executed by the user's browser. DHS IAIP Daily; IBM Lotus DHS IAIP Daily; Notes 6.5.4 and prior are affected. No official patch is known at this time.

Category 27.1 *Vulnerability assessment*

2005-07-06 **McAfee IntruShield Security Management System vulnerabilities multiple scripting sanitize data HTML**

DHS IAIP Daily; http://www.securityfocus.com/bid/14167/info

MCAFEE INTRUSHIELD SECURITY MANAGEMENT SYSTEM MULTIPLE VULNERABILITIES

McAfee IntruShield Security Management System is susceptible to multiple vulnerabilities. The first two issues are cross-site scripting vulnerabilities in the 'intruvert/jsp/systemHealth/SystemEvent.jsp' script. These issues are due to a failure of the application to properly sanitize user-supplied data prior to utilizing it in dynamically generated HTML. The next two issues are authorization bypass vulnerabilities leading to information disclosure and the ability to acknowledge, de-acknowledge, and delete security alerts. These vulnerabilities require a valid user account in the affected application. \Users of affected packages should contact the vendor for further information.

Category 27.1 *Vulnerability assessment*

2005-07-07 **Vulnerability AIX FTP server ephemeral data ports IBM hosts protocol utilize memory sockets**

DHS IAIP Daily; http://www.kb.cert.org/vuls/id/118125

AIX FTP SERVER MAY NOT PROPERLY TIMEOUT EPHEMERAL DATA PORTS

IBM AIX includes an FTP server, ftpd, which allows files to be transferred between hosts with the FTP protocol. This server is vulnerable to a condition where an attacker may be able to utilize all available ephemeral ports on the system. When the ephemeral port range is exhausted, no more ports are available for the system to use for an indefinite period of time, resulting in a system-wide network-based denial of service. Additionally, the memory usage caused by the sockets in use by ftpd may also create a local denial of service condition by limiting system resources available to other processes. AIX 5.1, 5.2, and 5.3 are affected. A remote, authenticated user may be able to limit system and network resources and cause a denial-of-service condition. If anonymous FTP access is allowed, anonymous users are considered to be authenticated and may cause the same denial-of-service conditions. Users should contact IBM or their vendor for information on resolutions, workarounds, updates, and fixes.

Category 27.1 *Vulnerability assessment*

2005-07-07 **zlib buffer overflow vulnerability DoS data arbitrary code priveleges Linux**

DHS IAIP Daily; http://secunia.com/advisories/15949/

ZLIB "INFTREES.C" BUFFER OVERFLOW VULNERABILITY

A vulnerability has been reported in zlib, which can be exploited by malicious people to conduct a DoS (Denial of Service) against a vulnerable application, or potentially to execute arbitrary code. The vulnerability is caused due to a boundary error in "inftrees.c" when handling corrupted compressed data streams. This can be exploited to crash any application that uses the zlib library, or potentially to execute arbitrary code with privileges of the vulnerable application. The vulnerability has been reported in version 1.2.2. Prior versions may also be affected. No updates are currently available from the vendor, but several Linux distributions have issued updated packages.

Category 27.1 *Vulnerability assessment*

2005-07-08 **Secunia phpSecurePages vulnerability compromise system Input parameter external local resources**

DHS IAIP Daily; http://secunia.com/advisories/15994/

PHPSECUREPAGES "CFGPROGDIR" FILE INCLUSION VULNERABILITY

A vulnerability has been discovered in phpSecurePages which can be exploited by malicious people to compromise a vulnerable system. Input passed to the "cfgProgDir" parameter in "phpSecurePages/secure.php" isn't properly verified, before it is used to include files. This can be exploited to include arbitrary files from external and local resources. Successful exploitation requires that "register_globals" is enabled. The vulnerability has been confirmed in version 0.28 beta. Other versions may also be affected.

Category 27.1 *Vulnerability assessment*

2005-07-08 **PunBB SQL Injection PHP vulnerabilities system Input array template avatar**

DHS IAIP Daily; http://secunia.com/advisories/15990/

PUNBB SQL INJECTION AND PHP CODE EXECUTION VULNERABILITIES

Vulnerabilities have been discovered in PunBB which can be exploited by malicious people to conduct SQL injection attacks and compromise a vulnerable system. 1) Input passed to the "temp" array parameter in "profile.php" isn't properly sanitised before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code. Successful exploitation requires that "register_globals" is enabled. 2) An error in the template system can be exploited to include arbitrary local files via e.g. the "redirect_url" parameter. This can further be exploited to execute arbitrary PHP code by referencing a specially crafted avatar image containing PHP code. The vulnerabilities has been reported in version 1.2.5 and prior. Original Advisories: http://www.hardened-php.net/advisory-082005.php and http://www.hardened-php.net/advisory-092005.php

---

Category 27.1 *Vulnerability assessment*

2005-07-08 **Linux format flaw compression format Linux Unix hackers BSD bug zlib DoS library Danish Secunia vulnerability dire ranking**

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml?articleID=165701026

LINUX COMPRESSION FORMAT FLAW FOUND

A critical flaw in a compression format widely used in Linux and Unix can give hackers a way into machines, security experts said Friday, July 8. A patch for the zlib library isn't available, but several Linux and BSD distributors have rolled out fixes of their own. The bug, which affects the current version of zlib, 1.2.2, can be exploited to create a denial-of-service (DoS) attack, which could crash any application using the library or let the attacker plant code of his own remotely, according to an alert by Danish security firm Secunia. The company rated the zlib vulnerability as "Highly critical," its second-most dire ranking.

Category 27.1 *Vulnerability assessment*

2005-07-11 **MMS Ripper MMST streams overflow vulnerability arbitrary commands flaw IDs**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1043

MMS RIPPER (MMSRIP) MMST STREAMS HEAP OVERFLOW VULNERABILITY

A vulnerability was identified in MMS Ripper, which could be exploited by attackers to execute arbitrary commands. This flaw is due to a heap overflow error in the "mms_interp_header()" function when handling multiple stream IDs, which may be exploited via a malicious server to compromise a vulnerable system. Users should upgrade to MMS Ripper version 0.6.4 or later: http://nbenoit.tuxfamily.org/projects/mmsrip/

Category 27.1 *Vulnerability assessment*

2005-07-11 **ISC DHCPD format string vulnerability remote serverdata logged unsafe Exploitation debuging**

DHS IAIP Daily; http://www.securityfocus.com/bid/11591/info

ISC DHCPD REMOTE FORMAT STRING VULNERABILITY

A remote format string vulnerability is reported in the ISC DHCPD server package. User supplied data is logged in an unsafe fashion. Exploitation of this vulnerability may result in arbitrary code being executed by the DHCP server. Although unconfirmed it is conjectured that this issue may only be exploitable when debugging functionality is enabled. It is reported that the vendor has released an update to address this vulnerability. This update is reported to be located at: ftp://ftp.isc.org/isc/dhcp/dhcp-3.0.2rc1.tar.gz

---

Category 27.1 *Vulnerability assessment*

2005-07-11 **SPiD remote PHP inclusion vulnerability server input validation error parameter arbitrary privileges**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1041

SPID "LANG_PATH" REMOTE PHP FILE INCLUSION VULNERABILITY

A vulnerability was identified in SPiD, which may be exploited by attackers to compromise a vulnerable web server. This flaw is due to an input validation error in "lang.php" when processing a specially crafted "lang_path" parameter, which may be exploited by remote attackers to include malicious files and execute arbitrary commands with the privileges of the web server. The FrSIRT is not aware of any official supplied patch for this issue.

Category 27.1 *Vulnerability assessment*

2005-07-11 **phpWebSite PHP execution vulnerability malicious compromise CVS**

DHS IAIP Daily; http://secunia.com/advisories/16001/

PHPWEBSITE PEAR XML_RPC PHP CODE EXECUTION

A vulnerability has been reported in phpWebSite, which can be exploited by malicious people to compromise a vulnerable system. The vulnerability has reportedly been fixed in the CVS repository.

Category 27.1 *Vulnerability assessment*

2005-07-12 **Cisco CallManager memory software processing component IP media DoS attacks leaks corruption interrupter rebooting executed**

DHS IAIP Daily; http://www.cisco.com/warp/public/707/cisco−sa−20050712−ccm.s html

CISCO CALLMANAGER MEMORY HANDLING VULNERABILITIES

Cisco CallManager (CCM) is the software-based call-processing component of the Cisco IP telephony solution which extends enterprise telephony features and functions to packet telephony network devices such as IP phones, media processing devices, voice-over-IP (VoIP) gateways, and multimedia applications. Cisco CallManager 3.3 and earlier, 4.0, and 4.1 are vulnerable to Denial of Service (DoS) attacks, memory leaks, and memory corruption which may result in services being interrupted, servers rebooting, or arbitrary code being executed. Cisco has made free software available to address these vulnerabilities.

Category 27.1 *Vulnerability assessment*

2005-07-12 **Technical Cyber Security Alert Microsoft Windows Internet Explorer Word Vulnerabilities Office privileges system**

DHS IAIP Daily; http://www.us−cert.gov/cas/techalerts/TA05−193A.html

MICROSOFT WINDOWS, INTERNET EXPLORER, AND WORD VULNERABILITIES

Microsoft has released updates that address critical vulnerabilities in Windows, Office, and Internet Explorer. Exploitation of these vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary code with the privileges of the user. If the user is logged on with administrative privileges, the attacker could take control of an affected system. Microsoft has provided the updates for these vulnerabilities: http://www.microsoft.com/technet/security/bulletin/ms05-jul. mspx

---

Category 27.1 *Vulnerability assessment*

2005-07-13 **Yawp "_Yawp[conf_path]" PHP inclusion exploited attackers server validation error malicious**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1081

YAWP "_YAWP[CONF_PATH]" REMOTE PHP FILE INCLUSION VULNERABILITY

A vulnerability was identified in Yawp, which may be exploited by attackers to compromise a vulnerable web server. This flaw is due to an input validation error when processing a specially crafted "_Yawp[conf_path]" parameter, which may be exploited by remote attackers to include malicious files and execute arbitrary commands with the privileges of the web server. Yawp version 1.0.6 and prior are affected. Users should update to Yawp version 1.1.0 : http://phpyawp.com/yawiki/index.php?page=DownloadAndInstall

---

Category 27.1 *Vulnerability assessment*

2005-07-13 **WebEOC US-CERT crisis management application gather coordinate disseminate emergency operations URIs**

DHS IAIP Daily; http://www.kb.cert.org/vuls/

MULTIPLE VULNERABILITIES IN WEBEOC

The US-CERT has released serveral vulnerability notes to address issues in WebEOC is a web-based crisis information management application that provides functions to gather, coordinate, and disseminate information between emergency personnel and emergency operations centers (EOC). According to VU#258834, in numerous places in a WebEOC system, resources are requested via URIs. An attacker may be able exploit this design by crafting a URI that will directly access a resource, thus elevating that attacker's privileges. According to VU#491770, WebEOC uses weak algorithms to encrypt sensitive information. A remote attacker could recover or derive a private encryption keys, or apply simple cryptanalytic techniques to decipher an encrypted message. According to VU#138538, WebEOC contains multiple cross-site scripting 12 vulnerabilities. A remote attacker may be able to execute arbitrary script using a vulnerable WebEOC site. In addition, that attacker may be able to retrieve sensitive data from WebEOC site. According to VU#956762, WebEOC does not restrict the size of files that an authenticated user can upload into a back-end database. An authorized attacker may be able to consume a large amount of system resources. As system resources are exhausted, system operation may be disrupted resulting in a denial-of-service condition. According to VU#372797, a remote attacker may be able to execute SQL queries on a server, possibly with elevated privileges. As a result, attackers may be able to view or modify the contents of a WebEOC database. According to VU#165290, WebEOC insecurely stores sensitive information in easily accessible application components. Sensitive information may be easily accessible to untrusted parties.

Category 27.1 *Vulnerability assessment*

2005-07-13 **MIT Kerberos KDC US-CERT unauthenticated attacker code execution**

DHS IAIP Daily; http://www.kb.cert.org/vuls/

VULNERABILITIES IN MIT KERBEROS 5

Kerberos is a network authentication system which uses a trusted third party (a KDC) to authenticate clients and servers to each other. Several vulnerabilities have been reported. According to US-CERT Vulnerability Note VU#259798, an unauthenticated attacker can cause MIT krb5 Key Distribution Center (KDC) to overflow a heap buffer by one byte, possibly leading to arbitrary code execution. Patch details are available in MIT krb5 Security Advisory 2005-002. According to US-CERT Vulnerability Note VU#623332, an unauthenticated attacker can cause krb5_recvauth() function to free a block of memory twice, possibly leading to arbitrary code execution. Patch details are avilalbe in MIT krb5 Security Advisory 2005-003.

Category 27.1 *Vulnerability assessment*

2005-07-13 **Oracle Products Vulnerabilities Critical insecure consequences Apache Java Sun Microsystems**

DHS IAIP Daily; http://www.us−cert.gov/cas/techalerts/TA05−194A.html

ORACLE PRODUCTS CONTAIN MULTIPLE VULNERABILITIES

Oracle released a Critical Patch Update in July 2005 that addresses more than forty vulnerabilities in different Oracle products and components. The Critical Patch Update provides information about which components are affected, what access and authorization are required, and how data confidentiality, integrity, and availability may be impacted. Public reports describe vulnerabilities related to insecure password and temporary file handling and SQL injection. The impacts of these vulnerabilities vary depending on product or component and configuration. Potential consequences include remote execution of arbitrary code or commands, information disclosure, and denial of service. An attacker who compromises an Oracle database may be able to gain access to sensitive information. US-CERT strongly recommends that sites running Oracle review the Critical Patch Update, apply patches, and take other mitigating action as appropriate. Oracle HTTP Server is based on the Apache HTTP Server. Some Oracle products include Java components from Sun Microsystems. According to Oracle, the July 2005 Critical Patch Update addresses previously disclosed vulnerabilities in Apache and Java. Oracle also notes that Oracle Database Client-only installations are not affected by vulnerabilities listed in the July 2005 Critical Patch Update.

Category 27.1 *Vulnerability assessment*

2005-07-13 **Mozilla Suite Firefox Thunderbird vulnerabilities bypass**

DHS IAIP Daily; http://www.securityfocus.com/bid/14242/info

MOZILLA SUITE, FIREFOX AND THUNDERBIRD MULTIPLE VULNERABILITIES

The Mozilla Foundation has released 12 security advisories specifying security vulnerabilities in Mozilla Suite, Firefox, and Thunderbird. These vulnerabilities allow attackers to execute arbitrary machine code in the context of the vulnerable application, bypass security checks, execute script code in the context of targeted Websites to disclose confidential information; other attacks are also possible. These vulnerabilities have been addressed in Firefox version 1.0.5, Mozilla Suite 1.7.9. Mozilla Thunderbird has not been fixed at this time. The issues described here will be split into individual BIDs as further analysis is completed. This BID will then be retired.

Category 27.1 *Vulnerability assessment*

2005-07-14 **Seagull PHP Framework execution vulnerablility malicious 0.43**

DHS IAIP Daily; http://secunia.com/advisories/16074/

SEAGULL PHP FRAMEWORK PEAR XML_RPC PHP CODE EXECUTION

A vulnerability has been reported in Seagull PHP Framework, which can be exploited by malicious people to compromise a vulnerable system. The vulnerability has been reported in version 0.43. Prior versions may also be affected.

Category 27.1 *Vulnerability assessment*

2005-07-14 **Sophos Anti-Virus BZip2 vulnerability denial setting failure scans EM library**

DHS IAIP Daily; http://www.securityfocus.com/bid/14270/info

SOPHOS ANTI-VIRUS BZIP2 ARCHIVE HANDLING REMOTE DENIAL OF SERVICE VULNERABILITY

Sophos Anti-Virus is prone to a remote denial of service vulnerability when it is configured to 'Scan inside archive files'. This is not a default setting. The issue exists due to failure of the software to adequately sanitize 'Extra field length' values contained in BZip2 archives. Ultimately this vulnerability may be exploited to conduct a denial of proper service for legitimate users. Attackers may leverage this issue to prevent the software from completing file scans, for files received subsequent to an attack. This may allow the attacker to bypass Anti-Virus scans. The vendor has released updates to address this issue. These updates may be automatically applied by customers that are using the EM Library or manually from Sophos.

Category 27.1 *Vulnerability assessment*

2005-07-16 **Microsoft Security Advisory vulnerability Remote Desktop Services RDP**

DHS IAIP Daily;
http://www.microsoft.com/technet/security/advisory/904797.ms px

MICROSOFT SECURITY ADVISORY (904797): VULNERABILITY IN REMOTE DESKTOP PROTOCOL (RDP) COULD LEAD TO DENIAL OF SERVICE

Microsoft is investigating new public reports of a vulnerability in Remote Desktop Services. There are no reports of attacks that try to use the reported vulnerability or of customer impact at this time. The initial investigation has revealed that a denial of service vulnerability exists that could allow an attacker to send a specially crafted Remote Desktop Protocol (RDP) request to an affected system. The investigation has determined that this is limited to a denial of service, and therefore an attacker could not use this vulnerability to take complete control of a system. Services that utilize the Remote Desktop Protocol are not enabled by default, however if a service were enabled, an attacker could cause this system to restart.

Category 27.1 *Vulnerability assessment*

2005-07-18 **Xerox Vulnerabilities Microserver Web HTTP**

DHS IAIP Daily;
http://www.xerox.com/downloads/usa/en/c/cert_XRX05_007.pdf

VULNERABILITIES IN THE XEROX MICROSERVER WEB SERVER

There are multiple vulnerabilities in the web server code that could allow unauthorized access to the web server including vulnerabilities that could bypass authentication; specially constructed HTTP requests can cause denial of service or allow unauthorized file access on an attacked machine; and cross-site scripting allowing contents of web pages to be modified in an unauthorized manner. If successful, an attacker could make unauthorized changes to the system configuration. Customer and user passwords are not exposed. A patch is available. This patch is a cumulative patch that incorporates the security patches documented in Security Bulletins XRX04-002 (P4), XRX04-007 (P10), XRX04-009 (P17) and XRX05-005 (P21) for the products listed below.

Category 27.1 *Vulnerability assessment*

2005-07-18 **CERT VU#973635 SSH Tectia Server Windows hostkey Sexure Shell Servers DNS hijacking**

DHS IAIP Daily; http://www.kb.cert.org/vuls/id/973635

SSH COMMUNICATIONS SECURITY SSH TECTIA SERVER ON WINDOWS ALLOWS LOCAL ACCESS TO HOST IDENTIFICATION KEY

SSH Tectia Server for Microsoft Windows creates the hostkey with permissions that allow any user to read the file. As a result, any user logged into the system can read the private SSH hostkey. Previous versions of SSH Tectia Server were known as SSH Secure Shell for Windows Servers. The hostkey is used to authenticate the server to the client. This defends against redirection attacks, such as DNS hijacking that cause the client to connect to a malicious server. In such cases, clients that know the public hostkey can verify that the server has the private hostkey, thereby verifying the server is correct. If an attacker copies the private hostkey of a server, they can configure a server with the same private key as the legitimate server. Such a server would appear valid to clients if another attack, such as DNS hijacking, was used to trick the client into connecting to the attacker's server.

Category 27.1 *Vulnerability assessment*

2005-07-20 **FrSIRT arbitrary vulnerability Greasemonkey error malicious web page contents directories**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1147

GREASEMONKEY FIREFOX EXTENSION ARBITRARY FILE DISCLOSURE ISSUE

A vulnerability was identified in Greasemonkey, which could be exploited by remote attackers to read arbitrary files on a vulnerable system. This flaw is due to a design error when using insecure "GM_*" functions (i.e. GM_xmlhttpRequest, GM_getValue, or GM_getValue), which could be exploited via a malicious web page to read any file on a vulnerable system or list the contents of local directories. User should upgrade to Greasemonkey version 0.3.5 : https://addons.mozilla.org/extensions/moreinfo.php?applicati on=firefox&id=748

Category 27.1 *Vulnerability assessment*

2005-07-20 **ReviewPost PHP Pro SQL injection vulnerability malicious Input**

DHS IAIP Daily; http://secunia.com/advisories/16134/

REVIEWPOST PHP PRO "SORT" SQL INJECTION VULNERABILITY

A vulnerability has been reported in ReviewPost, which can be exploited by malicious people to conduct SQL injection attacks. Input passed to the "sort" parameter in "showproduct.php" isn't properly sanitised before being used in a SQL query. This can be exploited to manipulate SQL queries by injecting arbitrary SQL code.

Category 27.1 *Vulnerability assessment*

2005-07-21 **Tracker Mozilla Firefox vulnerability HTML target race violation crash exploit**

DHS IAIP Daily; http://securitytracker.com/alerts/2005/Jul/1014550.html

MOZILLA FIREFOX XPCOM RACE CONDITION LETS REMOTE USERS CRASH THE BROWSER

A vulnerability was reported in Mozilla Firefox in the cross platform component object model (xpcom) implementation. A remote user can cause a target user's browser to crash. 15 A remote user can create specially crafted HTML that, when loaded by the target user, will exploit a race condition in executing dom calls to delete objects in the page before they have been referenced. As a result, an access violation will occur and the target user's browser will crash. A demonstration exploit is available. No solution is currently known to be available.

Category 27.1 *Vulnerability assessment*

2005-07-25 **GoodTech SMTP Sever buffer commands flaw error smtpd command exploited compromise system**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1199

GOODTECH SMTP SERVER REMOTE BUFFER OVERFLOW VULNERABILITY

A vulnerability was identified in GoodTech SMTP Server, which could be exploited by remote attackers to execute arbitrary commands. This flaw is due to a buffer overflow error in smtpd when processing a specially crafted "RCPT TO" command, which could be exploited by attackers to compromise a vulnerable system. GoodTech SMTP Server for Windows NT/2000/XP/2003 version 5.16 and prior are affected. Users should upgrade to GoodTech SMTP Server version 5.17: http://www.goodtechsys.com/smtpdnt2000.asp

---

Category 27.1 *Vulnerability assessment*

2005-07-25 **FTPLocate vulnerability sanitization data commands executed context unauthorized hosting Web server**

DHS IAIP Daily; http://www.securityfocus.com/bid/14367/discuss

FTPLOCATE REMOTE COMMAND EXECUTION VULNERABILITY

FtpLocate is prone to a remote arbitrary command execution vulnerability. This issue presents itself due to insufficient sanitization of user-supplied data. An attacker can supply arbitrary commands and have them executed in the context of the server. This issue may facilitate unauthorized remote access to the computer running the hosting Web server. Currently Security Focus is not aware of any vendor-supplied patches for this issue.

Category 27.1 *Vulnerability assessment*

2005-07-25 **PHPFirstpost file vulnerability susceptible PHP code priveledges**

DHS IAIP Daily; http://www.securityfocus.com/bid/14371/info

PHPFIRSTPOST BLOCK.PHP REMOTE FILE INCLUDE VULNERABILITY

Phpfirstpost is susceptible to a remote PHP file include vulnerability. This issue is due to a failure in the application to properly sanitize user-supplied input. An attacker may exploit this issue to execute arbitrary PHP code on an affected computer with the privileges of the Web server process. This may facilitate unauthorized access. Currently Security Focus is not aware of any vendor-supplied patches for this issue.

Category 27.1 *Vulnerability assessment*

2005-07-25 **Clam AV heap Antivirus complete control SMTP SMB HTTP FTP bugs TNEF CHM FSG**

DHS IAIP Daily; http://www.rem0te.com/public/images/clamav.pdf

CLAMAV LIBRARY REMØTE HEAP OVERFLOWS SECURITY ADVISORY

ClamAV Antivirus Library is vulnerable to buffer overflows allowing attackers complete control of the system. These vulnerabilities can be exploited remotely without user interaction or authentication through common protocols such as SMTP, SMB, HTTP, FTP, etc. Specifically, ClamAV is responsible for parsing multiple file formats. At least four of its file format processors contain remote security bugs. Specifically, during the processing of TNEF, CHM, & FSG formats an attacker is able to trigger several integer overflows that allow attackers to overwrite heap data to obtain complete control of the system. These vulnerabilities can be reached by default and triggered without user interaction by sending an e-mail containing crafted data. Successful exploitation of ClamAV protected systems allows attackers unauthorized control of data and related privileges. ClamAV 0.86.1 (current) and prior are affected. Users should upgrade to Clam Antivirus (ClamAV) version 0.86.2 : http://sourceforge.net/project/showfiles.php?group_id=86638& release_id=344514

Category 27.1 *Vulnerability assessment*

2005-07-25 **Sun Microsystems vulnerability multilanguage Japanese unpriveleged priveleges application libmle Solaris**

DHS IAIP Daily; http://sunsolve.sun.com/search/document.do?assetkey=1−26−101 807−1

SECURITY VULNERABILITY IN THE MULTILANGUAGE ENVIRONMENT LIBRARY "LIBMLE" SHIPPED WITH THE JAPANESE LOCALE

A security vulnerability in the multilanguage environment library, "libmle" (shipped with the Japanese locale) may allow a local unprivileged user to be able to execute arbitrary code or commands with elevated privileges. The code or commands executed by the user would run with the privileges of the application dynamically linked to the libmle library. This issue is addressed in the following releases: Solaris 7 with patch 111646-01 or later and Solaris 8 with patch 111647-01 or later

---

Category 27.1 *Vulnerability assessment*

2005-07-26 **Atomic Photo Album vulnerability compromise server input error exploited malicious arbitrary FrSIRT**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1215

ATOMIC PHOTO ALBUM "APA_MODULE_BASEDIR" FILE INCLUSION VULNERABILITY

A vulnerability was identified in Atomic Photo Album, which may be exploited by attackers to compromise a vulnerable web server. This flaw is due to an input validation error in the "apa_phpinclude.inc.php" script when processing a specially crafted "apa_module_basedir" parameter, which may be exploited by remote attackers to include malicious files and execute arbitrary commands with the privileges of the web server. Atomic Photo Album version 1.0.5 and prior are affected. The FrSIRT is not aware of any official supplied patch for this issue.

Category 27.1 *Vulnerability assessment*

2005-07-26 **ProFTPD Shutdown Message vulnerability string server shutdown directory trigger**

DHS IAIP Daily; http://www.securityfocus.com/bid/14381/solution

PROFTPD SHUTDOWN MESSAGE FORMAT STRING VULNERABILITY

A format string vulnerability exists in ProFTPD. This issue is exposed when the server prints a shutdown message containing certain variables such as the current directory. If an attacker could create a directory on the server, it may be possible to trigger this issue. Successful exploitation will result in arbitrary code execution in the context of the server. This issue has been addressed in ProFTPD 1.3.0rc2: ftp://ftp.proftpd.org/distrib/source/proftpd-1.3.0rc2.tar.gz

---

Category 27.1 *Vulnerability assessment*

2005-07-26 **FrSIRT FtpLocate vulnerability arbitrary flaw input validation error filter pipe character**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1217

FTPLOCATE "FLSEARCH.PL" REMOTE COMMAND EXECUTION VULNERABILITY

A vulnerability was identified in FtpLocate, which may be exploited by remote attackers to execute arbitrary commands. This flaw is due to an input validation error in the "flsearch.pl" script that does not properly filter a specially crafted "fsite" parameter, which may be exploited by remote attackers to execute arbitrary commands via the pipe character. FtpLocate version 2.02 and prior are affected. The FrSIRT is not aware of any official supplied patch for this issue.

Category 27.1 *Vulnerability assessment*

2005-07-26 **Security Focus SPI Dynamics WebInspect application script injection vulnerability data content Internet Explorer COM installation execution**

DHS IAIP Daily; http://www.securityfocus.com/bid/14385/info

SPI DYNAMICS WEBINSPECT CROSS APPLICATION SCRIPT INJECTION VULNERABILITY

WebInspect is vulnerable to a cross-application script injection vulnerability. This issue is due to a failure of the application to properly sanitize user-supplied data prior to including it in content rendered in an Internet Explorer COM object. This vulnerability allows attackers to execute arbitrary script code in the context of the vulnerable application. By exploiting the knowledge of predictable files on the targeted system, attackers may also cause arbitrary script code to be executed in the "Local Machine" zone, facilitating remote machine code installation and execution. Security Focus is not currently aware of any vendor-supplied patches for this issue.

Category 27.1 *Vulnerability assessment*

2005-07-26 **IBM Lotus Domino WebMail vulnerability affected disclosure attacks crack account**

DHS IAIP Daily; http://www.securityfocus.com/bid/14388/discuss

IBM LOTUS DOMINO WEBMAIL INFORMATION DISCLOSURE VULNERABILITY

IBM Lotus Domino WebMail is affected by an information disclosure vulnerability. An attacker can disclose a user's password hash. They may subsequently carry out brute force attacks to crack the password and gain access to the user's account. Security Focus is not currently aware of any vendor-supplied patches for this issue.

Category 27.1 *Vulnerability assessment*

2005-07-26 **Security Tracker Apache buffer overflow vulnerability processing CRLs child printing LogLevel**

DHS IAIP Daily; http://www.securitytracker.com/alerts/2005/Jul/1014575.html

APACHE MOD_SSL OFF-BY-ONE BUFFER OVERFLOW IN PROCESSING CRLS MAY LET REMOTE USERS DENY SERVICE

A vulnerability was reported in Apache mod_ssl in the processing of certificate revocation lists (CRLs). A remote user may be able to cause denial of service conditions. A remote user can create a specially crafted CRL that, when processed by the Apache mod_ssl callback function, will trigger an off-by-one buffer overflow. A remote user can cause the Apache server child process to crash. The vulnerability can be triggered when printing CRL information at the 'debug' LogLevel. The vendor has issued a source code fix, available via SVN.

Category 27.1 *Vulnerability assessment*

2005-07-26 **IBM Access Connections Shared Section permissions vulnerability insecure memory attackers**

DHS IAIP Daily; http://www.securityfocus.com/bid/14387/info

IBM ACCESS CONNECTIONS SHARED SECTION INSECURE PERMISSIONS VULNERABILITY

IBM Access Connections utilizes Shared Sections in an insecure manner.
It creates a Shared Section memory region with insecure permissions allowing local attackers to gain inappropriate access to it. Attackers may read the data stored in the memory region, gaining access to potentially sensitive information. They may also write arbitrary data to the shared memory segment, potentially crashing the processes using the segment and denying service to legitimate users. Security Focus is not currently aware of any vendor-supplied patches for this issue.

Category 27.1 *Vulnerability assessment*

2005-07-26 **FTPShell denial vulnerability prone service failure problem opens closes terminate exploit**

DHS IAIP Daily; http://www.securityfocus.com/bid/14382/info

FTPSHELL SERVER DENIAL OF SERVICE VULNERABILITY

FTPshell server is prone to a denial of service vulnerability. This issue is due to a failure in the application to handle exceptional conditions. The problem presents itself when an attacker opens and closes, without using the 'quit' command, a connection to the application multiple times. This will cause the application to terminate. An attacker can exploit this vulnerability to deny service to legitimate users. Security Focus is not currently aware of any vendor-supplied patches for this issue.

Category 27.1 *Vulnerability assessment*

2005-07-27 **eMule Kad Packets Zlib vulnerabilities buffer overflow error library streams**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1238

EMULE KAD PACKETS REMOTE DENIAL OF SERVICE AND ZLIB VULNERABILITIES

Multiple vulnerabilities were identified in eMule, which could be exploited by remote attackers to cause a denial of service or execute arbitrary commands. The first issue is due to a buffer overflow error in the Zlib library when decompressing specially crafted data streams, which could be exploited, via a malformed stream embedded within network communication, to execute arbitrary commands. The second vulnerability is due to an unspecified error when processing malformed Kad packets, which could be exploited by remote attackers to cause a denial of service. eMule version 0.46b and prior are affected. Users should upgrade to eMule version 0.46c

---

Category 27.1 *Vulnerability assessment*

2005-07-27 **VBZooM injection vulnerability SQL input validation error**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1234

VBZOOM "SUBJECTID" PARAMETER REMOTE SQL INJECTION VULNERABILITY

A vulnerability was identified in VBZooM, which may be exploited by remote attackers to execute arbitrary SQL commands. This flaw is due to an input validation error in the "show.php" script when processing a specially crafted "SubjectID" parameter, which may be exploited by remote users to conduct SQL injection attacks. VBZooM version 1.11 and prior are affected. The FrSIRT is not aware of any official supplied patch for this issue.

Category 27.1 *Vulnerability assessment*

2005-07-27 **FrSIRT Cisco IOS vulnerability flaw overflow errorattacker arbitrary code device firmware**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1248

CISCO IOS UNSPECIFIED REMOTE HEAP OVERFLOW VULNERABILITY

A vulnerability was identified in Cisco Internet Operating System (IOS), which could be exploited by remote attackers to execute arbitrary commands. This flaw is due to a heap overflow error when processing specially crafted packets, which could be exploited by an unauthenticated attacker to execute arbitrary code and compromise a vulnerable device. Cisco IOS version 12.x and 11.x l are affected. It is reported that the vendor has addressed this vulnerability in an April firmware release.

Category 27.1 *Vulnerability assessment*

2005-07-27 **FrSIRT Sophos Antivirus vulnerability malware overflow malformed e-mail**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/

SOPHOS ANTIVIRUS PRODUCTS REMOTE HEAP OVERFLOW VULNERABILITY

A critical vulnerability was identified in multiple Sophos AntiVirus products, which may be exploited by remote attackers or malware to execute arbitrary code. This flaw is due to a heap 9 overflow error when analyzing malformed files, which may be exploited by an unauthenticated remote attacker to execute arbitrary commands by sending an e-mail containing a specially crafted attachment to a vulnerable system. No further details have been disclosed. The following products are affected: Sophos Anti-Virus versions prior to 3.96.0 (on Windows, Unix, NetWare, OS/2, OpenVMS); Sophos Anti-Virus versions prior to 4.5.4 (on all platforms); and Sophos Anti-Virus Small Business Edition Sophos Anti-Virus Small Business Edition will be updated by July 29. Users should upgrade to Sophos Anti-Virus version 3.96.0 or 4.5.4: http://www.sophos.com/support/updates

---

Category 27.1 *Vulnerability assessment*

2005-07-27 **Security Focus Novell GroupWise Client buffer vulnerability post office malicious**

DHS IAIP Daily; http://www.securityfocus.com/bid/14398/discuss

NOVELL GROUPWISE CLIENT REMOTE BUFFER OVERFLOW VULNERABILITY

Novell GroupWise Client is affected by a remote buffer overflow vulnerability. Specifically, this vulnerability arises when a user attempts to log in to a GroupWise post office that contains a malicious 'GWVW02??.INI' file. This can facilitate unauthorized access in the context of the user. This issue affects all versions of Novell GroupWise 6.5 client dated prior to July 15, 2005. Novell has released Technical Information Documents TID10098314 and TID2971927 including GroupWise 6.5 SP5 Client rev 6 to address this issue.

Category 27.1 *Vulnerability assessment*

2005-07-27 **FrSIRT Ethereal Multiple Protocol Dissector Zlib vulnerabilities buffer error string null LDAP AgentX PER DHCP BER MEGACO GIOP SMB WBXML H1 DOCSIS SMPP HTTP DCERPC CAMEL RADIUS Telnet NCP**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1237

ETHEREAL MULTIPLE PROTOCOL DISSECTOR AND ZLIB VULNERABILITIES

Multiple vulnerabilities were identified in Ethereal, which could be exploited by remote attackers to cause a denial of service or execute arbitrary commands. The first issue is due to a buffer overflow error in the Zlib library when decompressing specially crafted data streams, which could be exploited, via a malformed stream embedded within network communication, to execute arbitrary commands. Various buffer overflow, format string, and null pointer vulnerabilities were identified in the LDAP, AgentX, 802.3, PER, DHCP, BER, MEGACO, GIOP, SMB, WBXML, H1, DOCSIS, SMPP, HTTP, DCERPC, CAMEL, RADIUS, Telnet, IS-IS LSP and NCP dissectors, which could be exploited by attackers to compromise a vulnerable system or cause the application to crash. Ethereal versions 0.8.5 through 0.10.11 are affected. Users should upgrade to Ethereal version 0.10.12: http://www.ethereal.com/download.html

---

Category 27.1 *Vulnerability assessment*

2005-07-27 **Mozilla Suite Firefox script vulnerabilities security JavaScript protocol URIs code installation execution malicious**

DHS IAIP Daily; http://www.securityfocus.com/bid/13641/info

MOZILLA SUITE AND FIREFOX MULTIPLE SCRIPT MANAGER SECURITY BYPASS VULNERABILITIES

Multiple issues exist in Mozilla Suite and Firefox. These issues allow attackers to bypass security checks in the script security manager. Security checks in the script security manager are designed to prevent script injection vulnerabilities. An attacker sending certain undisclosed JavaScript in 'view-source:', and 'jar:' pseudo protocol URIs, may bypass these security checks. These vulnerabilities allow remote attackers to execute script code with elevated privileges, leading to the installation and execution of malicious applications on an affected computer. Cross-site scripting, and other attacks are also likely possible. The vendor has released an advisory, as well as upgraded versions of Mozilla Suite, and Mozilla Firefox to resolve these issues.

Category 27.1 *Vulnerability assessment*

2005-09-28 **FrSIRT IBM AIX buffer vulnerability priveleges parameters**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/1877

IBM AIX "GETCONF" COMMAND LOCAL BUFFER OVERFLOW VULNERABILITY

A vulnerability has been identified in IBM AIX. This can be exploited by local attackers to obtain elevated privileges. This issue is due to an unspecified error in the "getconf" command that does not properly handle specially crafted parameters,. This vulnerability could be exploited by malicious users to execute arbitrary commands with "root" privileges.

Category 27.1 *Vulnerability assessment*

2005-10-07 **IBM HTTP Server PCRE byte vulnerabilities DoS**

DHS IAIP Daily; http://secunia.com/advisories/17036/

IBM HTTP SERVER PCRE AND BYTE-RANGE FILTER VULNERABILITIES

IBM has acknowledged two vulnerabilities in IBM HTTP Server. These vulnerabilities can be exploited by malicious people to cause a DoS (Denial of Service), or by malicious, local users to gain escalated privileges via a specially crafted ".htaccess" file.

Category 27.1 *Vulnerability assessment*

2005-10-10 **imapproxy string vulnerability flaw format server compromise IMAP**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/2014

IMAPPROXY "PARSEBANNERANDCAPABILITY" FORMAT STRING VULNERABILITY

A vulnerability has been identified in imapproxy, which could be exploited by remote attackers to execute arbitrary commands. This flaw is due to a format string error in the "ParseBannerAndCapability()" [main.c] function that does not properly handle a specially crafted banner/capability line received from the server, which could be exploited by remote attackers to compromise a vulnerable system by convincing a user to connect to a specially crafted IMAP server. The FrSIRT is not aware of any official supplied patch for this issue.

Category 27.1 *Vulnerability assessment*

2005-10-10 **Linux Kernel vulnerabilities trigger denial of service memory**

DHS IAIP Daily; http://www.securityfocus.com/bid/15049/references

LINUX KERNEL MULTIPLE SECURITY VULNERABILITIES

Linux kernel is prone to multiple vulnerabilities. These issues may allow local and remote attackers to trigger denial of service conditions or disclose sensitive kernel memory. Linux kernel 2.6.x versions are known to be vulnerable at the moment. Other versions may be affected as well. Various patches are available to address these issues:
http://www.securityfocus.com/bid/15049/references

Category 27.1 *Vulnerability assessment*

2005-10-10 **Kaspersky Engine CHM parser buffer overflow vulnerability context**

DHS IAIP Daily; http://www.securityfocus.com/bid/15054/info

KASPERSKY ANTI-VIRUS ENGINE CHM FILE PARSER REMOTE BUFFER OVERFLOW VULNERABILITY

Kaspersky Anti-Virus Engine is prone to a remote buffer overflow vulnerability. This issue presents itself when an attacker sends a maliciously crafted CHM file to an affected computer and this file is processed by Kaspersky's CHM file parser. This vulnerability allows attackers to execute arbitrary machine code in the context of the affected application. Attackers may gain privileged remote access to computers running the affected application. The vendor has released a signature update to address this issue. Users with updated signatures released after July 2005 are not vulnerable.

Category 27.1 *Vulnerability assessment*

2005-10-10 **Computer Associates iGateway buffer vulnerability flaw buffer overflow error HTTP GET debug**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/2028

COMPUTER ASSOCIATES IGATEWAY REMOTE BUFFER OVERFLOW VULNERABILITY

A vulnerability has been identified in various Computer Associates products, which could be exploited by remote attackers to execute arbitrary commands. This flaw is due to a buffer overflow error in the iGateway component that does not properly handle specially crafted HTTP GET requests (port 5250) when debug mode is enabled, which could be exploited by remote attackers to execute arbitrary commands and compromise a vulnerable system. No solution is currently available.

Category 27.1 *Vulnerability assessment*

2005-10-10 **PHPMyAdmin vulnerability script code Web access**

DHS IAIP Daily; http://www.securityfocus.com/bid/15053/info

PHPMYADMIN LOCAL FILE INCLUDE VULNERABILITY

phpMyAdmin is prone to a local file include vulnerability. An attacker may leverage this issue to execute arbitrary server-side script code that resides on an affected computer with the privileges of the Web server process. This may potentially facilitate unauthorized access. phpMyAdmin 2.6.4-pl1 is reported to be vulnerable. Other versions may be affected as well. There are no vendor-supplied patches currently available for this issue.

Category 27.1 *Vulnerability assessment*

2005-10-10 **Shorewall MACLIST vulnerability Netfilter Firewall Client version**

DHS IAIP Daily; http://www.securiteam.com/unixfocus/6F00C00EAM.html

SHOREWALL MACLIST SECURITY VULNERABILITY

The Shoreline Firewall, "more commonly known as 'Shorewall', is a high-level tool for configuring Netfilter. You describe your firewall/gateway requirements using entries in a set of configuration files". A problem has been reported in the Shorewall Firewall that enables a Client accepted by MAC-Filter to bypass any other rule. This Issue doesn't apply to any Shorewall Version before 2.2.0. Users of any version before 2.2.5 are encouraged to update to a newer version (at least 2.2.5, better 2.4.1) of Shorewall. Shorewall Version 2.0.x is still supported, but Users of 2.0.x are encouraged to upgrade to a newer version.

Category 27.1 *Vulnerability assessment*

2005-10-11 **SGI IRIX design vulnerability runpriv Silicon Graphics Inc binary directory**

DHS IAIP Daily;
http://www.idefense.com/application/poi/display?id=312&type=
vulnerabilities&flashstatus=true

SGI IRIX RUNPRIV DESIGN ERROR VULNERABILITY

Local exploitation of a design error vulnerability in the runpriv command included in multiple versions of Silicon Graphics Inc.'s IRIX could allow for arbitrary code execution as the root user. Exploitation requires an attacker to have access to an account which has been granted usage of a binary in the /usr/sysadm/privbin directory. As root must explicitly allow such privileges, the impact of this vulnerability is lessened significantly. Exploitation does not require any knowledge of application internals, making exploitation trivial, even for unskilled attackers. Vendor patch 7004 for IRIX 6.5.27 and 6.5.28 is available at: http://support.sgi.com/

Category 27.1 *Vulnerability assessment*

2005-10-11 **Linux Kernel memory denial of service vulnerabilities crash**

DHS IAIP Daily; http://www.securityfocus.com/bid/15076/solution

LINUX KERNEL MULTIPLE MEMORY LEAK LOCAL DENIAL OF SERVICE VULNERABILITIES

Two local denial of service vulnerabilities affects the Linux kernel. These issues are due to a design flaw that creates memory leaks. These vulnerabilities may be exploited by local users to consume excessive kernel resources, likely triggering a kernel crash, denying service to legitimate users. These issues affect Linux kernel versions prior to 2.6.14-rc4. The vendor has released version 2.6.14-rc4 to address these issues.

Category 27.1 *Vulnerability assessment*

2005-10-11 **Alert Microsoft Windows Internet Explorer Exchange Server vulnerabilities denial of service control**

DHS IAIP Daily; http://www.us−cert.gov/cas/alerts/SA05−284A.html

MICROSOFT WINDOWS, INTERNET EXPLORER, AND EXCHANGE SERVER VULNERABILITIES

Microsoft has released updates that address critical vulnerabilities in Windows, Internet Explorer, and Exchange Server. Exploitation of these vulnerabilities could allow a remote, unauthenticated attacker to execute arbitrary code or cause a denial of service on an affected system. Exploitation of these vulnerabilities may allow a remote, unauthenticated attacker to execute arbitrary code with SYSTEM privileges or with the privileges of the user. If the user is logged on with administrative privileges, the attacker could take complete control of an affected system. An attacker may also be able to cause a denial of service. Updates are available on the Microsoft Update site: http://www.microsoft.com/technet/security/bulletin/ms05-oct. mspx

---

Category 27.1 *Vulnerability assessment*

2005-10-11 **WinRAR string overflow vulnerabilities Two compromise system diagnostic error filename encoded**

DHS IAIP Daily; http://secunia.com/secunia_research/2005−53/advisory/

WINRAR FORMAT STRING AND BUFFER OVERFLOW VULNERABILITIES

Two vulnerabilities in WinRAR can be exploited by malicious people to compromise a user's system. 1) A format string error exists when displaying a diagnostic error message that informs the user of an invalid filename in an UUE/XXE encoded file. This can be exploited to execute arbitrary code when a malicious UUE/XXE file is decoded. 2) A boundary error in UNACEV2.DLL can be exploited to cause a stack-based buffer overflow. This allows arbitrary code execution when a malicious ACE archive containing a file with an overly long file name is extracted. Users should update to version 3.51.

Category 27.1 *Vulnerability assessment*

2005-10-12 **VERITAS NetBackup string vulnerability Java command**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/2072

VERITAS NETBACKUP BPJAVA-MSVC REMOTE FORMAT STRING VULNERABILITY

A vulnerability has been identified in VERITAS NetBackup servers and clients. This could be exploited by remote attackers to execute arbitrary commands. The vulnerability is due to a format string error in the Java authentication service "bpjava-msvc" that does not properly handle a specially crafted "COMMAND_LOGON_TO_MSERVER" command (port 13722), which could be exploited by remote attacker.

Category 27.1 *Vulnerability assessment*

2005-10-12 **Microsoft Windows FTP transversal vulnerability input corruption malicious**

DHS IAIP Daily; http://www.securityfocus.com/bid/12160/solution

MICROSOFT WINDOWS FTP CLIENT DIRECTORY TRAVERSAL VULNERABILITY

Microsoft Windows FTP client is prone to a directory traversal vulnerability. This issue is due to a failure of the application to properly sanitize user supplied input. This vulnerability may cause a remote attacker to place files in an arbitrary location on a vulnerable computer. This can lead to data corruption or creation of potentially malicious files on a vulnerable computer.

Category 27.1 *Vulnerability assessment*

2005-10-13 **Cisco IOS firewall proxy buffer overflow vulnerability exploitation denial of service arbitrary code security FTP Telnet protocols**

DHS IAIP Daily; http://www.securityfocus.com/bid/14770/references

CISCO IOS FIREWALL AUTHENTICATION PROXY BUFFER OVERFLOW VULNERABILITY

Cisco IOS Firewall Authentication Proxy is prone to a buffer overflow condition. Successful exploitation of this issue could cause a denial of service or potential execution of arbitrary code. This feature allows network administrators to apply specific security policies on a per user basis. This issue affects the FTP and Telnet protocols, but not HTTP.

Category 27.1 *Vulnerability assessment*

2005-10-13 **Symantec Brightmail Antispam MIME denial of service vulnerability**

DHS IAIP Daily; http://www.securityfocus.com/bid/15087/references

SYMANTEC BRIGHTMAIL ANTISPAM MALFORMED MIME MESSAGE DENIAL OF SERVICE VULNERABILITY

Symantec Brightmail AntiSpam is susceptible to a denial of service vulnerability. This may cause a potential denial of service issue that has been identified and fixed in the Symantec Brightmail AntiSpam product.

Category 27.1 *Vulnerability assessment*

2005-10-14 **Computer Associates iGateway debug HTTP GET buffer vulnerability component CA UNIX Linux Windows**

DHS IAIP Daily; http://www.securityfocus.com/archive/1/413408

COMPUTER ASSOCIATES IGATEWAY DEBUG MODE HTTP GET REQUEST BUFFER OVERFLOW VULNERABILITY

The Computer Associates iGateway common component, which is included with several CA products for UNIX/Linux/Windows platforms, contains a buffer overflow vulnerability. This could allow remote attackers to execute arbitrary code on Windows platforms, or cause iGateway denial of service on UNIX and Linux. The vulnerability is due to improper bounds checking on HTTP GET requests by the iGateway component when debug mode is enabled.

Category 27.1 *Vulnerability assessment*

2005-10-17 **Security Focus Sun Solaris Proc Filesystem denial of service vulnerability**

DHS IAIP Daily; http://www.securityfocus.com/bid/15115/info

SUN SOLARIS PROC FILESYSTEM LOCAL DENIAL OF SERVICE VULNERABILITY 10-16

Sun Solaris is prone to a local denial of service vulnerability. This can be susceptible to a system panic in the '/proc' filesystem and cause a denial of service. The system will panic with a message similar to the following: BAD TRAP: type=e (#pf Page fault) rp=d48dce48 addr=24 occurred in module "procfs" due to a NULL pointer dereference.

Category 27.1 *Vulnerability assessment*

2005-10-17 **Lynx NNTP buffer overflow vulnerability headers URIs Exploitation execution**

DHS IAIP Daily; http://www.securityfocus.com/bid/15117/references

LYNX NNTP ARTICLE HEADER BUFFER OVERFLOW VULNERABILITY

Lynx is prone to a buffer overflow when handling NNTP article headers. This issue may be exploited when the browser handles NNTP content, such as through 'news:' or 'nntp:' URIs. Exploitation may result in code execution in the context of the program user.

Category 27.1 *Vulnerability assessment*

2005-10-18 **Technical Cyber Security Alert Snort Back Orifice buffer overflow modular ping UDP root SYSTEM**

DHS IAIP Daily; http://www.us−cert.gov/cas/techalerts/TA05−291A.html

SNORT BACK ORIFICE PREPROCESSOR BUFFER OVERFLOW

Snort preprocessors are modular plugins that extend functionality by operating on packets before the detection engine is run. The Back Orifice preprocessor decodes packets to determine if they contain Back Orifice ping messages. The ping detection code does not adequately limit the amount of data that is read from the packet into a fixed-length buffer, thus creating the potential for a buffer overflow. The vulnerable code will process any UDP packet that is not destined to or sourced from the default Back Orifice port (31337/udp). An attacker could exploit this vulnerability by sending a specially crafted UDP packet to a host or network monitored by Snort. A remote attacker who can send UDP packets to a Snort sensor may be able to execute arbitrary code. Snort typically runs with root or SYSTEM privileges, so an attacker could take complete control of a vulnerable system. An attacker does not need to target a Snort sensor directly; the attacker can target any host or network monitored by Snort. Sourcefire has released Snort 2.4.3: http://www.snort.org/dl/ Additional information is available in US-CERT Vulnerability Note VU#175500: http://www.kb.cert.org/vuls/id/177500

Category 27.1 *Vulnerability assessment*

2005-10-18 **Oracle October security vulnerabilities Database Server Enterprise Manager Application Server Collaboration Suite E Business Suite and Applications Peoplesoft Enterprise JD Edwards EnterpriseOne**

DHS IAIP Daily; http://www.securityfocus.com/bid/15134/info

ORACLE OCTOBER SECURITY UPDATE MULTIPLE VULNERABILITIES

Various Oracle Database Server, Oracle Enterprise Manager, Oracle Application Server, Oracle Collaboration Suite, Oracle E-Business Suite and Applications, and Oracle PeopleSoft Enterprise and JD Edwards EnterpriseOne are affected by multiple vulnerabilities. The issues identified by the vendor affect security properties of the Oracle products and present local and remote threats. Oracle has released a Critical Patch Update advisory for October 2005 to address these vulnerabilities. This Critical Patch Update addresses the vulnerabilities for supported releases. Oracle Critical Patch update: http://www.oracle.com/technology/deploy/security/pdf/cpuoct2 005.html

---

Category 27.1 *Vulnerability assessment*

2005-10-19 **Technical Cyber Security Alert Oracle vulnerabilities Critical Patch Update products components configuration commands information disclosure denial of service**

DHS IAIP Daily; http://www.us−cert.gov/cas/techalerts/TA05−292A.html

ORACLE PRODUCTS CONTAIN MULTIPLE VULNERABILITIES

Oracle has released a Critical Patch Update that addresses more than eighty vulnerabilities in different Oracle products and components. The impact of these vulnerabilities varies depending on the product, component, and configuration of the system. Potential consequences include remote execution of arbitrary code or commands, information disclosure, and denial of service. An attacker who compromises an Oracle database may be able to gain access to sensitive information. US-CERT recommends that sites running Oracle review the Critical Patch Update, apply patches, and take other mitigating action as appropriate. Critical Patch Update: http://www.oracle.com/technology/deploy/security/pdf/cpuoct2 005.html

---

Category 27.1 *Vulnerability assessment*

2005-10-19 **Avaya CMS IR Solaris Xsun Xprt privilege arbitrary command**

DHS IAIP Daily; http://secunia.com/advisories/17246/

AVAYA CMS / IR SOLARIS XSUN AND XPRT PRIVILEGE ESCALATION VULNERABILITY

A vulnerability has been found in CMS and IR. This can be exploited by malicious, local users to gain escalated privileges. This vulnerability may allow a local unprivileged user the ability to execute arbitrary code with the privileges of either the Xsun(1) or Xprt(1) command.

Category 27.1 *Vulnerability assessment*

2005-10-20 **HP OpemView operations VantagePoint JRE vulnerability arbitrary commands error Web**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/2150

HP OPENVIEW OPERATIONS AND OPENVIEW VANTAGEPOINT JRE VULNERABILITY

A vulnerability has been identified in HP OpenView Operations and OpenView VantagePoint. This could be exploited by remote attackers to execute arbitrary commands. This flaw is due to an error in Java Runtime Environment (JRE) and may be exploited via a malicious Web page to read and/write arbitrary files on a vulnerable system and execute local applications with the privileges of the user running the untrusted applet.

Category 27.1 *Vulnerability assessment*

2005-10-21 **Microsoft patch problem DirectShow media software DirectX**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/holes/s tory/0,10801,105646,00.html

MICROSOFT REPORTS SECOND PATCH PROBLEM; WINDOWS 2000 USERS MAY BE UNPROTECTED

A critical patch – Security Update MS05-050 – released by Microsoft on October 11 as part of the company's monthly security software fixes related to Microsoft's DirectShow streaming media software may have left users vulnerable. Microsoft DirectX 8.0 or 9.0 users who may have accidentally installed the patch written for DirectX 7.0 will still be vulnerable to the underlying vulnerability. The patch is supposed to address a problem in DirectShow that could allow an attacker to seize control of an unpatched system. According to Microsoft, customers who received Update MS05-050 automatically or who correctly followed the steps in Microsoft's security bulletin won't be affected. Another patch released on October 11 – MS05-051 – gave users difficulties as well. Microsoft Security Bulletin: http://www.microsoft.com/technet/security/bulletin/ms05-oct. mspx

---

Category 27.1 *Vulnerability assessment*

2005-10-22 **RSA buffer overflow vulnerability boundary error**

DHS IAIP Daily; http://secunia.com/advisories/17281/

RSA AUTHENTICATION AGENT FOR WEB "REDIRECT" BUFFER OVERFLOW VULNERABILITY

A vulnerability in RSA Authentication Agent for Web for Internet Information Services has been detected. The vulnerability is caused due to a boundary error in IISWebAgentIF.dll. This can be exploited to cause a stack-based buffer overflow via a GET request with an overly long "url" parameter in the "Redirect" method. The vulnerability has been reported in version 5.2 and 5.3. Other versions may also be affected. According to Secunia, the vendor may have a patch available.

Category 27.1 *Vulnerability assessment*

2005-10-22 **Sophos visio processing overflow vulnerability bounds checking integrity OSVDB**

DHS IAIP Daily; http://www.osvdb.org/displayvuln.php?osvdb_id=18464

SOPHOS ANTI-VIRUS VISIO FILE PROCESSING OVERFLOW VULNERABILITY

A remote overflow exists in Sophos anti-virus in which the anti-virus engine fails to perform proper bounds checking, which results in a heap-based buffer overflow. With a specially crafted visio file, a remote attacker can cause arbitrary code execution resulting in a loss of integrity. According to OSVDB, the vendor should be contacted for an appropriate upgrade. An upgrade is required as there are no known workarounds. Vendor Specific Advisory URL: http://www.sophos.com/support/knowledgebase/article/3409.htm l

---

Category 27.1 *Vulnerability assessment*

2005-10-22 **RSA Web redirect overflow vulnerability IIS validate parameter GET ISAPI termination restart**

DHS IAIP Daily; http://www.osvdb.org/displayvuln.php?osvdb_id=20151

RSA AUTHENTICATION AGENT FOR WEB IISWEBAGENTIF.DLL REDIRECT OVERFLOW VULNERABILITY

A remote overflow exists in RSA authentication agent for Web for IIS. IISWebAgentIF.dll fails to validate the length of the "url" parameter in the "Redirect" method, resulting in a stack-based buffer overflow. With a specially crafted GET request, an attacker can cause arbitrary code execution resulting in a loss of integrity. RSA Authentication Agent for Web for IIS is an ISAPI filter which runs in-process with inetinfo.exe. Any attempt to exploit this flaw will result in the termination and potential restart of the IIS service. Currently, there are no known workarounds or upgrades to correct this issue. However, RSA Security has reportedly released a patch to address this vulnerability. RSA Security: http://rsasecurity.com/

Category 27.1 *Vulnerability assessment*

2005-10-22 **CA iGateway debug HTTP GET request overflow vulnerability checking buffer**

DHS IAIP Daily; http://www.osvdb.org/displayvuln.php?osvdb_id=19920

CA IGATEWAY DEBUG MODE HTTP GET REQUEST OVERFLOW VULNERABILITY

A remote overflow exists in Computer Associates iGateway. The application fails to perform proper bounds checking resulting in a buffer overflow. With a specially crafted HTTP GET request, a remote attacker can cause arbitrary code execution with SYSTEM privileges resulting in a loss of integrity. This flaw is only exploitable if a non-standard installation has been performed and when the iGateway component has been explicitly configured to run with diagnostic debug tracing enabled. The vulnerability can be fixed with an upgrade to version 4.0.050623 or higher, as recommended by Computer Associates. An upgrade is required as there are no known workarounds. Vendor Specific Advisory URL: http://www3.ca.com/securityadvisor/vulninfo/vuln.aspx?id=334 85

Category 27.1 *Vulnerability assessment*

2005-10-24 **Oracle patches NGSS bugs October buffer**

DHS IAIP Daily;
http://www.techworld.com/news/index.cfm?newsID=4644&printerf riendly=1

ORACLE'S RECENT SECURITY PATCHES MAY LEAVE SERIOUS PROBLEMS UNFIXED

According to Mark Litchfield of Next Generation Security Software (NGSS), who discovered eighteen of the 88 bugs fixed in last week's update from Oracle, the patch could allow attackers to continue taking advantage of some of the bugs. Litchfield says "Having downloaded and given the Oracle October patch a cursory examination, some of the flaws …remain exploitable… the patch is not sufficient." The bugs discovered by NGSS include a buffer overflow vulnerability and 17 PL/SQL injection flaws. Few details have yet been released publicly about most of the flaws. Oracle Critical Patch Update http://www.oracle.com/technology/deploy/security/pdf/cpuoct2 005.html

---

Category 27.1 *Vulnerability assessment*

2005-10-25 **vendor anit-virus evasion vulnerability malicious software security**

DHS IAIP Daily; http://www.securityfocus.com/bid/15189/info

MULTIPLE VENDOR ANTI-VIRUS MAGIC BYTE DETECTION EVASION VULNERABILITY

Multiple vendor anti-virus software is prone to a detection evasion vulnerability. The problem presents itself in the way various anti-virus software determines the type of file it is scanning. An attacker can exploit this vulnerability to pass malicious files past the anti-virus software. This results in a false sense of security, and ultimately could lead to the execution of arbitrary code on the user's machine. SecurityFocus is not aware of any vendor-supplied patches for this issue.

Category 27.1 *Vulnerability assessment*

2005-10-25 **Symantec Web accounts default password vulnerability password**

DHS IAIP Daily; http://www.securityfocus.com/bid/15188

SYMANTEC DISCOVERY WEB ACCOUNTS DEFAULT PASSWORD VULNERABILITY

Symantec Discovery is prone to a vulnerability regarding the installation password. Remote and local attackers can exploit this issue to gain access to the database without requiring a valid password. This may facilitate further attacks against the database and possibly the underlying system. SecurityFocus reports that Symantec has released patches to address this issue in supported versions. Symantec Website: http://www.symantec.com/avcenter/security/Content/2005.10.24 .html

---

Category 27.1 *Vulnerability assessment*

2005-10-25 **German program software vulnerabilities viruses Trojan horses malicious software malware IT test Internet barometer**

DHS IAIP Daily;
http://www.infoworld.com/article/05/10/25/HNmsgermansecurity _1.html

GERMAN ONLINE SECURITY PROGRAM AIMS TO MAKE USERS AWARE OF SOFTWARE VULNERABILITIES

A German program called "Safe in the Net" seeks to make users aware of e-mail viruses, Trojan horses, and other malicious software. The program, launched earlier this year by a German subsidiary of Microsoft, is offering CDs for users of Windows-based computers that contain programs to locate and remove malware and reboot infected machines. The program includes several components, including: an IT security information package with checklists and examples of good IT security practices; support for software developers and students; a security check; an online test certificate; information on how to buy and sell securely on the Internet; and a security barometer, which warns of current viruses, Trojans and other malware. Developers believe that the program could serve as a model for similar programs in other European and North American markets. Security Initiative: http://www.sicher-im-netz.de.

Category 27.1 *Vulnerability assessment*

2005-10-26 **University of Washington IMAP buffer overflow vulnerability imap mailbox**

DHS IAIP Daily; http://www.securityfocus.com/bid/15009/references

UNIVERSITY OF WASHINGTON IMAP MAILBOX NAME BUFFER OVERFLOW VULNERABILITY

University of Washington imap is prone to a buffer overflow vulnerability. This issue is exposed when the application parses mailbox names. Remote exploitation allows attackers to execute arbitrary code. The vulnerability specifically exists due to insufficient bounds checking on user supplied values.

Category 27.1 *Vulnerability assessment*

2005-10-27 **SGI Linux vulnerabilities Secunia patch**

DHS IAIP Daily; http://secunia.com/advisories/17335/

SGI ISSUES MULTIPLE UPDATES FOR ADVANCED LINUX ENVIRONMENT

SGI has issued updates to fix vulnerabilities in Linux. The vulnerabilities can be exploited to gain escalated privileges, gain knowledge of sensitive information, bypass certain security restrictions, and compromise a user's system. Secunia reports that SGI has issued a patch for SGI Advanced Linux Environment.

Category 27.1 *Vulnerability assessment*

2005-11-10 **computer security threats networked peripheral devices**

DHS IAIP Daily; http://www.pcworld.com/news/article/0,aid,123483,00.asp

ANY NETWORKED OFFICE GEAR CAN BE VULNERABLE TO ONLINE ATTACKERS

On Tuesday, November 9, at a two-day Office Document Solutions conference in Boston, MA, a number of presenters implored makers of printers, copiers, scanners, and other such devices to start thinking about security threats to office gear beyond just computers. According to Jim Joyce, senior vice president for office services at Xerox Global Services, "Network-connected output devices are becoming an absolute primary target of people, foreign and domestic, who are penetrating networks...The reason for that is many of them are large devices with large disk drives, with a fair amount of memory and are network connected and are not secure." Joyce said that Xerox has poured some $20 million in recent years into technologies to better manage office and document systems and is putting a particular emphasis on security. He noted that some machines, such as multifunction devices, might have several operating systems in them that could provide security holes if not protected.

Category 27.1 *Vulnerability assessment*

2005-11-22 **patching deployment fix IT department faster vulnerability assessment**

DHS IAIP Daily;
http://www.computerweekly.com/Articles/2005/11/22/213048/ITd
epartmentsgetfasteratpatchingsystems.htm

IT DEPARTMENTS GET FASTER AT PATCHING SYSTEMS

IT departments have significantly reduced the time they take to patch their systems when new security vulnerabilities, viruses, or worms become public. The average time taken for IT departments to patch half of their external-facing systems has fallen to 19 days, down from 21 days a year ago, and from 30 days two years ago, according to IT security supplier Qualys. IT departments have reduced the time taken to patch half of their internal systems from 52 days to 48 days, according to an analysis of 32 million vulnerability scans of Qualys systems. However, the research showed that 80% of security exploits appear before companies patch half of their systems. Similarly, it showed worms cause most damage within the first 15 days of an outbreak.

Category 27.1 *Vulnerability assessment*

2005-12-12 **research finding security expert port scan sniffing hack attacks low correlation**

DHS IAIP Daily;
http://www.securitypipeline.com/news/175000553;jsessionid=M4
IGXZPVFH0JCQSNDBOCKHSCJUMEKJVN

SECURITY EXPERT FINDS PORT SCANS NOT TIED TO HACK ATTACKS

Port scanning, the practice of sniffing for computers with unprotected and open ports, isn't much of a harbinger of an attack, a University of Maryland researcher said Monday, December 12. Michel Cukier, an assistant professor at the College Park, MD,-based school, said that contrary to common thought, few port scans actually result in an attack. In fact, only about five percent of attacks are preceded by port scans alone. "But when you combine port scans with other kinds of scans, particularly vulnerability scans, there's a much higher probability of an attack," said Cukier. Nearly three-quarters of the attacks prefaced by some kind of scan came after both a port and a vulnerability scan were run against the exposed PCs, noted Cukier's report. Through his research, Cukier expected to see a higher correlation between port scanning and attacks, but the analysis also showed that it was relatively easy to spot the difference between a port scan and a more dangerous vulnerability scan simply by counting up the number of data packets received by the PC. Cukier and his researchers concluded that there seems to be no link between port scans and attacks. Cukier's research paper: http://www.enre.umd.edu/faculty/cukier/81_cukier_m.pdf

---

Category 27.1 *Vulnerability assessment*

2006-04-24 **hacker toolkit attack unpatched vulnerable computers Internet Explorer IE Firefox browsers**

DHS IAIP Daily; http://www.informationweek.com/news/showArticle.jhtml?articl 23
eID=186700539

HACKER'S TOOLKIT ATTACKS UNPATCHED COMPUTERS.

A dirt-cheap, do-it-yourself hacking kit sold by a Russian Website is being used by more than 1,000 malicious Websites, a security company said Monday, April 24. Those sites have confiscated hundreds of thousands of computers using the "smartbomb" kit, which sniffs for seven unpatched vulnerabilities in Internet Explorer and Firefox, then attacks the easiest-to-exploit weakness. For $15 to $20, hackers can buy the "Web Attacker Toolkit," said San Diego-based Websense in an online alert. The tool, which uses a point-and-click interface, can be planted on malicious sites -- or on previously-compromised computers -- to ambush unsuspecting users. "It puts a bunch of code on a site that not only detects what browser the victim is running, but then selects one of seven different vulnerabilities to exploit, depending on how well-patched the browser is," said Dan Hubbard, senior director of security and research at Websense. Websense Informational Alert: Web attacker sites increase: http://www.websensesecuritylabs.com/alerts/alert.php?AlertID =472

27.2 Port scans

Category 27.2 *Port scans*

1999-10-11 **scanning probing proxies**

SANS http://www.sans.org/newlook/resources/ringzero.htm

Widespread port scans were reported in late September to the System Administration, Networking, and Security (SANS) Institute, which coordinated the effort to analyze the problem. Results: someone has probably distributed a Trojan Horse running under Windows that scans ports 80, 8080 and 3128 (and sometimes other ports in the 8000 range) for proxies. SANS advised system administrators to watch for outbound traffic for the target ports. Admins should also either disable unused ports or set firewalls to preclude proxies from being used by outsiders.

Category 27.2 *Port scans*

2000-10-17 **worm penetration port scan infection counterattack response revenge retaliation infection**

RISKS 21 09

A correspondent called "Jeremy" noted in RISKS that the number of netbios probes went up by an order of magnitude in September and October. He pointed out that these systems are presumably infected with a worm or virus and are doing the bidding of the malware writers; however, the infected systems are also announcing all over the Net that they have poor security. "Jeremy" postulated that there could be three types of active response to these probes by anyone interested:
* sterilizing the infections remotely;
* planting another virus or worm;
* disabling the infected machine.

27.3 Intrusion detection systems

Category 27.3 *Intrusion detection systems*

1998-02-16 **intrusion detection criminal hacker penetration alarm**

Communications Week

In _Communications Week_, an article about CyberCop from Network Associates described an interesting case study of intrusion detection at "a large financial services company" that had a beta-test version of the software installed. Apparently the software spotted a couple of penetration attempts and also helped thwart a denial-of-service attack.

Category 27.3 *Intrusion detection systems*

1998-11-30 **intrusion detection tool free event log analysis**

CNET news.com http://www.news.com/News/Item/Textonly/0,25,29352,00.html

The Centrax Corporation announced that it would give away its Centrax Log Analyst (CLA), a tool it described as follows: "CLA is an easy-to-use, snap-in component for the Microsoft Management Console (MMC). CLA analyzes the security logs of Windows NT servers, searching for and alerting you to potential system misuses. These patterns of misuse, called activity signatures, can be as subtle as suspicious file browsing or as treacherous as three consecutive failed logins. Use CLA to centrally analyze your computer network and reduce the headache of manually scanning large security logs."

Category 27.3 *Intrusion detection systems*

1999-02-18 **intrusion detection software log alert warning penetration**

OTC

Internet Security Systems (ISS) has launched a new enterprise threat management system. The RealSecure 3.0 software detects attacks on both network and system levels and responds to any attack automatically. The product includes new detection methods for the latest kinds of attacks, including back door attacks, denial-of-service attacks and other unauthorized access methods. Customers will also receive updates about new uncovered threats.

Category 27.3 *Intrusion detection systems*

1999-03-16 **intrusion detection protocol standards**

http://www.nwfusion.com/news/1999/0316security.html

The IETF working group on intrusion detection proposed a new scheme, the Intrusion Detection Message Exchange Protocol (IDMEP), for sharing information about attacks on systems and networks. Using the standard message formats, any participating system could automatically send messages describing the attack type and relevant addressing information.

Category 27.3 *Intrusion detection systems*

1999-04-10 **security product coordination intrusion detection error firewalls reporting paging alerts warnings**

OTC

Network Associates announced a product for handling trousers: "Event Orchestrator, a security technology that enables products and tools from third-party vendors to coordinate responses to security breeches." Oh wait, that's probably not trousers; they meant security _breaches_. According to the puffery, Event Orchestrator is an object technology based on the Component Object Model that maps a company's security policies to actions," says Zachary Nelson, VP and general manager for Network Associates' Service Desk product line. It picks up alerts from security tools, checks the events against company policies, then takes appropriate action based on the level of risk. For example, if Network Associates' CyberCop Monitor detects a hacker attack, Event Orchestrator can order the ports on a firewall closed to block access rather than page a network administrator to do the same. "Properly configured, Event Orchestrator can react far faster than I can," says Christopher Ward, director of corporate security for Pagemart Wireless Inc., a wireless paging company in Dallas. The system can help to make different components of the security architecture work more smoothly together, especially when the configuration of one device, such as a firewall, can have an effect on others, such as anti-virus products.

Category 27.3 *Intrusion detection systems*

1999-04-13 **intrusion detection White Paper Buyers' Guide product terminology standards descriptions selection criteria**

Business Wire

ICSA.net convened the Intrusion Detection Systems Consortium in April and presented a White Paper clarifying the concepts and standardizing the terminology used to describe intrusion-detection products (see < http://www.icsa.net/services/consortia/intrusion/intrusion.pdf >). In December they published a free (with registration) Buyers' Guide to Intrusion Detection.

Category 27.3 *Intrusion detection systems*

1999-04-21 **intrusion detection product perimeter defenses**

Business Wire

CyberSafe Corporation announced Centrax v 2.2 intrusion detection software they describe as "the first and only product to integrate host-and network-based intrusion detection, vulnerability assessment, and policy management under a single, easy-to-use interface." See <http://www.cybersafe.com> for more details.

Category 27.3 *Intrusion detection systems*

1999-06-14 **slow port scan bypass intrusion detection criminal hacker data diddling deletion malicious penetration password file Linux**

Computerworld

In early 1999, a criminal hacker called "Moof"went on a rampage against Linux servers in a wide range of ISPs and colleges in the US, the UK and Canada. The cracker was using a "slow port scan" in which a probe packet gets sent one port at a time — one port every three hours. Such slow scans are not picked up by intrusion-detection systems, which tend to roll over their detection stacks every 10 minutes or so. In addition, the criminal uses different source addresses for different packets to make it even harder to detect the port scan. Once "Moof" had identified vulnerabilities, (s)he attacked the vulnerable system, installed back doors and used the compromised system to launch more slow scans for new victims. Finally, the criminal erased crucial file system entries on the latest victim, making the system crash.

Category 27.3 *Intrusion detection systems*

1999-08-03 **intrusion detection response unauthorized modification digital signature**

The Australian & http://www.creative.com.au/cdt_prod/securepage.html

Creative Digital Technology (CDT) announced a system of digital signatures for Web servers that would allow the server instantly to stop supplying a hacked page. Unauthorized modifications of any kind to a signed Web page would be detected by the security software and the content blocked so that no one could receive it. More important, the software would substitute a copy of the original, unmodified, Web page from a strongly-encrypted cache. The company showed a responsible attitude towards open quality assurance by offering a cash prize — but only to universities — for the first computer scientists and students who could demonstrate a vulnerability in their system. See <http://www.creative.com.au/cdt_prod/securepage.html> for more information on the SecurePage product.

Category 27.3 *Intrusion detection systems*

1999-08-14 **information warfare surveillance intrusion detection penetration analysis government FBI FIDNET**

National Journal

Neil Munro published a thorough review of the politics of the FIDNet (Federal Intrusion Detection Network) proposal in the _National Journal_ on 1999-08-14. The furore over the monitoring plans included opponents not only from the civil liberties camp but also, in an unlikely combination, representatives of high-tech firms. Companies expressed horror at the thought of mandatory reporting of computer crime because they mistrust the government's ability to safeguard their information and fear of ridicule and embarrassment if the truth were to be revealed to the public. In addition, people with libertarian tendencies just plain dislike government regulation of _anything_.

Category 27.3 *Intrusion detection systems*

1999-08-29 **information warfare surveillance intrusion detection penetration analysis government FBI FIDNET**

New York Times, Washington Post, Wired

The privacy community was not pleased when the Clinton Administration and the FBI announced their FIDNET initiative in July 1999 to monitor network intrusions not only on government systems but also critical infrastructure components such as banking, communications and transport. House Majority Leader Dick Armey (R-TX) attacked the FIDNET proposal and the House Appropriations Committee removed funding for the project from its versions of the relevant appropriations bills. In August, one of FIDNET's main architects spoke out in defense of the plan. Richard Clarke, National Coordinator for Security, Infrastructure Protection and Counterterrorism, explained that fears of an "electronic Pearl Harbor" (a term popularized by Winn Schwartau of <infowar.com> in the early 1990s) led to Presidential Decision Directive 63 and that FIDNET was one of the first major computer-security programs proposed in response to the Directive. He assured skeptics of minimal involvement of the FBI and said that FIDNET would be managed by the NIPC (National Infrastructure Protection Center), not the Department of Justice. The system would not intrude on personal or corporate privacy, he said. On 27 Sept, Rep. Armey sent another challenge to the Dept of Justice demanding clarification of critical elements of FIDNET. In January 2000, the Administration tried again, bundling FidNET into anti-cybercrime proposals presented by the Department of Commerce.

Category 27.3 *Intrusion detection systems*

2004-01-23 **Florida instrusion detection systems IDS funding**

NIPC/DHS; http://www.fcw.com/geb/articles/2004/0119/web−florida−01−20−04.asp

January 20, Federal Computer Week — Florida governor seeks IT funding overhaul.

Florida Governor Jeb Bush on Tuesday, January 20, outlined a 2004-2005 budget that calls for several changes at the State Technology Office (STO), including consolidating its funds to gain better control of cross-sector initiatives. This year, the STO's Information Technology Security Office is developing a statewide intrusion detection service, or Cyber Center, using funding from a federal grant. That service "will move the office into an expanded role to provide physical monitoring of the state's IT infrastructure to detect, prevent and minimize cybercrime," according to budget documents. Governor Bush requested almost $1.1 million of the state's money to continue the security office's work. The new budget also reflects the STO's shift from legacy systems to Web-based services. Over all of this, the budget proposes a complete reorganization of the STO's programs into a single budget. "This realignment of budget authority within a single budget entity will provide the necessary flexibility for the State Technology Office to meet the needs of its IT partners and customers as needed, while also maintaining the requisite level of budgetary accountability."

Category 27.3 *Intrusion detection systems*

2004-10-23 **neural networks University of Florida**

NewsScan; http://www.wired.com/news/medtech/0,1286,65438,00.Html

NEURAL NETWORK AT THE CONTROLS

Researchers at the University of Florida have created a neural network made up of 25,000 disembodied rat neurons and hooked it up to a flight simulator on a desktop computer. The neurons, which are growing on top of a multi-electrode array, are fed information about the simulated F-22's horizontal and vertical movements by stimulating the electrodes, causing them to fire in patterns that are then used to control the aircraft. "It's as if the neurons control the stick in the aircraft, they can move it back and forth and left and right," says UF professor Thomas DeMarse. "The electrodes allow us to record the activity from the neurons and stimulate them so we can listen to the conversation among the neurons and also input information back into the neural network." Thus far, the network has "learned" how to control the fighter jet's pitch and roll in a broad range of weather conditions, but DeMarse plans to improve the system by having the "brain" use a horizon to judge how well it's controlling the aircraft. The goal is to find out how the neurons communicate with each other and eventually translate that knowledge into the development of a novel computing architecture. (Wired.com 23 Oct 2004)

[MK note: of possible value for future intrusion-detection systems?]

Category 27.3 *Intrusion detection systems*

2005-04-27 **data leakage loss confidentiality control database privacy personal information audit test procedure risk management**

RISKS 23 87

COMPROMISE-DETECTION TEST FOR PERSONAL-INFORMATION DATABASES

Pekka Pihlajasaari wrote from South Africa about an excellent method for detecting compromise of personal-information databases:

Many articles documenting the risks of exposure of personally identifiable information bemoan the possibility of compromise. There seems to be very little quantitative information on the number of cases where the information is used inappropriately.

If a selection of unused social security numbers were identified as probes, these could be used by credit bureaux and other large databases as proxies for compromise. Any use of these numbers would be positive confirmation of breach of the related database, and an indication of the rate at which harvested numbers are utilised. While this does pollute the datasets with incorrect data, this provides an in-band mechanism to detect misuse. The practise has been in use by mailing list rental companies to count the number of times a list is used.

The low occurrence of the probes makes wholesale harvesting easy to detect and difficult for the harvester to protect themselves against. This risk, of course, is that the list of probe numbers is compromised!

[MK notes that criminals' creation and fraudulent use of fake SSNs that happened to match the probes would trigger false positives in this system, but that problem does not invalidate the method proposed as a useful tool.]

Category 27.3 *Intrusion detection systems*

2005-07-14 **Apple OS X fixes crash data firewall filtering 10.4 Tiger widgets Dashboard warning install**

DHS IAIP Daily; http://www.vnunet.com/vnunet/news/2139781/apple−issues−two−s ecurity

APPLE UNVEILS OS X SECURITY PATCHES

Apple has released two security fixes for bugs in its OS X operating system. The first patch plugs a hole that could allow hackers to crash a system by sending a specially crafted data packet. The flaw effectively opens up the system for a denial of service attack. A security notice on Apple's Website says that the flaw affects only the 10.4 versions of OS X and will not harm computers that sit behind a 12 firewall or are otherwise protected through packet filtering. The other patch targets a bug in the 10.4 Tiger operating system that allows users inadvertently to overwrite standard widgets in Apple's Dashboard application. The update provides a warning when a user attempts to install a widget that has the same name as an existing one. Previously the new widget would run instead of the system widget, effectively making the original one inaccessible to the user. This latest update moves OS X 10.4 to version 10.4.2.

Category 27.3 *Intrusion detection systems*

2005-10-04 **network attack tracking intrusion detection academic campus Internet comparison intelligence project Columbia University**

EDUPAGE; http://chronicle.com/daily/2005/10/2005100401t.htm

RESEARCH PROJECT WILL TRACK NETWORK ATTACKS

A research project will collect regular snapshots of computer networks from as many as 10 colleges and universities in an effort to improve protections from and responses to Internet attacks. The Information Security in Academic Institutions project, an initiative of the Columbia University Teachers College, uses monitoring technology called Dshield and has already been tested at three institutions. The other institutions in the project have yet to be named, and the system may eventually be widely available. The system will give network administrators data about the state of networks, allowing them to gain a better understanding of Internet attacks by comparing data from before, during, and after an attack. Steffani A. Burd, executive director of the project, described it as "a 360-degree view of what's going on." The system will also pool data collected from participating institutions and make it available anonymously on the Web. This aggregation of data will allow a comparison between activity on the Internet generally and what's happening at campuses. Chronicle of Higher Education, 4 October 2005 (sub. Req'd)

27.4 Firewalls & other perimeter defenses

Category 27.4 *Firewalls & other perimeter defenses*

1997-05-31 **addiction cyber-pets**

RISKS 19 20

In a further outbreak of silliness, Dr Daniel DeSouza of Toronto set up an Internet support group to help bereaved owners of dead Tamagotchi cyber-pets.

Category 27.4 *Firewalls & other perimeter defenses*

1997-06-17 **Internet addiction**

EDUPAGE

A Cincinnati mother lost possession of her children when police discovered she was locking them into a filthy room in order to surf the Net 12 hours a day.

Category 27.4 *Firewalls & other perimeter defenses*

1997-09-09 **Internet addiction**

AP

A woman with the wonderful eponymous married name of "Sandra Hacker" was ordered by a judge in Cincinnati to take parenting classes after she pleaded guilty to midemeanor child endangering. She was arrested in a filthy apartment where her 2, 3 and 5-year old children grovelled in squalor while she spent 12 hours a day surfing the Internet.

Category 27.4 *Firewalls & other perimeter defenses*

1997-10-02 **ergonomics information fatique syndrome**

EDUPAGE

In an exhausting piece of news, Reuters reported that half of all senior managers and a third of all managers suffer from Information Fatigue Syndrome and are getting physically sick from the stress of information overload.

Category 27.4 *Firewalls & other perimeter defenses*

1997-12-17 **video seizures epilepsy**

RISKS 19 51

Hundreds of children in Japan went into seizures when a TV cartoon show flashed stoboscopic images of a colorful explosion on their screens.

Category 27.4 *Firewalls & other perimeter defenses*

1998-05-04 **firewall standards certification criteria ICSA**

Government Computer News 17 12

ICSA warned that federal agencies might be vulnerable because some firewall products in use did not meet their firewall standards. Many products did not meet the latest ICSA test criteria; some also lack adequate documentation, often leading to vulnerabilities because of mistakes during installation. ICSA introduced its Version 2.0 criteria for firewall testing in Jun 1997. As C. J. Dorobek wrote in _Government Computer News_, "All of the 25 products examined eventually passed version 1.0, but 11 of them required some modification or debugging; only 40 of 43 products could pass version 2.0, with 24 needing modification. The number of products needing correction is up to 51 percent, and ICSA officials say they are noting a trend toward poor quality since newer products, especially those designed for Windows NT, are failing more often."

Category 27.4 *Firewalls & other perimeter defenses*

1999-02-18 **personal firewall PCs intrusion detection**

PR

Signal 9 Solutions of Kanata, ON (Canada) announced its ConSeal PC Firewall in February 1999, claiming that it was "the first firewall designed especially for the individual Internet user/surfer and SOHO small office/home office." [This news came as a surprise to users of products such as AtGuard from Walker, Richer & Quinn, released more than a year earlier.]

Category 27.4 *Firewalls & other perimeter defenses*

1999-02-23 **partition separation classified unclassified tunneling access-control firewall**

Australian

Dr Mark Anderson of the Australian Defence Science and Technology Organisation (DSTO) won the Minister for Defence Achievement Award for his development of the Starlight suite of INFOSEC products. The Starlight products allow secure access to unclassified systems on a workstation that includes classified systems and also an intrusion-detection system called Shapes Vector.

Category 27.4 *Firewalls & other perimeter defenses*

1999-02-24 **firewall configuration tips hints suggestions policies**

OTC

Finnish telecommunications company Nokia shared some of its INFOSEC recommendations in February 1999. Some of the key points:
* disallow pings outright: drop them entirely without any response.
* log everything coming into the firewall.
* configure NAT (network address translation) to drop ICMP packets without response.
* use the stealth rule: drop (not reject) any packet directed to the firewall (as opposed to the network inside).
* use VPNs where possible and re-authenticate users before granting access to restricted areas of the network.

Category 27.4 *Firewalls & other perimeter defenses*

1999-04-13 **firewall secure Web server criminal hackers**

PR

In an odd bit of publicity, Systems Advisory Group Enterprises, Inc. (SAGE) announced in April 1999 that Carolyn Meinel, a criminal-hacker sympathizer much detested by criminal hackers agreed to use the BRICKHouse(TM) Web server to protect the new Happy Hacker Web site <www.happyhacker.org> from hostile attackers.

Category 27.4 *Firewalls & other perimeter defenses*

1999-08-03 **personal firewall filtering home computer PC workstation intrusion-detection**

Business Wire and www.networkice.com

Network ICE launched its new personal firewall in August 1999. BlackICE software was described as suitable for home computers, especially those connected via cable modems, to block attacks from criminal hackers. The detailed log files serve the intrusion detection function by providing useful forensic evidence of the attacks. The company's press releases stressed the following features:
* Corporate strength intrusion defense for the consumer market.
* Runs on Windows 95, Windows 98, and Windows NT operating systems.
* Protects against over 200 signatures or known attacks such as Back Orifice, Smurf attacks and port scans.
* "Instant On" installation for quick and easy start up
* Intuitive user interface details hacker identification, intrusion severity level and attack summary
* Live alert mechanism for instant Internet attack notification
* AdvICE link for quick help and detailed information on Internet hacks

See <http://www.networkice.com> for more information. Cost of a one-year subscription was $40.

Category 27.4 *Firewalls & other perimeter defenses*

1999-09-27 **DSL cable modem ISP firewall**

PR

The Texas ISP Texas.Net announced that its DSL and cable modem users would not require individual firewalls, claiming that its own firewalls would do the job of protecting them against intrusion and damage.

Category 27.4 *Firewalls & other perimeter defenses*

1999-11-17 **virtual private network HTTP tunnel bypass firewall**

Network News, GNU

The NoCrew hacker group presented the world with HTTPTunnel, a tool to create an encrypted bi-directional data path that can elude firewalls and break policy on connections into and out of corporate networks. Writing in a firewalls discussion list, Stevin Bellovin wrote, "Firewalls are based on two fundamental assumptions: that anyone on the outside may be bad, and that all actors on the inside are good. If the latter assumption is false, your firewall is useless. Once upon a time, the inside "actors" referred to people. In an era of mobile code — mobile in the sense of both Java/ActiveX and in reference to outside code that is installed — the word refers to the such programs as well."

He continued, "Here we have a piece of `malware' — code designed to subvert administrative policy. Although perhaps in theory it could be installed by, say, a Makefile in some popular package, or by a Trojan horse in something you run, most likely it would be deliberately installed by someone who doesn't like the firewall. But the difference isn't that important — what matters is that either is a bad actor on the inside. The precise tunnel chosen isn't that interesting, either. . . . *Any* bidirectional channel can be used as a tunnel — and if your users are hell-bent on getting around your firewall, they're going to. *Maybe* you can use traffic analysis to find such things, but then you're in a serious arms race. You can't use technical means to enforce a stricter security policy than your organizational culture will support, though human means, such as a chat with management, may work."

Category 27.4 *Firewalls & other perimeter defenses*

2000-02-26 **cable modem home PC workstation criminal hackers vulnerability tunneling corporate systems compromise passwords dialup**

Australian

Security expert Christopher Rouland of Internet Security Systems (ISS) warned that cable-modem users are at risk of attack by criminal hackers because of the users' full-time presence on the Net. He urged users to protect their PCs against penetration and warned against tunneling to their corporate systems when using cable modems. Hackers who penetrate unprotected cable-modem users' systems could steal dialup IDs and passwords stored on the local computers, he said.

Category 27.4 *Firewalls & other perimeter defenses*

2000-08-13 **firewall vulnerabilities exploits demonstration conference**

RISKS, ZDNet 21 02
http://www.zdnet.com/zdnn/stories/news/0,4586,2610719,00.html

A demonstration at the Black Hat security conference in Las Vegas showed how the Checkpoint Firewall-1 could easily be defeated by hackers. The successful attacks included
* impersonation of an authorized admin;
* making a non-secured Internet connection look like an authorized VPN connection;
* exploiting filtering algorithm errors to pass dangerous commands through the firewall.
The panelists warned that their demonstration was not specific to the Checkpoint product but applied to other products as well. The Director of Product Marketing for Checkpoint warned that the exploits depended on bad configuration of the devices. Fixes for the vulnerabilities were issued with the cooperation of the three lecturers (John McDonald and Thomas Lopatic of Data Protect GmbH plus Dug Song of U. Michigan).

Category 27.4 *Firewalls & other perimeter defenses*

2002-01-20 **firewall VPN DoS prevention content filtering**

Security Wire Digest 4 5

ZYXEL LAUNCHES THREE IPSEC VPN FIREWALLS
ZyXEL Communications, a manufacturer of firewall and broadband access devices, last week [January 2002] released three new firewall products--ZyWALL 1, ZyWALL 50 and ZyWALL 100. The products are scaled to allow home or business users to purchase a firewall with the exact number of VPN tunnels they require. ZyWALL offers stateful packet inspection, denial-of-service (DoS) attack prevention and Internet content filtering.
http://www.zyxel.com

Category 27.4 *Firewalls & other perimeter defenses*

2002-03-14 **firewall ISP Internet service provider interaction default disable denial-of-service**

RISKS 21 98

Tim Loeb reported that connecting to the Earthlink ISP disables Windows XP's firewall without notification. This happens even though the firewall does work -- once -- immediately after being enabled. However, logging on to the network again immediately disables the firewall.

Category 27.4 *Firewalls & other perimeter defenses*

2002-04-25 **firewall proxy servers US military DoD Department of Defense US Army**

Security Wire Digest 4 32

*ARMY INSTALLS WEB PROXY SERVERS
The Army has set up proxy servers for its public Web sites to help prevent the actual sites from being attacked. The practice is common in the corporate world, where proxy servers allow public access to company information without providing crackers direct means to access the Web server. Gartner Group security analyst John Pescatore told Federal Computer Week that Web sites' susceptibility to defacement decreases from 67 percent to less than 5 percent with good application-level firewalls, which are similar to the proxy server system being used by Army sites. The server setup is part of a broader program called Web Risk Assessment Cell, created in 1999 to monitor Department of Defense Web sites and maintain the security of sensitive data accessible on public Web sites.

Category 27.4 *Firewalls & other perimeter defenses*

2004-02-20 **personal firewall ZoneAlarm vulnerability e-mail attack buffer overflow**

DHS IAIP Daily; http://www.eweek.com/article2/0,4149,1530946,00.asp

February 20, eWeek — ZoneAlarm bug bares system to e-mail attack.

Security vendor Zone Labs has disclosed that several versions of its personal-firewall products are vulnerable to a buffer-overflow attack. ZoneAlarm, ZoneAlarm Plus and ZoneAlarm Pro 4.0.0 versions; ZoneAlarm Pro 4.5.0; as well as Zone Labs Integrity Client 4.0.0 are vulnerable. ZoneAlarm users are advised to upgrade to Version 4.5.538.001. The problem was described by eEye Digital Security on the BugTraq mailing list. The firewalls process SMTP (e-mail) traffic sent to or from the system. According to the description, a sufficiently large value in the SMTP "RCPT TO" command can overflow a stack-based buffer in the TrueVector Internet Monitor (vsmon.exe) process. According to Zone Labs, "If successfully exploited, a skilled attacker could cause the firewall to stop processing traffic, execute arbitrary code, or elevate malicious code's privileges." An attacker with local access and restricted privileges could invoke the attack by sending an e-mail with the overflowed RCPT TO command. The user could elevate his privileges to SYSTEM level, and a remote user could invoke the attack by manipulating the system into sending an e-mail with the overflow value. Additional information available here: http://download.zonelabs.com/bin/free/securityAlert/8.html

---

Category 27.4 *Firewalls & other perimeter defenses*

2004-03-31 **new security hacking toolkit Cisco warning threat vulnerability**

DHS IAIP Daily;
http://www.computerworld.com/securitytopics/security/story/0,10801,91748,00.html

March 29, IDG News Service — Cisco warns of new hacking tool kit.

Cisco Systems Inc. has warned customers about the public release of computer code that exploits multiple security vulnerabilities in Cisco products. Using exploits for nine software vulnerabilities, the program could allow malicious hackers to compromise Cisco's Catalyst switches or a wide variety of machines running versions of the company's Internetwork Operating System (IOS). Called the Cisco Global Exploiter, the program appears to give users a menu of choices, depending on the system they are trying to crack. It offers, for example, the "Cisco 677/678 Telnet Buffer Overflow Vulnerability" or the "Cisco Catalyst 3500 XL Remote Arbitrary Command Vulnerability," according to the Web site, www.k-otik.com. Computer code for a program matching the description in the Cisco security notice was posted on the French-language computer security exploit site yesterday. While many of the exploits can be used only to shut down affected Cisco devices in denial-of-service attacks, at least one enables remote attackers to run malicious code on the affected system without needing a username or password, according to the Cisco security notice. Customers should patch software vulnerabilities exploited by the program.

Category 27.4 *Firewalls & other perimeter defenses*

2004-08-19 **Cisco Internetwork Operating System IOS vulnerability OSPF packets denial-of-service DoS**

DHS IAIP Daily; http://www.kb.cert.org/vuls/id/989406

August 19, US-CERT — Vulnerability Note VU#989406: Cisco IOS fails to properly handle malformed OSPF packets.

Cisco Internetwork Operating System (IOS) is a very widely deployed network operating system. IOS provides support for the Open Shortest Path First (OSPF) protocol. There is a denial-of-service vulnerability in the way OSPF packets are processed by IOS. By sending a specially crafted OSPF packet to an affected device, a remote, unauthenticated attacker could cause the device to reload. Repeated exploitation of this vulnerability could result in a denial-of-service condition. In order to exploit this vulnerability, an attacker would need to know several parameters. These parameters include the OSPF area number, netmask, hello, and dead timers, which are configured on the affected device. Information about upgrading is available on the Cisco Website: http://www.cisco.com/warp/public/707/cisco-sa-20040818-ospf. Shtml

---

Category 27.4 *Firewalls & other perimeter defenses*

2004-08-27 **Cisco Internetwork Operating System IOS telnet denial of service DoS vulnerability**

DHS IAIP Daily;
http://www.cisco.com/en/US/products/products_security_advisory09186a00802a
cbf6.shtml#summary

August 27, Cisco Security Advisory — Cisco telnet denial of service vulnerability.

A denial-of-service vulnerability exists in Cisco's Internetwork Operating System (IOS). This vulnerability could allow remote attackers to prevent new connections to remote management services on a vulnerable device. This vulnerability allows specially crafted TCP packets sent to the telnet or reverse telnet service to cause the device to refuse subsequent connections to these management services. There are reports of this vulnerability being actively exploited. Patches and workarounds are available through the Source link below.

Category 27.4 *Firewalls & other perimeter defenses*

2004-11-11 **Cisco Internetwork Operation System IOS vulnerability DHCP protocol exploit denial of service DoS attack**

DHS IAIP Daily; http://www.kb.cert.org/vuls/id/630104

November 11, US-CERT — Technical Cyber Security Alert TA04-316A: Cisco IOS Input Queue Vulnerability.

There is a vulnerability in the way Cisco IOS processes Dynamic Host Configuration Protocol (DHCP packets). Exploitation of this vulnerability may lead to a denial of service. The processing of DHCP packets is enabled by default. The Dynamic Host Configuration Protocol (DHCP) provides a means for distributing configuration information to hosts on a TCP/IP network. The Cisco Internetwork Operating System (IOS) contains a vulnerability that allows malformed DHCP packets to cause an affected device to stop processing incoming network traffic. By sending a specially crafted DHCP packet to an affected device, a remote, unauthenticated attacker could cause the device to stop processing incoming network traffic. Repeated exploitation of this vulnerability could lead to a sustained denial-of-service condition. In order to regain functionality, the device must be rebooted to clear the input queue on the interface. Cisco is tracking this issue as CSCee50294. US-CERT is tracking this issue as VU#630104. A solution is to upgrade to fixed versions of IOS available at: http://www.cisco.com/warp/public/707/cisco-sa-20041110-dhcp. Shtml

---

Category 27.4 *Firewalls & other perimeter defenses*

2004-11-19 **ZoneAlarm advertising blocking vulnerability denial of service DoS**

DHS IAIP Daily; http://secunia.com/advisories/13244/

November 19, Secunia — ZoneAlarm advertising blocking denial of service vulnerability.

A vulnerability has been reported in ZoneAlarm Pro and ZoneAlarm Security Suite, which can be exploited by malicious people to cause a DoS (Denial of Service). The vulnerability is caused due to an error in the Ad-Blocking feature (disabled by default) when processing JavaScript and can be exploited by tricking a user into visiting a malicious Website containing specially crafted JavaScript. Update to version 5.5.062 or later via the "Check For Update" feature.

Category 27.4 *Firewalls & other perimeter defenses*

2005-01-19 **Cisco Internetwork Operating System IOS call processing solutions telephony vulnerability denial of service DoS attack update issued**

DHS IAIP Daily; http://www.cisco.com/warp/public/707/cisco−sa−20050119−itscm e.shtml

VULNERABILITY IN CISCO IOS EMBEDDED CALL PROCESSING SOLUTIONS

Cisco Internetwork Operating System (IOS®) Software release trains 12.1YD, 12.2T, 12.3 and 12.3T, when configured for the Cisco IOS Telephony Service (ITS), Cisco Call Manager Express (CME) or Survivable Remote Site Telephony (SRST) may contain a vulnerability in processing certain malformed control protocol messages. A successful exploitation of this vulnerability may cause a reload of the device and could be exploited repeatedly to produce a Denial of Service (DoS). Vendor solution available through Source link below.

Category 27.4 *Firewalls & other perimeter defenses*

2005-01-26 **Cisco Internetwork Operating System IOS Border Gateway Protocol BGP packet reload vulnerability denial of service DoS attack update issued**

DHS IAIP Daily; http://www.cisco.com/warp/public/707/cisco−sa−20050126−bgp.s html#software

CISCO IOS MISFORMED BGP PACKET CAUSES RELOAD

A Cisco device running IOS® and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service attack from a malformed BGP packet. Only devices with the command bgp log-neighbor-changes configured are vulnerable. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. Solution available through Source link below.

Category 27.4 *Firewalls & other perimeter defenses*

2005-01-27 **Cisco Internetwork Operating System IOS MPLS interface disable vulnerability update issued**

DHS IAIP Daily; http://securitytracker.com/alerts/2005/Jan/1013015.html

CISCO IOS MPLS DISABLED INTERFACES LET REMOTE USERS DENY SERVICE

A vulnerability was reported in Cisco IOS in the processing of Multi Protocol Label Switching (MPLS) packets. A remote user can cause denial of service conditions. A remote user on a local network segment can send a specially crafted packet to an MPLS disabled interface to cause the interface to reset. Original advisory and solution available at: http://www.cisco.com/warp/public/707/cisco-sa-20050126-les.s html

---

Category 27.4 *Firewalls & other perimeter defenses*

2005-01-27 **Cisco Internetwork Operating System IOS reload IPv6 packets vulnerability denial of service DoS conditions update issued**

DHS IAIP Daily; http://securitytracker.com/alerts/2005/Jan/1013016.html

CISCO IOS CAN BE RELOADED BY REMOTE USERS SENDING MULTIPLE IPV6 PACKETS

A vulnerability was reported in Cisco IOS in the processing of IPv6 packets. A remote user can cause denial of service conditions. A remote user can send multiple specially crafted IPv6 packets to the target device to cause the device to reload. Only systems configured for IPv6 are affected. The vulnerability can be exploited repeatedly to cause prolonged denial of service conditions. Original advisory and solution available at: http://www.cisco.com/warp/public/707/cisco-sa-20050126-ipv6. shtml

---

Category 27.4 *Firewalls & other perimeter defenses*

2005-04-06 **Cisco Internetwork Operating System Internet Key Exchange IKE X authority Xauth authentication bypass vulnerabilities update issued**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2005/0321

CISCO IOS IKE XAUTH AUTHENTICATION BYPASS VULNERABILITIES

Two vulnerabilities were identified in Cisco IOS, which may be exploited by remote attackers to gain unauthorized access to the network resources. The first flaw resides in the Easy VPN Server XAUTH feature which fails to handle certain malformed packets (port 500/udp). The second vulnerability exists where the ISAKMP profile is assigned but the attributes that are configured in the ISAKMP profile are not processed. Original advisory and solution: http://www.cisco.com/en/US/products/products_security_advisory09186a008042d519.shtml#software

---

Category 27.4 *Firewalls & other perimeter defenses*

2006-03-09 **Zone Labs ZoneAlarm Security Suite privilege escalation vulnerabilities**

DHS IAIP Daily; http://www.securiteam.com/windowsntfocus/5IP012KI0K.html 23

EIGHTEEN WAYS TO ESCALATE PRIVILEGES IN ZONE LABS ZONEALARM SECURITY SUITE.

A locally exploitable security vulnerability in Zone Labs ZoneAlarm Security Suite allows normal users to elevate their privileges. Analysis: Instead of using the full path to the DLL during the load process only the name of the DLL is used. This causes several instances of Windows PATH trolling where Windows tries to locate the DLL in the directories listed in its PATH environment variable on behalf of the vsmon.exe process. This PATH trolling is what makes the vsmon.exe process vulnerable to several privilege escalation techniques. Vulnerable product: Zone Labs ZoneAlarm Security Suite build 6.1.744.000. Patches/Workarounds: The vendor was notified several times but there was no response.

Category 27.4 *Firewalls & other perimeter defenses*

2006-03-13 **ZoneAlarm personal firewall software TrueVector Service local privilege escalation vulnerability no solution**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2006/0947 23

ZONEALARM TRUEVECTOR SERVICE LOCAL PRIVILEGE ESCALATION VULNERABILITY

A vulnerability has been identified in ZoneAlarm, which could be exploited by malicious users to obtain elevated privileges. Analysis: The error in the TrueVector service ("VSMON.exe") that loads certain Dynamically Linked Libraries (DLL) in an insecure manner, which could be exploited by local attackers to execute arbitrary commands with SYSTEM privileges by placing a malicious DLL in a specific directory. Affected product: ZoneAlarm versions 6.x. Solution: The FrSIRT is not aware of any official supplied patch for this issue.

27.5 Honeypots

Category 27.5 *Honeypots*

2003-02-03 **exposed vulnerable server high attack rate honeypot**

NIPC/DHS

January 29, Silicon.com — Exposed server is a magnet for hack attacks.

The amount of hacking activity on the Internet has been revealed after one company set up an anonymous 'dummy test' server —and found it was maliciously attacked 467 times within 24 hours of being installed. The server, which contained no data and had no public profile, was attacked every single day over the next three weeks. PSINet Europe ran the test on an unprotected server at its Internet Data Center in Amsterdam, and registered a total of 626 malicious attacks over the three week period. A significant number of attacks originated from broadband or cable ISPs. PSINet's report into the experiment says that: "High bandwidth links do not only provide end users with faster download times—they also allow hackers to attack a wider target audience with a wider array of tools." PSINet also found that the bulk of the attacks originated from the United States and Western Europe and not in the most commonly expected areas of the former Eastern Bloc countries. Within Europe, Germany, Italy, the Netherlands and the UK were the most popular locations, while the countries most associated with attackers —Russia, Bulgaria and Romania—did not even feature. The findings of the PSINet Europe test are backed up by figures from the Gartner Group, which reported that 90 per cent of security breaches occur as a result of networks being incorrectly configured and managed.

27.7 Anti-malware technology

Category 27.7 Anti-malware technology

2002-03-10 **worldwide virus worm infection data top ten infectors malware**

Trend World Virus Tracking Center

The new Trend World Virus Tracking Center < http://wtc.trendmicro.com/wtc/ > shows the top ten viruses observed in the wild through "actual virus infections detected by HouseCall, our free on-line virus scanner for PCs, and by the Trend Virus Control System (TVCS), our central management solution for network administrators." Viewers can easily select geographical areas and time periods of the last 24 hours, 7 days, or 30 days as well as details of each virus or worm. For example, as of 10 March 2002, the top ten infectors worldwide in the previous 30 days were as follows (showing the number of infected computers logged in parentheses) and a brief description of some of the malware types from Trend Micro's links to its comprehensive Virus Encyclopedia:

PE_NIMDA.A-O (233,321) [This is a fast-spreading Internet worm and file infector in pure and original form. It arrives as an embedded attachment, README.EXE file, in an email that has an empty message body and, usually, an empty subject field. It does not require the email receiver to open the attachment for it to execute. It uses a known vulnerability in Internet Explorer-based email clients to execute the file attachment automatically. This is also known as Automatic Execution of Embedded MIME type. The infected email contains the executable attachment registered as content-type of audio/x-wav so that when recipients view the infected email, the default application associated with audio files is opened. This is usually the Windows Media Player. The embedded EXE file cannot be viewed in Microsoft Outlook.]

WORM_SIRCAM.A (113,409) [This Worm is a high-level program created in Delphi that propagates via email using SMTP commands. It sends copies of itself to all addresses listed in an infected user's address book and in temporary Internet cached files. It arrives with a random subject line, and an attachment by the same name. This Worm also propagates via shared network drives.]

PE_NIMDA.A (74,724) [

PE_MAGISTR.B (64,199) [This variant of PE_MAGISTR.A has polymorphic capabilities. It obtains email addresses from *.WAB, *.DBX, and *.MBX files found in the infected system's disk and then sends emails with its infected files as attachments. It may also include non-viral files such as .DOC, .GIF, and .TXT files as attachments to the emails it sends out.This destructive variant trashes the Hard Drive and deletes certain files.]

PE_FUNLOVE.4099 (56,146) [This virus infects all Win32 type Portable Executable (PE) files such as .EXE, .SCR, and .OCX in both Windows 9x and Windows NT 4.0. platforms. It searches for all Shared Network Folders with write access and then infects the files within them. To infect NT system files, the virus patches the integrity checking.]

PE_NIMDA.E (46,722)

PE_MAGISTR.A (37,346)

WORM_BADTRANS.B (36,157) [This memory-resident Internet worm is a variant of WORM_BADTRANS.A. It propagates via MAPI32, has a Key Logger component, and arrives with randomly selected double-extension filenames. It does not require the email receiver to open the attachment for it to execute. It uses a known vulnerability in Internet Explorer-based email clients (Microsoft Outlook and Microsoft Outlook Express) to automatically execute the file attachment. This is also known as Automatic Execution of Embedded MIME type.]

JS_EXCEPTION.GEN (31,733) [This Java Script (JS) Trojan changes the infected user's Internet Explorer startup page. One of this Trojan's samples (Coolsite samples) is a mass-mailer. It exploits security vulnerabilities in the Microsoft Virtual Machine. Some variants have non-destructive payloads that change the button caption, modify the appearance of Internet Explorer, and redirect links to a certain Web site.]

WORM.KLEZ.E (28,057) [This destructive mass-mailing worm propagates copies of itself across network drives. Upon execution, it drops two executable files, WINK*.EXE and WQK.EXE, in the Windows System folder. It also creates registry entries that allow it to run at system startup.

This worm terminates processes, and occasionally deletes files associated with certain antivirus programs. On the sixth (6) day of every odd-numbered month (January, March, May, July, September, November) it overwrites files with the following extensions: TXT, HTM , HTML , WAB , DOC , XLS , CPP , C , PAS , MPEG , MPG , BAK , MP3 , JPG.]

Category 27.7 *Anti-malware technology*

2002-07-18 **antivirus malware homeland defense**

NewsScan

BE PATRIOTIC -- UPDATE YOUR PC SECURITY SOFTWARE!
Keeping your home computer's anti-virus software isn't just good maintenance -- it's downright patriotic, says Richard Clarke, computer security adviser to President Bush. "Every American relies upon cyberspace and every American has to do something to secure their part of cyberspace," says Clarke, who's planning to unveil a national plan to protect cyberspace on Sept. 19. The plan, which is being hashed out among government officials with input from technology firms, will serve as the Internet component of the overall national strategy for homeland defense. It will include recommendations in five categories: home and small-business users; major corporations; "sectors" like banking, utilities and government; national issues; and global Internet users. (AP 17 Jul 2002)
http://apnews.excite.com/article/20020717/D7KQTBU80.htm

Category 27.7 *Anti-malware technology*

2002-11-01 **adaptive response anti-malware quarantine database prototype**

NewsScan

SOFTWARE REPAIRS DAMAGE WHILE SYSTEMS WORK
Researchers at Pennsylvania State University have developed software that can quarantine malicious commands and repair any damage that's been done to a system, while the database continues to process transactions. "We can't prevent attackers from getting in, but with this technology, the database can heal itself on the fly? The database can adapt its own behavior and reconfigure itself based on the attack," says Dr. Peng Liu, who heads up the Penn State team. The Cyber Security Group and the U.S. Air Force are testing a prototype of the software, which is not yet commercially available. Several large database vendors have begun offering self-healing systems, but analysts say the Penn State effort is the most advanced so far. "There are various tools that can detect anomalies, but they simply generate a report or display that calls someone's attention to it," says an IDC analyst. "The interesting part of the (Penn State) research? is the ability to automatically respond to the attack." (CNet News.com 31 Oct 2002)
http://news.com.com/2100-1001-964109.html?tag=fd_top

Category 27.7 *Anti-malware technology*

2002-11-26 **antimalware control bandwidth reduction throttle limitation spread response time worm e-mail**

NewsScan

ANTIVIRUS TOOL THROTTLES DOWN ON INFECTION RATE
Matthew Williamson, a researcher at the Hewlett-Packard labs in the UK, has developed a new approach to battling computer viruses. It slows down the infection rate significantly by limiting the number of connections at any one time by an infected computer. "The major problem with computer viruses is that because they spread so quickly and our response is so slow, they cause so much damage," says Williamson. "We are tackling the fundamental nature of a virus? When your machine gets an e-mail virus, it sends lots and lots of e-mail messages at a much higher rate than you would normally send them. So if I put a limit on the rate of e-mail messages that you can send in every 10 minutes, then a virus trying to send 100 or 200 messages will very quickly get delayed." Williamson found that using the "throttle" technique has a negligible impact on the day-to-day performance of his computer. (BBC News 26 Nov 2002)
http://news.bbc.co.uk/1/hi/technology/2511961.stm

Category 27.7 *Anti-malware technology*

2004-03-03 **antivirus scanner attachments password protection remove ZIP files security policy unintended consequences**

RISKS 23 24

UNINTENDED CONSEQUENCES OF ATTACKING VIRAL MAIL

With some viruses sending out e-mail containing password-protected attachments, some system administrators have taken to removing all password-protected attachments from inbound e-mail. Vassilis Prevalakis of the Computer Science Department at Drexel University points out that such broad-brush responses "will cause severe disruption to secure communications over e-mail." He thinks "we should resist such efforts and prevent the spammers and virus writers do to us what the government failed to do."

Category 27.7 *Anti-malware technology*

2004-06-18 **hack-back systems retaliations iSIMS Symbiot Security**

NewsScan

ATTACKING THE ATTACKERS: MAYBE NOT A GOOD IDEA

A company called Symbiot Security has created "Intelligent Security Infrastructure Management Systems" (iSIMS) that not only provide traditional defensive measures against viruses, worms, and other kinds of network vandalism -- but also offer the victims of vandalism a gradual escalation of
retaliation measures. These include the ability to flood the attacking computers with data. However, some experts say that retaliatory actions could be a very bad idea. Adrian Vanzyl of the security firm Seclarity comments: "So you are in effect breaking into each of those systems as you follow this person back. Are you legally liable for that? It's a very, very good question." And Dorothy Denning, professor of defense analysis at the Naval Postgraduate School, warns: "We've seen worms that have had major impact like causing delays in airline schedules, shutting down ATM machines, 911 systems and so on. Putting any kind of worm out there would be dangerous." (AP/San Jose Mercury News 18 Jun 2004)

Category 27.7 *Anti-malware technology*

2004-11-30 **virus throttling HP Hewlett Packard artificial intelligence AI slowing spread worms**

NewsScan;

'VIRUS-THROTTLE' SOFTWARE FROM HP

Software engineers at Hewlett-Packard are developing "virus-throttling" software to slow the spread of viruses and worms on the Internet by identifying suspicious behavior. HP chief technology officer Tony Redmond says, "Any worm or virus that depends on its ability to spread itself will be hurt by this technology." Alan Paller, director of research at the SANS Institute, says the overall idea "makes sense," and adds, "It's an arms race, not a simple war. I've been hearing people talk about the notion of throttling for a long time, and it's a spectacular idea if HP can get it to work." (Washington Post 30 Nov 2004)

Category 27.7 *Anti-malware technology*

2005-01-06 **Microsoft anti-spyware tool download antivirus viruses malware Microsoft McAfee Symantec**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=7260250

MICROSOFT LAUNCHES ANTISPYWARE TOOL

Microsoft this week began offering a test version of an antispyware application for download. The company had been promising such a tool for some time, and it will debut an antivirus tool next week for cleaning viruses and other malware from computers. A spokesperson for Microsoft also said it will begin offering a service called "A1" that will provide users with updates to these tools. Microsoft has been working to improve the security standards of its products, and the company's new tools represent its extension of those efforts into the software security market currently led by companies including McAfee and Symantec. Shares of both of those companies' stock fell sharply on the news of Microsoft's new security tools.

Category 27.7 *Anti-malware technology*

2005-01-14 **Microsoft anti-virus malware Stephen Cobb Chey Cobb**

NewsScan;

SAFE & SOUND IN THE CYBER AGE

"Microsoft the Security Company?"
by Stephen Cobb and Chey Cobb

Ever wonder why car companies don't make tires? A new Porsche doesn't come with Porsche tires even though Porsche engineers are some of the smartest in the world. We recently bought an almost-new Nissan and it came with the original tires, made by Goodyear. Of course, there are close relationships between car companies and tire companies, and they all have to work together on a variety of constantly evolving standards to make sure that the rubber that meets the roads fits the wheels on the wagon, so to speak. What has this got to do with computer security? Some alert NewsScan readers will have guessed already: Microsoft has planted its feet firmly in the computer security business. Now think of Microsoft as the GM of computing (actually a closer approximation of Microsoft's position in the IT world would be a mega-GM that had absorbed Ford, Toyota, Honda, and Daimler Chrysler). In other words, Microsoft makes most of the world's operating system software and most of the world's application software, which together make up the "cars" we are talking about. The safety of those cars, the rubber on the road in our analogy, is currently entrusted to a wide range of companies, big and small, companies like Symantec, Computer Associates, McAfee, Trend Micro, ZoneAlarm, Sygate, Grisoft, et al. These companies make their money selling products that help us to use Microsoft's products without skidding, crashing, or otherwise going off the virtual highway. For the most part they manage to perform this function without negatively impacting performance or the usability of our systems, while constantly evolving to meet new threats, many of which arise from defects in the very car they ride on, Microsoft's Windows OS and Office applications. However, through a series of recent announcements, Microsoft has indicated that it would like a slice of the revenue these security companies earn from protecting users of Microsoft products. Some Wall Street analysts have declared that this is a good move for Microsoft, and bad news for all those security companies that will lose market share to Microsoft. Given the slavish, sheep-like manner in which some investors follow the words of Wall Street analysts, it could indeed be good news for Microsoft, a sort of self-fulfilling investment prophecy, until the world wakes up to what a bad idea it is for Microsoft to make the tires for its cars. The last time Microsoft tried this, the results, for users, were dismal. Of course, these days it is hard to find a Wall Street analyst with a memory longer than the last four quarters, so you probably won't see many references to Microsoft's 1993 vintage Anti-Virus for DOS in current discussions of Microsoft's security ventures (but you can find a very detailed critique of the product, written about ten years ago by the late Yisrael Radai of the Hebrew University of Jerusalem, at cobb.com/pclan, or just Google "MSAV"). We would like to quote from the first paragraph of this review: "The very fact that such software [Microsoft AV] is supplied with DOS makes it likely that it will become one of the most widely used AV packages in the world and the de facto standard, regardless of its quality. Precisely for this reason, it will be specifically targeted by virus writers. If there are any weaknesses whatsoever in the software, they will be ruthlessly exploited by these people." In fact, Microsoft's implementation of anti-virus back then was so bad it never gained traction in the market place, but that does not undermine the serious implications of Mr. Radai's very astute observations. During the last ten years Microsoft has become more effective at forcing its software on users -- flaws and all (you will know this if you have ever tried to remove Internet Explorer from your Windows computer). Of course, today's malicious code writers frequently target products by Symantec, McAfee, et al. But the very fact that there is still an "et al." provides a depth of protection that will be eroded by any further expansion of Microsoft into the security arena. Perhaps the best outcome will be a repeat of the Firefox phenomenon, in which increasingly sophisticated users decide that the best way to deal with systemic security flaws in Microsoft's browser is to use a different browser. This has already produced a significant decline in market share for Internet Explorer. Heck, with Apple now selling a very powerful Mac for less than $500, complete with cool applications like Garage Band and Appleworks, some people may decide to drive the Internet highway in a completely different vehicle, on tires of their own choosing. [Chey Cobb, CISSP, wrote "Network Security for Dummies" and has provided computer security advice to numerous intelligence agencies. Her e-mail address is chey at soteira dot org. Stephen Cobb, CISSP, wrote "Privacy for Business" and helped launch several successful security companies. He can be reached as scobb at cobb dot com.]

Category 27.7 *Anti-malware technology*

2005-02-08 **Microsoft acquire antivirus maker Sybari Software viruses worms threats security Romanian company GeCAD Software Giant Software Company business technology**

EDUPAGE; http://www.nytimes.com/2005/02/09/technology/09soft.html

MICROSOFT TO ACQUIRE ANTIVIRUS MAKER

Microsoft has announced plans to acquire privately held Sybari Software, maker of software that protects against viruses, worms, and other threats. Microsoft has purchased other companies as part of its efforts to increase security, including a Romanian antivirus company, GeCAD Software, in 2003 and antispyware maker Giant Software Company in December of last year. Mike Nash, corporate vice president in Microsoft's security business and technology unit, said that with the latest purchase, Microsoft will begin offering stand-alone antivirus products. He said the company would soon offer a product based on Sybari technology and geared toward business customers. Other products designed to protect PCs from Web-based attacks will follow, though Nash did not provide a time frame for those applications.

Category 27.7 *Anti-malware technology*

2005-02-16 **Bill Gates IE anti-spyware conference security Microsoft Internet Explorer browser flaws operating systems**

EDUPAGE; http://online.wsj.com/article/0,,SB110848565696255359,00.html

GATES PROMISES NEW IE, FREE ANTISPYWARE

Speaking at a computer-security conference in San Francisco, Microsoft Chairman Bill Gates outlined a number of steps the company will take to address growing security concerns over its products. This summer, Microsoft will release a test version of Internet Explorer 7, the first major update of its browser in four years. Microsoft's browser has been the target of strong criticism for its security flaws. Gates said IE 7 will include antispyware tools for no extra cost, though other officials from Microsoft said the company would offer a paid subscription service to help consumers "manage" antispyware efforts. Gates also said the company would offer a range of antivirus products by the end of the year, which is later than many analysts had expected. Officials from competing computer-security companies said Microsoft's offering similar products by itself is not a source of great concern; rather, it is Microsoft's ability to bundle such tools with its operating systems that worries them. Gregor Freund, chief technology officer at Check Point Software, said if Microsoft bundles spyware with Windows, it is "playing a game that no one else can play." Wall Street Journal, 16 February 2005 (sub. req'd)

Category 27.7 *Anti-malware technology*

2005-04-26 **denial of service software quality assurance QS antivirus signature file endless CPU loop reboot update**

RISKS 23 85

MAJOR DAMAGE CAUSED BY BAD UPDATE FILE FOR TRENDMICRO ANTIVIRUS

TrendMicro released a defective antivirus update file on 23 Apr 2005 that was picked up automatically by many users in Japan. The bad file caused a CPU loop that consumed 100% of the processor time on Windows XP SP2 and Windows 2003 Server systems. Effects reported to RISKS by Chiaki Ishikawa included (as examples of many others)

- JR railway reservation division could not check the reservation status (fed via network to PCs?) and so diverted (telephone) inquiring customers to manned counters at railway stations;

- Kyodo wire service could not send out automatic wire service news for a few hours, and so resorted to send out important news via FAX (I believe that the initial news articles from Kyodo was sent in this manner);

- Osaka subway system saw its computer to distribute accident information to its stations failed to reboot; and

- Toyama city's election committee could not handle advance voting for its mayoral and city alderman elections on their computer and had to resort to manual processing.

Category 27.7 *Anti-malware technology*

2005-06-20 **hacker security tools attacked software vulnerability Symantec F-Secure CheckPoint**

DHS IAIP Daily;
http://news.com.com/Security+tools+face+increased+attack/210 0−1002_3−5754773.html?tag=nefd.top

SECURITY TOOLS FACE INCREASED ATTACK ACCORDING TO RESEARCH GROUP

As the pool of easily exploitable Windows security bugs dries up, hackers are looking for holes in security software to break into PCs, Yankee Group analysts said in a research paper published Monday, June 20. According to the Yankee Group, software makers of ubiquitous antivirus products have not yet been forced to acknowledge and fix potential problems in their code. Microsoft's Windows operating system has been a favorite target of hackers, but new security flaws are being discovered in security products at a faster rate than in Microsoft's products, the analysts wrote. Symantec, F-Secure and CheckPoint Software Technologies are among the vendors that have seen a rise in the number of security issues that affect their products in the past years and the Yankee Group predicts a "rising tide" of vulnerabilities will soon be found in security products. Yankee Group findings: http://www.yankeegroup.com/public/news_releases/news_release_detail.jsp?ID=PressReleases/news_06202005_FearandLoathing_P R.htm

---

Category 27.7 *Anti-malware technology*

2005-10-19 **Rootkit professional commercialization worm evade antivirus scanners StillSecure intrusion vulnerability network applications**

DHS IAIP Daily; http://www.vnunet.com/vnunet/news/2144149/rootkits−turn−prof essional

ROOTKIT CREATORS TURN PROFESSIONAL

Security experts are reporting a surge in the level of professionalism and commercialization in the creation of rootkits, a tool that helps worm authors slip past malware detection tools. Antivirus vendor F-Secure has reported that it has detected a new rootkit designed to bypass detection by most of the modern rootkit detection engines. Traditionally a rootkit would be designed to evade only one security product, such as Symantec's or F-Secure's antivirus scanners. Allen Schimel, chief strategy officer at StillSecure, a developer of intrusion detection, vulnerability management, and network access control applications, says "These rootkits just cranked it up a notch in their ability to evade multiple antivirus products." Schimel also warns that if these tools are effective in penetrating a computer's defenses, more worm authors are likely to start using them. The version of the rootkit detected by F-Secure is called Golden Hacker Defender.

Category 27.7 *Anti-malware technology*

2006-02-01 **technology companies cooperation anti-spyware CSA Labs McAfee Symantec Thompson Cyber Security Labs Trend Micro**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4669304.stm 23

FIVE COMPANIES COOPERATE AGAINST SPYWARE

A group of computer security companies is cooperating on an initiative to help consumers combat the growing problem of spyware, which is estimated to be increasing by 50 to 100 percent per year. ICSA Labs, McAfee, Symantec, Thompson Cyber Security Labs, and Trend Micro will initially offer tools that will help users identify spyware on their systems and effectively remove it. That effort will involve developing a common naming scheme for malicious programs and a coordination of various removal tools. Later, the five members of the group will work on tools that can help users avoid spyware in the first place. A related effort called Stop Badware was announced recently by Google, Sun Microsystems, the Berkman Center for Internet and Society, and the Oxford Internet Institute.

Category 27.7 *Anti-malware technology*

2006-03-06 **Internet browser safe surfing MIT SiteAdvisor color-coded security rating**

DHS IAIP Daily; http://www.smh.com.au/news/breaking/new−safety−net−for−web−s urfers/2006/03/06/1141493583941.html 23

NEW SAFETY NET FOR WEB SURFERS.

A fresh approach to "safe surfing" has been dreamt up by a group of Massachusetts Institute of Technology engineers involved in a crusade to make the Internet a safer place for their friends and families. The result of their labors is a product called SiteAdvisor which labels particular Websites with a color-coded security rating to help users identify those that might contain spyware, spam, viruses, and online scams. The millions of Websites on the Internet are trawled using sophisticated computer "robots" that can intelligently analyze the safety of a given destination. The tool then presents its findings alongside search engines such as Google, Yahoo! or MSN and labels results as either green, yellow or red. SiteAdvisor: http://www.siteadvisor.com/preview/

Category 27.7 *Anti-malware technology*

2006-03-13 **McAfee antivirus update DAT programming error file deletion update issued**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/story/0,10801,109525,00.html?SKC=security−109525 23

MCAFEE ANTIVIRUS UPDATE WREAKS HAVOC.

A faulty antivirus update from McAfee Inc. that mistakenly identified hundreds of programs as a Windows virus has resulted in some companies accidentally deleting significant amounts of data from affected computers. The McAfee update (DAT 4715) released on Friday, March 10, was designed to protect computers against the W95/CTX virus. But because of a programming error, the update also incorrectly identified, renamed and quarantined hundreds of legitimate executables. For companies that had configured their McAfee antivirus program to automatically delete bad files, the error resulted in the loss of hundreds, and in some cases even thousands, of files on systems in which the update had been installed, said Johannes Ullrich, chief technology officer at the SANS Internet Storm Center in Bethesda, MD. McAfee released a new patch (DAT 4716) updating the earlier one, five hours later.

Category 27.7 *Anti-malware technology*

2006-03-14 **antivirus false positive quarantine delete system files products patch**

RISKS; news.com http://tinyurl.com/jtaht 24 20

McAFEE ANTIVIRUS ATTACKS SYSTEM FILES & MICROSOFT OFFICE

According to McAfee spokesperson Joe Telafici, speaking to CNET News.com writer Joris Evers, >At about 1 p.m. PST [on March 10, 2006] we started getting reports that people were seeing an unusual number of W95/CTX infections in their environment," Telafici said. "Files that we did identify would probably be deleted or quarantined, depending on your settings."< Evers continued, "McAfee's antivirus software detected Excel.exe and Graph.exe, two Microsoft Office components, as well as other software, including AdobeUpdateManager.exe, an application installed alongside Adobe products that deals with software updates, Telafici said. . . . The problem occurred with virus definition file 4715, which was released at about 10:45 a.m. on Friday as part of McAfee's daily update cycle. The repaired, emergency-definition file 4716 was pushed out at about 3:30 p.m."

[MK adds: Hmm, many people have been arguing for years that MS products are malware. . . .]

Category 27.7 *Anti-malware technology*

2006-03-30 **McAfee VirusScan buffer overflow vulnerability system compromise boundary error solution update**

DHS IAIP Daily; http://secunia.com/advisories/19451/ 23

MCAFEE VIRUSSCAN DUNZIP32.DLL BUFFER OVERFLOW VULNERABILITY.

A vulnerability has been discovered in McAfee VirusScan, which potentially can be exploited to compromise a user's system. Analysis: The vulnerability is caused due to a boundary error in a 3rd-party compression library (DUNZIP32.dll) when processing virus definition files. This can be exploited to cause a buffer overflow via a specially crafted definition file. Affected software: McAfee SecurityCenter 6.x; McAfee VirusScan 10.x. Solution: Update to the fixed version of DUNZIP32.dll via online update.

Category 27.7 *Anti-malware technology*

2006-04-21 **Symantec Scan Engine multiple vulnerability solution update**

DHS IAIP Daily; http://www.securityfocus.com/archive/1/431734 23

SYMANTEC SCAN ENGINE MULTIPLE VULNERABILITIES.

Three vulnerabilities have been discovered in the Symantec Scan Engine. The Scan Engine is a TCP/IP server and programming interface that enables third parties to incorporate support for Symantec content scanning technologies into their proprietary applications. This gateway-level product should not be confused with Symantec's desktop product. Analysis: The Symantec Scan Engine fails to properly authenticate Web-based user logins. Anyone with knowledge of the underlying communication mechanism can control the Scan Engine server. Symantec Scan Engine uses a static private DSA key for SSL communications. This key cannot be changed by end users and is easily extracted. This opens the product to a potential man-in-the-middle attack. Products affected: Symantec Scan Engine 5.0. Solution: Symantec Engineers have verified these issues and have added fixes to the latest product update (5.1). Symantec strongly recommends all customers immediately apply the latest updates for their supported product versions to protect against these types of threats. Symantec Scan Engine updates are available through the Platinum Support Website for Platinum customers or through the FileConnect-Electronic Software Distribution Website for all licensed users. Platinum Support Website: https://www-secure.symantec.com/platinum/login.html FileConnect: https://fileconnect.symantec.com/licenselogin.jsp Symantec April 21, 2006 advisory: http://www.symantec.com/avcenter/security/Content/2006.04.21 .html

---

Category 27.7 *Anti-malware technology*

2006-05-09 **Sophos anti-virus cabinet file handling memory corruption vulnerability solution update**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2006/1730 23

SOPHOS ANTI-VIRUS PRODUCTS CABINET FILE HANDLING MEMORY CORRUPTION VULNERABILITY.

A vulnerability has been identified in various Sophos Anti-Virus products, which could be exploited by attackers or malware to take complete control of an affected system. Analysis: This flaw is due to a heap corruption error within the unpacking of Microsoft Cabinet (".CAB") files containing invalid folder count values within the CAB header, which could be exploited by attackers to execute arbitrary commands and compromise a vulnerable system by sending an e-mail containing a malicious CAB file to a machine being protected by an affected Anti-Virus product. Refer to source advisory for a complete list of vulnerable products. Solution: Apply patches: http://www.sophos.com/support/knowledgebase/article/4934.html

28.1 Spyware, Web bugs & cookies

Category 28.1 *Spyware, Web bugs & cookies*

1997-01-21 **Cookies privacy profiling permission consumer browser**

RISKS 18 78

Some Web sites pass cookies to the next URL which can include sensitive information.

Category 28.1 *Spyware, Web bugs & cookies*

1998-03-17 **cookies Web privacy**

EDUPAGE

U.S. DOE SAYS COOKIES AREN'T BAD FOR YOU
The U.S. Department of Energy's Computer Incident Advisory Capability has issued an information bulletin stating that privacy advocates' fears over the use of cookies — a popular technique for tracking Web site visitors — are unfounded. The claims that Web cookies may be used to gather information on "passwords, credit card numbers, and a list of the software on your computer" is not even "close to the truth," according to the bulletin. In fact, information that is gathered via cookies — usually a user's numerical Internet address, browser type and operating system — can also be recorded in a Web server's log files. "Cookies just make it easier. [A server] cannot find out your name or e-mail address, or anything about your computer using cookies," says the bulletin. (TechWeb 16 Mar 98)

[MK comment: "mostly harmless" à la Douglas Adams?]

Category 28.1 *Spyware, Web bugs & cookies*

1998-06-28 **cookies privacy Web**

EDUPAGE

COOKIE-KILLER
Engineers at Luckman Interactive in Los Angeles have come up with Anonymous Cookie software that finds cookies — data stored by Web sites on a visitor's computer so that it can be accessed the next time that site is visited — and hides them, so that the user can surf the Web incognito. The program can also be deactivated with the click of a mouse, restoring preexisting cookies. The program is free and can be downloaded from the Luckman Interactive site. (Discover Jul 98)
http://www.luckman.com/

Category 28.1 *Spyware, Web bugs & cookies*

1999-11-24 **banner advertisements data capture privacy surveillance Web Internet license software freeware spyware**

ZDNet http://www.zdnet.co.uk/news/1999/46/ns-11692.html

Conducent <http://www.conducent.com> pays software developers to include modules in their programs that display banner ads. A contributor to the RISKS Forum, Bill Royds, reported that the modules initiate a TCP/IP connection to Conducent computers and report on which program is running and other information about the user's system such as IP address. In addition, the reporting module responds to connection failure (e.g., through firewall restrictions) by initiating a storm of connection attempts (10 per second). Conducent responded dismissively that their licenses are clear and said, "It is up to the user to take the time to read the installation notes wherein the advertising-supported version of the software is explained comprehensively."

Category 28.1 *Spyware, Web bugs & cookies*

1999-11-30 **Trojan program privacy invasion reporting TCP/IP Internet browsing statistics visit sites advertising controversy arguments criticism spyware**

AP

Comet Systems Inc's cute cartoon cursors were downloaded by millions of people, many of them children. However, the free software turned out to be a Trojan: the modified programs initiated TCP/IP communications through the users' Internet connections and reported on which sites were being visited by each copy of the programs when the users went to any of 60,000 sites providing links to the cursor programs. Purpose: gathering statistics about Web usage patterns. Company officials argued that there were no links between the serial numbers and any identifying information about the users.

Category 28.1 *Spyware, Web bugs & cookies*

1999-12-06 **privacy cookies Web e-mail Trojan vulnerability tracking covert**

USA Today

Computer scientist Richard S. Smith (famous in part for helping to unmask David L. Smith, the author of the Melissa virus) discovered that popular e-mail clients such as MS-Outlook and Netscape Messenger allow anyone to send a victim a concealed cookie via e-mail that will then allow tracking through the Web as the cookie-infested user browses various sites. Privacy groups including the Center for Media Education, the Consumer Federation of America, the Electronic Frontier Foundation, the Electronic Privacy Information Center, Junkbusters, Privacy International, and Ralph Nader's Consumer Project on Technology all protested the covert use of this technology. Microsoft and Netscape announced that they would plug this security hole in their products.

Category 28.1 *Spyware, Web bugs & cookies*

2000-08-31 **privacy surveillance covert channel data leakage confidentiality monitoring**

NewsScan;
http://www.sjmercury.com/svtech/news/breaking/merc/docs/016246.htm

PRIVACY FOUNDATION SLAMS "WEB BUGS"
The Denver-based Privacy Foundation . . . [said] that documents created with software that uses a hotlink shortcut to include images stored on a remote computer could be rigged to "phone home" to another computer and report where and how often a document is read. The technique, known as a "Web bug," is used in Microsoft word processing and spreadsheet applications, but is also found in other companies' software that uses automatic links to Web pages. "Because a linked Web image must be fetched from a remote Web server, the server is in a position to track when a Word document is opened and possibly by whom," says Privacy Foundation chief technology officer Richard Smith, who adds that there is no evidence anyone has exploited the arrangement. Web bugs can be as small as a single pixel, making them nearly invisible, says Smith. "In most cases, the reader of a particular document will not know that the document is bugged, or that the Web bug is surreptitiously sending identifying information back through the Internet." Microsoft program manager Eric Schultze says, "These [concerns] are not in any way specific to Microsoft or any other vendor, they are Internet issues. This could happen on any Web-enabled application or on any vendor's operating system." (Reuters/San Jose Mercury News 31 Aug 2000)

Category 28.1 *Spyware, Web bugs & cookies*

2001-02-01 **spyware prohibition control privacy consumer software**

NewsScan

SPYWARE SECURITY BILL RESURFACES
U.S. Senator John Edwards (D-NC) has reintroduced legislation that would protect the privacy of individuals from software that monitors their surfing habits. The Spyware Control and Privacy Protection Act was originally filed in October 2000, but Congress failed to take action on it. The Act mandates that companies that use codes to track the activities of Internet users would have to notify Web site visitors of their surveillance actions in plain language. Businesses that gather data would be required to let users know what information has been gathered, provide a way to correct errors, and safeguard the data against unauthorized access by hackers. (InfoWorld.com 31 Jan 2001)
http://www.infoworld.com/articles/hn/xml/01/01/31/010131hnedwards.xml?p=br&s=5

Category 28.1 *Spyware, Web bugs & cookies*

2001-06-15 **spyware Java covert installation unauthorized software Internet server firewall end-user license agreement EULA**

RISKS 21 49

Bill Tolle reported in RISKS on covert installation of spyware. Mr Tolle accepted an offer for rebates from < www.ebates.com > and discovered that the service had installed "Javarun.exe" on his system; "the program was trying to access the Internet and was also trying to act as a server for the Internet. Fortunately, the firewall caught it and stopped it." The covert installation was apparently the result of his having forgotten to disable Java in Internet Explorer while he was signing up for the service. Nowhere in the end-user license agreement was there any indication that a subscription would involve installation of such spyware.

Category 28.1 *Spyware, Web bugs & cookies*

2002-04-06 **HTML e-mail Web bugs spyware firewalls browsers configuration adware cookies**

RISKS 22 03

Stefanie Olsen, writing for CNET News, noted the rising concern over the use of HTML e-mail containing spyware such as Web bugs -- 1-pixel invisible images that reside on Web sites where counters keep track of who is downloading them, thus keeping a record of the success of spam campaigns.

[MK comment: most personal firewalls (e.g., ZoneAlarm) and some browsers (e.g., Opera) allow configuration that stops downloads of materials from outside a target Web site, thus interfering with adware and spyware.]

Category 28.1 *Spyware, Web bugs & cookies*

2002-06-27 **spyware communication firewall instant messaging chat**

RISKS 22 13

Michael Weiner reported, "Since I installed MS Messenger 4.6 (4.6.0082) on my machine, my firewall is going wild: In addition to numerous Microsoft sites, Messenger is contacting the following sites each time I log in: expedia.com, xp.mcafee.com, carpoint.msn.com and port-64-1956779-zzt0prespect.devices.datareturn.net. No way to know what information MS Messenger is transmitting to these sites, I did not find any meaningful information on it on the Microsoft website..."

Category 28.1 *Spyware, Web bugs & cookies*

2002-10-14 **P3P Platform for Privacy Preferences W3C standards proprietary implementation browsers developers**

NewsScan

THE COLORS OF PRIVACY
Be careful what you ask for: you may just get it (more or less). Privacy advocates put continuous pressure on Microsoft to pay careful attention to privacy concerns, but many Web publishers are now unhappy with Microsoft's implementation of the Internet Explorer 6.0 browser, which seeks to discourage third-party tracking abuses by blocking third-party "cookies" unless the third party's privacy policy meets strict standards. Third parties are required to put their policy into the P3P ("platform for privacy preferences") protocol specified by the World Wide Web Consortium, but there are vastly different levels of compliance with that standard, and there is worry that publishers will put a great deal of work into complying with Explorer's implementation of the standard, and then learn that Microsoft has decided to change the standard with the next software release. Carl Fischer of iVillage says, "Our legal department has been working on this for months. And Microsoft can just change its standards down the line. They're imposing a one-size-fits-all rule for hundreds of different privacy policies. Why should that be up to Microsoft?" (New York Times 14 Oct 2002)

Category 28.1 *Spyware, Web bugs & cookies*

2003-11-19 **Spyware UK ThreatLab Clearswift recording confidential data anti-spyware Ad-Ware Pest Patrol**

NewsScan

SPYWARE IN THE CROSSHAIRS
After several years of mounting concern, worries over "spyware," which surreptitiously deposits information-stealing software on computers, are coming to a head. Last summer, a corporate IT manager's nightmare came true when an e-mail sent to a British credit card and finance company carried a secret software program capable of recording confidential corporate data and sending it over the Net. "The good old days of script kiddies and geeks are well gone," says Pete Simpson, manager of the ThreatLab division of U.K. security firm Clearswift. "These are criminal gangs, and the motive is clearly profit." In response to the growing threat, legislation has been introduced in Congress that would outlaw both corporate spyware and the annoying kind that comes bundled with free software programs such as Kazaa and is used to deliver advertising. But in a report released Tuesday, the Center for Democracy and Technology argued against any legislation that specifically targets spyware, noting that most of the worst software-spying practices are already illegal. Rather, consumers would be better served by a broad-ranging privacy bill that would force all software programs to give clear notice when they are collecting information and give consumers the option to turn them off or easily uninstall them. Meanwhile, the Consortium of Anti-Spyware Technology Vendors, led by the creators of the spyware-battling Ad-Aware and Pest Patrol software programs, is developing standard definitions of "spyware," "adware," and other annoyances in an effort to present "best practices" recommendations to companies hoping to avoid being blocked by their software. (CNet News.com 19 Nov 2003)

Category 28.1 *Spyware, Web bugs & cookies*

2004-01-06 **anti spyware software AOL Earthlink**

NewsScan

AOL JOINS EARTHLINK IN OFFERING ANTI-SPYWARE SOFTWARE

America Online will soon start offering its customers anti-spyware software, following the lead of EarthLink, which is the only other major Internet service provider to provide its subscribers with software that automatically flags programs designed to secretly track users' Internet habits. Spyware usually finds its way onto a PC when users download file-sharing software or stumble onto certain Web sites. "Spyware is an electronic stalker that secretly watches the online activities of millions of Americans every day," says AOL executive VP David Gang. "Because spyware hides in the background and quietly attaches itself to other programs, most computer users don't even realize they have it on their machines." One EarthLink exec predicts that spyware eventually will outstrip computer viruses as an online scourge, because its motivation is rooted in a quest for profits rather than random malice. (Washington Post 6 Jan 2004)

Category 28.1 *Spyware, Web bugs & cookies*

2004-01-14 **spyware Earthlink prevention**

NewsBits; http://zdnet.com.com/2100-1104_2-5141073.html

EarthLink tool hunts down spyware

The company's Spy Audit software is intended to ferret out unwelcome programs that take up surreptitious residence on a computer's hard drive, typically when someone downloads freeware or shareware but also through e-mail and instant messaging. Those programs keep track of a computer user's online activity and can be difficult to locate and remove. Problems that arise from spyware's presence can range from the annoying --a barrage of pop-up ads--to the menacing, including the potential for data corruption and theft of personal information.

Category 28.1 *Spyware, Web bugs & cookies*

2004-02-04 **spyware insidious software detector Trojan horse SpyBan**

NewsScan

DOUBLE-AGENT SPYWARE

It turns out that at least one spyware program purporting to identify and delete unwanted advertising software actually installs its own spyware software on the unsuspecting user's computer. SpyBan has been singled out for such nefarious behavior by several competing anti-spyware companies: "I classified SpyBan as a Trojan Horse, since it gives the impression that it will protect your privacy, but does the opposite — it installs spyware," says a spokesman for Sweden-based Kephyr.com. The software allegedly leaves behind a program called Look2Me, which has been identified by Symantec as a spyware application: "Look2Me is a spyware program that monitors visited Web sites and submits the logged information to a server." The SpyBan Web site was shut down after reporters started snooping into its activities, but a trace of the company's domain name indicated the site was hosted at the same address as NicTech Networks. Experts say spyware and adware software can be difficult to track down because it's designed to "hide" on the user's PC. "I doubt anyone knows precisely what these things do, apart from the authors," says a researcher for PestPatrol, a legitimate anti-spyware outfit. "They are really complex. Viruses are easy compared to these things." (CNet News.com 4 Feb 2004)

Category 28.1 *Spyware, Web bugs & cookies*

2004-03-02 **anti-spyware bill SPYBLOCK**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A23307-2004Mar2.html

SENATE BILL TARGETS SPYWARE

U.S. Senators Ron Wyden (D-Ore.), Conrad Burns (R-Mont.) and Barbara Boxer (D-Calif.) are backing a bill dubbed the "SPYBLOCK" Act, which would make it illegal to use the Internet to install software on people's computers without their consent, and would require companies that offer software downloads to provide more information about what the programs do and what information they collect. The bill also would require ads generated by spyware or adware programs to be clearly labeled as such. "Computer users should have the security of knowing their privacy isn't being violated by software parasites that have secretly burrowed into their hard drive," says Wyden. Spyware has been around for years, but as its sneaky code has reached out to touch more users, the tide of public sentiment has now turned against it. "The major concern here is user control and transparency," says Ari Schwartz, associate director for the Center for Democracy and Technology. "We've found that many consumers do not understand what they're getting themselves into when they download software." Some skeptics say this latest effort is likely to be every bit as effective as the preceding CAN-SPAM Act, which many computer experts say has done little to curb the deluge of spam flooding consumers' in-boxes. "If you apply the mailbox test, the spam law hasn't had a significant effect. It would be nice to see the spam law working as intended before we say we want to follow the same route with spyware," says one attorney. (Washington Post 2 Mar 2004)

Category 28.1 *Spyware, Web bugs & cookies*

2004-03-04 **legislation US Senator spyware insidious software SPYBLOCK act law**

NIPC/DHS

March 02, Washington Post — Senators try to smoke out spyware.

Three U.S. senators are tackling the growing problem of "spyware," software programs that track what people do online, alter their Web browser settings and turn their computers into unwitting Internet advertising generators. The "SPYBLOCK" Act, which was introduced late last week, would make it illegal to use the Internet to install software on people's computers without their consent, and require companies that offer software downloads to provide more disclosure about what the programs do and what information they collect. The bill also would require Internet ads generated by the software to be clearly labeled. The bill would allow states to sue violators in federal court and would call on the Federal Trade Commission to impose fines and civil penalties under consumer protection laws. The bill probably will not cut down on the worst kinds of spyware -- programs that exploit computer security flaws to hijack Internet connections or install "dialer programs" that force the computer to call expensive online 1-900 adult services -- said Stewart Baker, an attorney in Washington, DC. In that sense, Baker said, it is a lot like the CAN-SPAM Act, which many experts said has done little to combat the problem of unsolicited bulk e-mail since it became law in January. The commission is scheduled to hold a public workshop on spyware, adware and other software on April 19.

Category 28.1 *Spyware, Web bugs & cookies*

2004-03-25 **spyware insidious software spam e-mail definition US Senator Kazaa**

NIPC/DHS

March 23, Reuters — Senators struggle to define computer spyware.

Programs that secretly track computer users' activities are becoming an online scourge rivaling "spam" e-mail and should be outlawed before they prompt consumers to abandon the Internet, members of the Senate communications subcommittee said Tuesday, March 23. But a bill sponsored by committee members will need to define the problem precisely to avoid outlawing pop-up ads and other annoying but essentially harmless technologies, consumer and business advocates said. Like the congressional debate about "spam" e-mail last year, much rests on the definition of what constitutes legitimate marketing activity and what should be outlawed. Some online advertisers and song-swapping networks like Kazaa place programs on users' computers to monitor their activity, or harness their processors for other activities. Other programs secretly track users' keystrokes to lift passwords and credit-card numbers, or sell "fixes" for software problems they create. A bill sponsored by Sen. Conrad Burns (R-MT) would require companies to obtain permission before installing a piece of software on a consumer's computer, and provide an easy way for the consumer to remove the software if he wished.

Category 28.1 *Spyware, Web bugs & cookies*

2004-04-13 **anti-spyware insidious software Utah law invasion privacy**

NewsScan

CHALLENGE TO UTAH'S NEW ANTI-SPYWARE LAW

A new Utah law called the Spyware Control Act (banning the practice of imposing pop-up ads on Internet users as they surf the Web) is being challenged in a federal lawsuit filed by the New York advertising company WhenU.com Inc., which argues that the law violates a constitutionally protected right to advertise. WhenU provides users with free software such as games and screen savers that come with a separate program, SaveNow, that tracks Web traffic and matches a user's surfing habits with particular advertisers. WhenU says its software is installed only with permission and doesn't invade privacy. (AP/San Jose Mercury News 13 Apr 2004)

Category 28.1 *Spyware, Web bugs & cookies*

2004-04-13 **home user PC infested spyware insidious software**

DHS IAIP Daily; http://news.bbc.co.uk/2/hi/technology/3633167.stm

April 16, BBC News (UK) — PCs 'infested' with spy programs.

Internet provider EarthLink says it uncovered 29.5 million examples of spyware on over one million computers scanned between January and March. These are parasite programs sometimes come attached to software downloaded from the Web. The details are often included in the license agreement small print that most users click through without reading. But sometimes they do not even need your permission to download, but just bury themselves on a hard drive as you browse the Internet. EarthLink said the most common type of spyware it found was adware. These are programs that displays ads on an infected computer and also sends data about surfing habits. But it also found examples of more insidious spyware. "It's disturbing that over 300,000 of the more serious system monitors and Trojans were uncovered," said Matt Cobb of EarthLink. System monitors can surreptitiously watch what you do, steal personal information and despatch it across the web, while Trojans can allow malicious hackers to get access to a computer and steal information.

Category 28.1 *Spyware, Web bugs & cookies*

2004-04-18 **spyware targetted Federal Trade Commission FTC**

NewsScan

FTC TARGETS SPYWARE

The Federal Trade Commission, which championed the anti-spam legislation recently enacted by Congress, now has another Internet scourge in its sights: spyware. The agency is sponsoring a workshop today to study technical and regulatory responses to spyware, but officials caution that legislation is unlikely to be passed this year. Adware (the most common type of spyware) usually piggybacks on other programs -- most notably music file-sharing or screen-saver software -- and then tracks users' Web surfing habits, relaying that information to ad companies that then bombard the user with pop-up ads. More malicious versions of spyware track keystrokes in order to steal credit card information or identity. House and Senate bills would require users' clear consent before downloads, but FTC bureau director Howard Beales says such approaches could prove cumbersome: "The question is whether there's a way to draw a workable line. If you download a set of (updates) for Windows, it comes with a bunch of different programs. You don't want to have to go through this every time." (USA Today 18 Apr 2004)

Category 28.1 *Spyware, Web bugs & cookies*

2004-04-19 **spyware legislation slowed market-based solution insidious software user unaware**

NewsScan

A GO-SLOW APPROACH TO SPYWARE LEGISLATION

Spyware (the generic term for software that is surreptitiously downloaded onto PCs when users are engaged in some activity such as instant messaging or surfing for music or games) comes in two major varieties: the relatively innocuous "adware" that places advertisements on people's computers, and the more insidious kind that capture user keystrokes in order to steal passwords or other private information. The Internet security firm McAfee says the number of "potentially unwanted programs" on its customers' computers grew from 643,000 in September 2003 to more than 2.5 million in March. Still, Commissioner Mozelle Thompson, a member of the Federal Trade Commission, warns against trying to solve the problem with hurried and ill-conceived legislation: "There are some kinds of practices that we may consider unfair or deceptive that we already have existing power to pursue." His alternate solution is for technology companies to develop standards for downloads that would distinguish them from spyware. Marc Rotenberg of the Electronic Privacy Information Center scoffs: "To expect that market-based solutions are going to protect the consumers, I think, is to misunderstand the problem." (Washington Post 19 Apr 2004)

Category 28.1 *Spyware, Web bugs & cookies*

2004-04-19 **Federak Trade Commission FTC industry solutions spyware**

DHS IAIP Daily; http://www.esecurityplanet.com/trends/article.php/3342471

April 19, eSecurity Planet — FTC urges industry solutions to spyware.

The Federal Trade Commission (FTC) says the solution to the invasive programs generally known as spyware is more likely to be found in better technology solutions and intensive consumer education than in either state or federal legislation. Spyware is vaguely defined and often confused by consumers with adware, which are usually legal and legitimate applications. Consumer and privacy advocates attending Monday's FTC Spyware Workshop were concerned about the growing number of programs that often surreptitiously piggyback on downloaded files; they report back Internet traffic patterns to advertisers and generate unwanted popups. Even when consumers delete the downloaded file, spyware often remains and continues to monitor the user's browsing habits. FTC Commissioner Mozelle Thompson asked industry Internet provider leaders to produce a set of best practices for the use of adware, including disclosure statements to consumers regarding what they are about to download.

Category 28.1 *Spyware, Web bugs & cookies*

2004-05-13 **spyware state laws combating Utah New York California**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/articles/A24746−2004May 13.html

May 13, Washington Post — States speed up spyware race.

State lawmakers' eagerness to crack down on Internet "spyware" could force the federal government to move sooner than expected to pass its own law. Only one state--Utah--has an anti-spyware law, but New York and California both are considering proposals. If enough states pass similar laws, businesses say the resulting "patchwork" of conflicting statutes would be almost impossible to obey, adding further pressure on Congress to act. "If the states are busy writing laws and particularly if they're writing inconsistent laws or laws that strongly interfere with certain markets, that certainly would strengthen the case for federal legislation," said Howard Beales, the Federal Trade Commission's top consumer protection official. At an April FTC hearing on 13 spyware, witnesses testified that computer users often don't know how the programs got onto their machines or how to remove them. Any national spyware law probably would preempt various state laws, much like the federal Can-Spam Act preempted tougher anti-spam laws in California and Washington. Beales said that Congress should not let the threat of state laws goad it into passing a poorly written bill.

Category 28.1 *Spyware, Web bugs & cookies*

2004-05-20 **e-mail messages read received location DidTheyReadIt.com violating physical space freak people**

NewsScan

IF YOU SEND IT, WILL THEY READ IT?

DidTheyReadIt.com, a new service costing $50 a year, allows a sender of e-mail to secretly track that e-mail to see whether anyone opens it, how long the recipient keeps it open, how many times it was opened, and where geographically the recipient read it. The whole process is invisible to the person who receives the message. Mitchell Kertzman of the technology investment firm Hummer Winblad says the service "violates our electronic space in a way that's as uncomfortable as someone violating our physical space. Add this company to the long list of people who are making the Internet a less attractive place to live and work." Technology expert Esther Dyson predicts that the service "will freak people out," but Case Western Reserve University professor Youngjin Yoo thinks people will be of two minds: "You will want to know how others treat your e-mail messages even if you don't necessary want others to know how you are treating theirs."

Category 28.1 *Spyware, Web bugs & cookies*

2004-05-30 **spyware browser security add-in downloads scanning software anti-malware scanner pop-up blocker freeware**

WP http://www.washingtonpost.com/wp-dyn/articles/A89-2004May29.html

SPYWARE BLOCKING FROM YAHOO

Yahoo's free browser toolbar, "Anti-Spy," was announced in May 2004. Using technology from PestPatrol, the company founded by Bob Bales -- who was one of the founders of the original National Computer Security Association (NCSA) back in the late 1980s -- the software blocks spyware, provides for scanning and removal of spyware, and blocks popups. By late 2004, the product was in full production and available for IE in a free download from < http://toolbar.yahoo.com >.

Category 28.1 *Spyware, Web bugs & cookies*

2004-06-03 **Web bugs privacy e-mail confirmation permission surreptitious covert data leakage**

http://www.nytimes.com/2004/06/03/technology/circuits/03spyy.html

COMPANY ENABLES WEB BUGS IN E-MAIL

Users of DidTheyReadIt.com route their e-mail through that company's servers so that it can be converted to HTML equipped with Web bugs. The spyware-infested e-mail can then report to the sender whether a recipient has opened the message and for how long. Privacy advocates protested that the surreptitious nature of the service makes it unethical. The providers of the service said they don't care.

Category 28.1 *Spyware, Web bugs & cookies*

2004-08-23 **virus spyware combination Websurfing information leak webcam privacy**

DHS IAIP Daily; http://www.webuser.co.uk/news/57657.html

August 23, Webuser — Virus spies on surfers.

A new virus, Rbot-GR, that can spy on computer users through their webcam is circulating across the Internet. The Rbot-GR worm, which spreads through shared networks, gives hackers access to the hard drive and secret passwords, as well as the ability to spy on people in their homes and workplaces through their webcams or microphones. Graham Cluley, senior consultant for Sophos said "This takes hacking to a whole new level. If your computer is infected and you have a webcam plugged in, then everything you do in front of the computer can be seen and everything you say can be recorded." Sophos believes that the worm is evidence of a growing trend in spying on innocent computer owners and poorly protected businesses. Users are advised to keep their PC's protected against the latest threats with anti-virus software and firewalls, and unplug their webcam when not using it.

Category 28.1 *Spyware, Web bugs & cookies*

2004-09-02 **Microsoft Windows XP operating system Service Pack 2 SP2 spyware interference update**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/articles/A57501−2004Sep 2.html

September 02, Associated Press — Microsoft warns spyware could bungle update.

Microsoft is warning users of the Windows XP operating system to check for spyware before downloading the free massive security update, called Service Pack 2. Barry Goff, a group product manager at Microsoft, said some spyware could cause computers to freeze up upon installation of the update. Spyware, which typically piggybacks with downloaded software such as file-sharing programs, tracks behavior, triggers pop-up ads and can otherwise cause problems on computers. Microsoft recommends that users clean their PCs of spyware and back up their data before turning on the auto update feature that automatically downloads Service Pack 2 (SP2). People who download SP2 also may need to check whether legitimate programs, such as third-party security software, need to be updated. Research firm IDC estimates that about 260 million copies of Windows XP have been sold.

Category 28.1 *Spyware, Web bugs & cookies*

2004-09-08 **copyright anti-spyware bills legislation proposed intellectual property crime Justice Department**

NewsScan

COPYRIGHT, SPYWARE BILLS MOVE FORWARD

The House Judiciary Committee has approved two bills that would establish criminal penalties of up to three years in prison for those who install spyware on others' computers and for Internet users who copy and distribute large quantities of music or movies without permission. "We must not let Internet technologies become a haven for criminals," said Rep. Lamar Smith (R-Texas). The copyright bill includes provisions for training federal agents to investigate intellectual-property crimes and would set up a Justice Department program to education the public about copyright rules. Both bills now head to the House floor for consideration; the Senate approved similar legislation in June. (Reuters/New York Times 8 Sep 2004)

Category 28.1 *Spyware, Web bugs & cookies*

2004-10-12 **spyware FTC lawsuit prosecution Wallace popup windows privacy hacking**

NewsScan; http://news.com.com/From+spam+king+to+spy+master/2100-1032_3-5406348.html

SPYWARE IN FTC'S CROSSHAIRS

The Federal Trade Commission is launching an aggressive new strategy to prosecute "spyware" perpetrators, and last week filed a civil lawsuit against former spam-king Sanford Wallace and his companies, Seismic Entertainment Productions and SmartBot. Wallace, who was once dubbed "Spamford" for his earlier misdeeds, operates the PassItOn.com Web site, which requires visitors to click through multiple pop-up windows in order to exit. In an interview with CNet last year, Wallace defended his practice of collecting personal information from people who visited his site: "We don't violate anybody's privacy; everything is disclosed. We're giving something away for free in exchange for consumers' permission to use private information. It's no secret. Publishers Clearinghouse has been doing this type of thing for years." However, an FTC investigator says Wallace's actions go far beyond informationgathering, by changing the home page of her Internet Explorer browser and using programming code to pop open the CD drive in her computer while displaying a message saying, "If your cd-rom drive opens… you desperately need to rid your system of spyware pop-ups immediately." Of course, the site then offers to sell a product called Spy Deleter. Anti-spyware activist Ari Schwartz says the FTC has "built a good case. This fits into the kinds of cases where FTC could get their feet wet on this issue."

Category 28.1 *Spyware, Web bugs & cookies*

2004-10-18 **spyware adware proxy servers blocking installation prevention screening**

NewsScan; http://online.wsj.com/article/0 (sub req'd)

NEW SOLUTIONS TO SPYWARE INVASION

Two companies have just released software programs aimed at eliminating the scourge of spyware. Blue Coat Systems, which specializes in proxy servers, is enhancing its security service with spyware- and adware-blocking software. It estimates that its product can prevent 98% of such unwanted programs from being installed. Webroot Software boasts a similar success rate with its anti-spyware software, which is installed directly on users' PCs. These two new products are notable because, while there are many products on the market that can remove spyware and adware from users' PCs, these two prevent their installation in the first place. Meta Group analyst Peter Firstbrook predicts that what ultimately will evolve is a "layered" defense system that combines centralized screening tools plus desktop software, similar to what's happened in the antivirus software market.

Category 28.1 *Spyware, Web bugs & cookies*

2004-11-15 **cookies advertising web privacy service surfing history**

NewsScan; http://www.nytimes.com/2004/11/15/technology/15ecom.html

NEW AD SERVICE TRACKS SURFING HABITS, MAINTAINS PRIVACY

Tacoda, based in New York, is touting its new online marketing service, which directs ads to Web site visitors based on their surfing history. No personal information is sought or collected -- AudienceMatch simply traces the path of a single computer through its network of 60 Web sites, using a cookie. "This is different than what DoubleClick was trying to do," says Tacoda CEO David Morgan. "This system uses no personally identifiable information, and no data is shared between publishers. Privacy is one of the biggest issues that will drive the success of this." Tacoda's Web network comprises 60 publishers that are visited by some 100 million people monthly, or about 75% of the U.S. Internet audience. Morgan compares AudienceMatch to Google's AdSense program, which allows marketers to bid for the right to position their text messages next to stories that have a related "theme." With AudienceMatch, however, advertisers bid not on keywords, but on preset groups, like "gadget geeks," or "car buyers." Gartner analyst Denise Garcia says AudienceMatch "enables advertisers to reach a lot more people with targeted ads, which, for them, is the next big wave." (New York Times 15 Nov 2004)

Category 28.1 *Spyware, Web bugs & cookies*

2005-01-04 **online marketer halt spyware litigation Sanford Wallace FTC deceptive software secretly installed**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?&storyID=7235820

ONLINE MARKETER AGREES TO HALT SPYWARE DURING LITIGATION

Alleged spyware kingpin Sanford Wallace has agreed to stop distributing spyware pending the resolution of charges filed against him and two of his companies by the Federal Trade Commission (FTC). In October, the FTC charged Wallace with deceptive trade practices, saying that Wallace's companies, Seismic Entertainment Productions and SmartBot.Net, distributed software that was secretly installed on users' computers. The software would cause problems on computers where it was installed and would then display pop-up ads for programs to remove the spyware. Under an agreement filed with the U.S. District Court in New Hampshire, Wallace, who does not admit guilt, does agree to halt the practice of secretly installing spyware while the litigation is proceeding. Wallace and his companies are still allowed to display pop-up ads.

Category 28.1 *Spyware, Web bugs & cookies*

2005-01-07 **anti-spyware software Microsoft review evaluation beta-test**

RISKS 23 66

NEWS! SLADE DOESN'T SLAM SPYWARE DEFENSE!

Veteran reviewer Rob Slade reported his first impressions of the Microsoft Anti-Spyware beta version. After detailed information on his explorations and tests, he summarized his findings as follows: "At the moment, after a very quick test, I'd provisionally recommend the use of the MS/Giant antispyware program, at least in fairly restricted and manual mode. I'd be interested in hearing from others who have tested the real-time operations more extensively, and particularly from anyone who has tested the Spynet capabilities, and what information is returned thereby."

Category 28.1 *Spyware, Web bugs & cookies*

2005-01-07 **Microsoft anti-spyware Windows**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A54902-2005Jan6.html

MICROSOFT OFFERS ANTI-SPYWARE SOFTWARE

In a move indicating its increasing interest in the security market, Microsoft is giving away software designed to protect Windows users from spyware (programs that transmit information about the user without his or her knowledge). Industry analysts believe the company will eventually enter the market for computer security software, and George Kafkarkou of Computer Associates says that Microsoft's entry into the antispyware arena brings "validation" to that marketplace. (Washington Post 7 Jan 2005)

Category 28.1 *Spyware, Web bugs & cookies*

2005-04-29 **spyware installation lawsuit New York Attorney General Intermix Media state law violation**

EDUPAGE; http://www.nytimes.com/2005/04/29/nyregion/29internet.html

SPITZER FILES SUIT AGAINST MARKETING FIRM FOR SPYWARE

New York Attorney General Eliot Spitzer has filed suit against California-based Intermix Media for installing spyware on millions of computers. The marketing company, which conceded that previous owners indeed distributed spyware, is accused of violating state laws concerning false advertising, deceptive business practices, and trespassing. The state is seeking injunctions barring the company from distributing any more spyware; an accounting of revenues the company realized from the spyware; and fines of $500 for each act of installing spyware. A statement from the company said that it voluntarily stopped installing spyware recently and that no personal information was ever collected with the secretly installed software. The statement hinted at trying to reach a settlement with New York, a resolution that observers said is a typical outcome of situations like this one. New York Times, 29 April 2005 (registration req'd)

Category 28.1 *Spyware, Web bugs & cookies*

2005-04-29 **lawsuit litigation spyware insidious software New York vs. California Internet company Intermix Media**

DHS IAIP Daily; http://www.nytimes.com/2005/04/29/nyregion/29internet.html

NEW YORK SUES CALIFORNIA INTERNET COMPANY ON USE OF SPYWARE

A broad investigation into Internet abuses led the New York attorney general to file a lawsuit on Thursday, April 28, accusing a California company of clogging computers across the nation with secretly installed spyware and adware, which can vex users and impede the flow of commerce on the Web. The attorney general, Eliot Spitzer, sued Intermix Media, a large Internet marketing firm, accusing it of embedding "several types of invasive and annoying" programs on its Web domains that can pop up, route users to unwanted sites or link them to Intermix's services and clients. In recent years, companies have tried to sneak what consumer advocates call parasitic software into computers that tracks users' browsing habits, but government inquiries into such practices have been rare, said Ben Edelman, a Harvard University researcher who studies spyware. An official with Intermix, in a statement posted on Thursday on the company's Website, said that the company neither promoted nor condoned spyware, and that many of the practices being challenged by Mr. Spitzer began under the company's previous leadership.

Category 28.1 *Spyware, Web bugs & cookies*

2005-05-24 **spyware malicious code installation affiliate program Russia business iframeDOLLARS**

EDUPAGE; http://www.techweb.com/wire/security/163700705

SPREADING SPYWARE THROUGH AN AFFILIATE PROGRAM

A business based in Russia is adopting the affiliate-program approach to spreading spyware around the globe. Called iframeDOLLARS, the company is offering Web site operators 6.1 cents for every computer on which the Web site installs code that exploits vulnerabilities in Windows and Internet Explorer. Microsoft has issued patches for the weaknesses, but unpatched computers remain at risk. The malicious code includes backdoors, Trojans, spyware, and adware. Operators of the iframeDOLLARS site claim to have paid out nearly $12,000 last week alone, which would translate to nearly 200,000 infected computers. Although spyware expert Richard Stiennon called the tactic "brazen" and said iframeDOLLARS might be making quite a bit of money from its scheme, Dan Hubbard, the head of security at Websense, gave iframeDOLLARS less credit. He noted that the company has been around for a while, trying various methods to install malicious code, and he said a number of others have tried similar affiliate programs to accomplish the same thing. TechWeb, 24 May 2005

Category 28.1 *Spyware, Web bugs & cookies*

2005-06-03 **spam anti-spam Anti-Spyware Coalition definition spyware Center for Democracy and Technology**

EDUPAGE; http://software.silicon.com/malware/0,3800003100,39130956,00.htm

SPAM FIGHTERS FORM NEW COALITION

A new group tentatively called the Anti-Spyware Coalition plans to publish guidelines to define spyware, best practices for software development, and a lexicon of common terms by the end of the summer. The guidelines will be open to public comment. The Center for Democracy and Technology, a public advocacy group based in Washington, is running the new initiative. The coalition formed two months after the collapse of the Consortium of Anti-Spyware Technology Vendors, which admitted a company suspected of making adware. According to David Fewer, staff counsel at the Ottawa-based Canadian Internet Policy and Public Interest Clinic, which is affiliated with the new consortium, judging whether software is spyware comes down to notice, consent, and control. Many adware and spyware products fail to meet all three requirements. Silicon.com, 3 June 2005

Category 28.1 *Spyware, Web bugs & cookies*

2005-06-15 **spyware malicious insidious software program anti-spyware lawsuit litigation New York Attorney General Eliot Spitzer**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=8798165

SPYWARE CHARGES RESULT IN $7.5 MILLION SETTLEMENT

California-based Intermix Media will pay New York State $7.5 million over three years to settle a spyware lawsuit. In the suit, New York Attorney General Eliot Spitzer had charged the company with violating state false-advertising and deceptive-practices laws. Intermix acknowledged that it formerly distributed software that was surreptitiously installed on users' computers, though as part of the settlement the company admitted no wrongdoing. Intermix had previously suspended the distribution of the software at issue; with the settlement, the company will permanently discontinue the practice. Intermix has also created a position of chief privacy officer since the lawsuit was originally filed, and officials from the company said they have cooperated with federal regulators. Reuters, 15 June 2005

Category 28.1 *Spyware, Web bugs & cookies*

2005-06-17 **spyware adware BitTorrent application distribution P2P peer-to-peer downloads**

DHS IAIP Daily; http://tech.nytimes.com/cnet/CNET_2100−7349_3−5750601.html

SPYWARE AND ADWARE IN BITTORRENT DOWNLOADS

Purveyors of the applications that produce pop-up ads on PC screens and track browsing habits have discovered BitTorrent as a new distribution channel. BitTorrent has grown into one of the most widely used means of downloading files such as movies or software. According to observers of the trend, videos and music that hide adware and spyware are increasingly being offered for 11 download on various BitTorrent Websites. Both spyware and adware are known to hurt PC performance because they use PC resources to run. Alex Eckelberry, president of Sunbelt Software, a maker of anti-spyware software stated: "[This] is a major concern. It is going to riddle your system with pop-ups, slow your system down and potentially cause system instability." The downloaded files typically were self-extracting archives that would also install the unwanted software, said Chris Boyd, a security researcher who runs the Vital Security Website. In most cases, users would be presented with a dialog box advising that the extra software was about to be installed and given the impression that the install was needed to get access to the desired content, he said.

Category 28.1 *Spyware, Web bugs & cookies*

2005-06-20 **spyware malicious code dissemination method drive-by download iFrameDollars.biz**

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1829174,00.asp

DRIVE-BY DOWNLOAD SITES CHAUFFEUR SPYWARE

Increasingly, spyware is making its way onto users' systems through so-called drive-by-download sites using nefarious methods that circumvent disclosure. One example is iFrameDollars.biz, which claims to be a Website affiliate company just for drive-by sites, using a model similar to aboveboard affiliate networks such as Commission Junction and LinkShare. The Website's "Terms" page says that iFrameDollars.biz pays 55 cents per install or $55 for 1,000 unique installs of a three KB program that "changes the homepage and installs toolbar and dialer." Website operators interested in joining the iFrameDollars.biz network must submit a URL for their Websites, an estimate of their daily traffic and the account number for an online payment service such as E-gold. In exchange, they are sent a small piece of HTML code containing the iFrame exploit, which the site owners are expected to attach to their pages. Web surfers who visit those pages using vulnerable versions of Windows or Microsoft Corp.'s Internet Explorer Web browser have iFrameDollars.biz's programs silently installed. In addition to distributing malicious code and adware through its affiliates, iFrameDollars.biz uses pop-up messages to tempt users into buying nonexistent software programs, taking a cut of any sales.

Category 28.1 *Spyware, Web bugs & cookies*

2005-07-12 **spyware Anti-Spyware Coalition definition**

EDUPAGE; http://news.com.com/2100-1029_3-5783926.html

COALITION TO RELEASE SPYWARE DEFINITION

The recently created Anti-Spyware Coalition is set to release a definition of spyware. According to officials from the group, the first step toward dealing with the growing problem of spyware and adware is to define very clearly what it is. The group's proposed definition, which the public can comment on until August 12, identifies spyware as software that is installed without adequate notification and that monitors computer users' activities. The group also proposes a broader definition that would include software that interferes with users' abilities to properly control their systems. Critics of the group's definitions argue that makers of spyware and adware stand to benefit the most from such a definition because it clearly delineates what they could do and get away with. After the comment period is closed, officials of the Anti-Spyware Coalition will incorporate the best suggestions into the final definitions. CNET, 12 July 2005

Category 28.1 *Spyware, Web bugs & cookies*

2005-07-26 **spyware unauthorized communication phone home data leakage confidentiality control surveillance malicious software malware survey bandwidth**

RISKS; http://www.theregister.co.uk/2005/07/25/spyware_screening/ 23 95

SPYWARE GETTING WORSE: VOLUME & STEALTH INCREASING

Outbound spyware transmissions from infested machines accounted for up to eight per cent of total outbound web traffic in pilot tests of a new managed spyware screening service. UK web security firm ScanSafe said the volume of traffic observed during a 10-week pilot test of its Spyware Screening service showed that spyware applications are becoming stealthier in their ability to hide their outbound 'covert' channels among normal web traffic. That's bad news because data sent when spyware "calls-home" can include confidential and even privileged information.

Spyware now accounts for around 20 per cent of web-based threats, which includes other malware such as worms and Trojans, and is still on the increase, according to ScanSafe. The firm said malware such as CoolWebSearch, which hides on an infected client using newly developed root-kit architecture, often evades detection.

[Abstract by Peter G. Neumann]

Category 28.1 *Spyware, Web bugs & cookies*

2005-10-05 **FTC Odysseus Marketing spyware malicious insidious software distribution anonymous file trading Google Yahoo lawsuit Kazanon**

EDUPAGE; http://msnbc.msn.com/id/9598897/

FTC SUES FOR ALLEGED SPYWARE

The Federal Trade Commission (FTC) has sued Odysseus Marketing, accusing the company of engaging in distributing spyware. Odysseus distributed an application called Kazanon, which supposedly allowed users to trade files anonymously, without fear of being identified by record companies. According to the FTC, users who downloaded the application also got a range of adware programs that fed advertisements to those users' computers and added items to the search results pages of popular search engines, including Google and Yahoo. The added items, which were indistinguishable from those supplied by the search engine, directed users to companies that paid Odysseus for the placement. Further, the software did not offer users a simple option to uninstall it. Walter Rines, owner of Odysseus, disputed all of the FTC's claims. He noted that the user agreement informs consumers of what will be installed when they download the Kazanon program. He also said an uninstall tool is available and that his company's software did not remove any search results but merely added to the list. Rines also said the lawsuit was "moot" because his company stopped distributing adware several weeks ago. MSNBC, 5 October 2005

Category 28.1 *Spyware, Web bugs & cookies*

2005-10-27 **anti-spyware malicious insidious software coalition guidelines**

EDUPAGE; http://news.com.com/2100-7348_3-5918113.html

ANTI-SPYWARE COALITION RELEASES GUIDELINES

The Anti-Spyware Coalition has released a definition of what constitutes spyware, as well as guidelines for dealing with spyware. The group's definition says that spyware is an application installed without sufficient consent of the user and that interferes with the user's ability to exert control over such things as security, privacy and personal information, and system resources. Critics had cautioned that a definition of spyware would allow developers of unwanted software to simply sidestep the characteristics included in the definition, thereby legitimizing their applications. The Anti-Spyware Coalition said it understands that concern and drafted a definition with enough latitude to avoid that problem. The group also identified good practices for how organizations should identify and prevent spyware. Included in the resources is guidance on how to rate the severity of particular spyware applications. The group will accept public comments on the newly released documents until November 27 and will release final versions in early 2006. CNET, 27 October 2005

Category 28.1 *Spyware, Web bugs & cookies*

2005-11-14 **FTC shut down spyware business social engineering**

DHS IAIP Daily; http://www.govtech.net/news/news.php?id=97252

FEDERAL TRADE COMMISSION SHUTS DOWN SPYWARE OPERATION

An operation that uses the lure of free lyric files, browser upgrades, and ring tones to download spyware and adware on consumers' computers has been ordered to halt its illegal downloads by a U.S. District Court at the request of the Federal Trade Commission (FTC). The court also halted the deceptive downloads of an affiliate who helped spread the malicious software by offering blogs free background music. The music code downloaded by the blogs was bundled with a program that flashed warnings to consumers about the security of their computer systems. Consumers who opted to upgrade by clicking, downloaded the spyware onto their computers. The FTC complaint alleges that the Websites of the defendants and their affiliates cause "installation boxes" to pop up on consumers' computer screens. In one variation of the scheme, the installation boxes offer a variety of "freeware," including music files, cell phone ring tones, photographs, wallpaper, and song lyrics. In another, the boxes warn that consumers' Internet browsers are defective, and claim to offer free browser upgrades or security patches. Consumers who download the supposed freeware or security upgrades do not receive what they are promised; instead, their computers are infected with spyware.

Category 28.1 *Spyware, Web bugs & cookies*

2005-12-01 **Adware company lawsuit high risk label Zone Labs**

EDUPAGE; http://news.zdnet.com/2100-9588_22-5979179.html

ADWARE COMPANY QUIBBLES WITH LABEL

A company that makes and distributes adware has filed a lawsuit against a computer security company that identifies the adware company's products as "high risk." The adware purveyor, 180solutions, contends that Zone Labs erred in saying that some of 180solutions's applications try to monitor mouse movements and keystrokes. Although some of its applications employ a technology that could be used in such a manner, those applications do not in fact work that way, according to 180solutions. Representatives from 180solutions said they tried to explain the situation to Zone Labs but were forced to file the lawsuit when Zone Labs refused to remove the applications in question from its list of high-risk tools. Eric Howes, a spyware researcher at the University of Illinois, said that despite its protestations, 180solutions remains "a perfectly legitimate target for anti-spyware companies." According to Howes, security professionals continue to "find unethical and illegal installations of 180's software." ZDNet, 1 December 2005

Category 28.1 *Spyware, Web bugs & cookies*

2005-12-18 **Websites spyware installation Microsoft Internet Explorer IE zero-day exploit bug**

DHS IAIP Daily;
http://www.techweb.com/wire/security/174907332;jsessionid=WR
E35TOIAV2AUQSNDBECKH0CJUMEKJVN

SITES INSTALLING SPYWARE VIA ZERO-DAY INTERNET EXPLORER BUG,

A still-unpatched Internet Explorer vulnerability that's been used by attackers since late November to compromise Windows PCs is now being used by large numbers of malicious Websites to plant spyware and adware, a security company claimed Thursday, December 8. San Diego-based Websense said in an alert that it's detected thousands of sites connecting to a main malicious URL that's "actively exploiting this vulnerability to execute malicious code," according to the warning. All it takes is a visit to one of the sites with Internet Explorer running on Windows 98, Windows Me, Windows 2000, or Windows XP, to compromise a computer, the warning noted. A bogus warning that the machine is infected with spyware appears and a so-called "spyware cleaning" application launches. That application then prompts the user to enter a credit card number. What's actually installed, however, is real spyware, which then connects to a URL in the .biz domain to download and run more than 10 other programs that install without the user's consent. According to Websense, the .biz domain Website is real, but has been compromised by hackers. It's hosted in the U.S., and is currently still online.

Category 28.1 *Spyware, Web bugs & cookies*

2006-01-05 **FTC settlement bogus anti-spyware scheme malicious insidious software malware CAN-SPAM spam Spyware Assassin Spykiller fraud**

EDUPAGE; http://www.internetnews.com/bus-news/article.php/3575421 23

FTC WINS SETTLEMENT FOR BOGUS ANTISPYWARE SCHEME

The operators of two supposed antispyware products agreed to pay nearly $2 million to settle complaints by the Federal Trade Commission (FTC) that the products amounted to nothing more than a scam. Last year, the FTC charged the operators of Spykiller and Spyware Assassin with running similar schemes to defraud consumers. According to the FTC, both companies used pop-up ads and e-mail to draw consumers to the companies' Web sites, where users could supposedly receive free scans of their machines. After the scans reported spyware, which frequently did not exist, users were offered a spyware-removal service for around $30-40. The removal also did not do what was advertised, said the FTC. In addition, many of the e-mail messages violated provisions of the CAN-SPAM Act. The makers of Spyware Assassin agreed to pay $76,000, which represents the amount the FTC spent on its investigation. Makers of Spykiller will pay $1.9 million.

Category 28.1 *Spyware, Web bugs & cookies*

2006-01-25 **anti-spyware malicious software Website StopBadware.org**

DHS IAIP Daily; http://www.usatoday.com/tech/news/computersecurity/2006−01−2 5−spyware_x.htm 23

FREE WEBSITE TO LIST PROGRAMS WITH SPYWARE.

A free Website, StopBadware.org, launched Wednesday, January 25, plans to provide a list of programs that contain spyware and other malicious software. It will also identify companies that develop the programs and distribute them on the Internet. Consumers can then decide if a program is safe to download. "For too long, these companies have been able to hide in the shadows of the Internet," says John Palfrey, who heads the Berkman Center of Internet & Society at Harvard Law School and is spearheading the project. "What we're after is a more accountable Internet." The initiative is being run by Harvard and the Oxford Institute and is backed by high-tech heavyweights including Google and Sun Microsystems. Consumer Reports' WebWatch is serving as a special adviser. In addition to spyware, the hit list of the StopBadware coalition includes malicious "adware" programs that serve up onslaughts of pop-up ads or software that contains hidden viruses and worms. By checking StopBadware.org, its organizers say, consumers can choose, in the first place, not to download a program containing the malicious software. The coalition is encouraging consumers to visit the Website to log their experiences with harmful programs. StopBadwar.org Website: http://www.stopbadware.org/

Category 28.1 *Spyware, Web bugs & cookies*

2006-01-25 **new Website malicious software program maker identification Harvard Oxford**

EDUPAGE; http://www.nytimes.com/2006/01/25/technology/25spy.html 23

NEW SITE AIMS TO IDENTIFY MAKERS OF MALICIOUS PROGRAMS

Researchers at Harvard Law School and Oxford University are launching a Web site that will identify organizations that distribute spyware, adware, and other unwanted computer programs, as well as the tactics they employ to intall their applications. StopBadware.org was financed initially by companies including Google, Lenovo, and Sun Microsystems. The site will also include an area where consumers can submit testimonials about their experiences with different software they have downloaded. John G. Palfrey Jr., executive director of the Berkman Center for Internet and Society at Harvard, said, "We want to turn the spotlight on the bad actors, but also give ordinary users a place to go and get an early warning before they download something that might harm their computer." According to the Pew Internet & American Life Project, 59 million U.S. adults said their computers were infected with spyware last year. Data from Consumer Reports indicate that despite consumer spending of $2.6 billion over the past two years on antivirus and antispyware tools, users still spent $3.5 billion in damages over the same period due to unwanted software.

Category 28.1 *Spyware, Web bugs & cookies*

2006-02-06 **University of Washington study spyware prevalent Internet software IE browsers**

DHS IAIP Daily; http://www.securityfocus.com/brief/128 23

STUDY: SPYWARE REMAINS RAMPANT AS WINAMP EXPLOITED.

A new study by the University of Washington finds that one in twenty executables on the Internet contain spyware. The study, which sampled more than 20 million Internet addresses, also found other disturbing trends. Among them: one in 62 Internet domains contains "drive-by download attacks," which try to force spyware onto the user's computer simply by visiting the Website. The problems for Web surfers primarily affect Microsoft's Internet Explorer browser but exist to a lesser extent for other browsers as well.

University of Washington study: http://www.cs.washington.edu/homes/gribble/papers/spycrawler.pdf

---

Category 28.1 *Spyware, Web bugs & cookies*

2006-03-17 **anti-spyware software checking Spycar**

DHS IAIP Daily; 23
http://www.infoworld.com/article/06/03/17/76590_HNspycar_1.html

NEW SPYCAR SOFTWARE WILL TEST ANTISPYWARE.

With security experts warning of "rogue" antispyware products that sometimes do more harm than good, two security researchers have decided to take matters into their own hands. They're working on a new software product, called Spycar, that will test the effectiveness of antispyware products. Spycar will contain about 25 small programs, each of which engages in the kind of nasty behavior normally associated with spyware. The software will then undo all of the changes it has made after the testing has been completed. Spycar will be available free of charge in May. More information will be made available on the http://www.intelguardians.com Website at that time.

Category 28.1 *Spyware, Web bugs & cookies*

2006-03-20 **adware spyware software manufacturer Badware Watch List Center for Democracy and Technology CDT Stopbadware Coalition**

DHS IAIP Daily; 23
http://www.infoworld.com/article/06/03/20/76595_HNbadware_1. html

TOUGH WEEK AHEAD FOR 'BADWARE' COMPANIES.

The fight against invasive software will take a step forward this week as the Center for Democracy and Technology (CDT) and the Google-backed Stopbadware Coalition will release two separate reports that state the names of undesirable software programs and the advertisers who help fund them. On Monday, March 20, the CDT will publish its report on the major advertisers who are behind so-called "adware" software. Two days later, the Stopbadware Coalition is set to release its first report, which will name several software programs to its Badware Watch List.

Category 28.1 *Spyware, Web bugs & cookies*

2006-03-20 **spyware adware panel roots online advertising**

DHS IAIP Daily; 23
http://www.infoworld.com/article/06/03/20/76629_HNspywarepan el_1.html

PANEL EXPLORES ROOTS OF SPYWARE, ADWARE.

Following the money trail behind the flood of spyware and adware on the Internet poses some sticky questions around liability, said a panel of spyware experts at a workshop in New York City Friday, March 17. Legal experts, government officials and technology professionals gathered at New York University School of Law to discuss the causes of and solutions to unwanted software programs that track Internet users' behavior. One panelist suggested that companies advertising online should develop more thorough policies to control where their ads go on the Internet.

Category 28.1 *Spyware, Web bugs & cookies*

2006-03-21 **spyware trail Kazaa advertisers StopBadware.org Google Badware Report**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1940747,00.asp 23

SPYWARE TRAIL LEADS TO KAZAA, BIG ADVERTISERS.

The StopBadware.org coalition, funded by Google, has listed the Kazaa file-sharing application at the top of a list of noxious software programs that present a threat to business and consumer users. The coalition, which counts Sun Microsystems and Lenovo among its sponsors, will recommend in its inaugural Badware Report that users stay away from Kazaa and three other programs that can be combined with Trojans and bots for use in data theft attacks. Adware and spyware programs that come bundled with peer-to-peer applications present a huge security risk to corporate networks, and StopBadware.org says Kazaa's claim to be spyware-free cannot be trusted. In addition to Kazaa, StopBadware.org said computer users should stay away SpyAxe, a rogue anti-spyware program; MediaPipe, a download manager that offers access to media content; and Waterfalls 3, a screensaver utility. StopBadware.org Report: http://www.stopbadware.org/pdfs/badwarev1r3.pdf

---

Category 28.1 *Spyware, Web bugs & cookies*

2006-03-24 **do-it-yourself spyware kit sale Russian Website WebAttacker SophosLabs**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1942497,00.asp 23

DO-IT-YOURSELF SPYWARE KIT SELLS FOR $20.

A do-it-yourself malware creation kit is being hawked on a Russian Website for less than $20, according to security researchers tracking the seedier side of the Internet. Virus hunters at SophosLabs discovered the spyware kit, called WebAttacker, on a Website run by self-professed spyware and adware developers. The WebAttacker kit includes scripts that simplify the task of infecting computers and spam-sending techniques to lure victims to specially rigged Websites.

Category 28.1 *Spyware, Web bugs & cookies*

2006-04-07 **rogue anti-spyware application warning SurfControl UnSpyPC false positive**

DHS IAIP Daily; http://www.theregister.co.uk/2006/04/07/unspypc/ 23

WARNING OVER ROGUE ANTI-SPYWARE APPLICATION.

A rogue anti-spyware application is falsely identifying popular security products and file system tools as spyware. Security firm SurfControl advises not to use the application, UnSpyPC. False-positive reporting is hardly unknown across many supposed anti-spyware applications, as SurfControl notes, but this case is particularly severe since UnSpyPC could disable critical security and business applications.

Category 28.1 *Spyware, Web bugs & cookies*

2006-04-19 **bogus fake anti-spyware software sales fraud fine**

DHS IAIP Daily; 23
http://www.sophos.com/pressoffice/news/articles/2006/04/spyw arechen.html

HEFTY FINE FOR MAN WHO MARKETED BOGUS ANTI-SPYWARE SOFTWARE.

SophosLabs reports a man has been fined almost $84,000 for marketing a bogus anti-spyware program, but has warned Web surfers that there are many other fake protection products being unethically promoted on the Internet. Zhijian Chen of Portland, OR, was found to have made thousands of dollars by sending spam messages that fooled people into believing that their computers were infected by spyware, and claiming that a product called "Spyware Cleaner" was the cure. According to court documents, Chen sent out e-mails and advertisements promoting the "Spyware Cleaner" software in exchange for a 75 percent commission on each $49.95 sale.

Category 28.1 *Spyware, Web bugs & cookies*

2006-04-19 **antispam lawsuit settlement CAN-SPAM Spyware Cleaner Secure Computer**

EDUPAGE; http://news.yahoo.com/s/ap/20060419/ap_on_hi_te/spam_lawsuit 23

SETTLEMENT REACHED IN ANTISPYWARE CASE

In a settlement announced by prosecutors in Washington State, Zhijian Chen of Oregon will pay about $84,000 in fines, restitution, and attorneys' fees following a scheme in which Chen sold consumers fraudulent antispyware services. Chen was charged with sending e-mail that led recipients to believe their computers were infected with spyware and that a product called Spyware Cleaner, made by Secure Computer, could clean their machines. Chen then collected a commission when users bought the product. State Attorney General Rob McKenna said, "We will not tolerate those who try to profit by preying on consumers' fears of spyware and other malware." New York-based Secure Computer as well as a number of officials from the company are also named in the lawsuit against Chen.

Category 28.1 *Spyware, Web bugs & cookies*

2006-05-16 **researchers fake anti-spyware ransomware report malicious code research**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1963097,00.asp 23

RESEARCHERS WARN OF FAKE ANTI-SPYWARE.

The latest report issued by Finjan's Malicious Code Research Center highlights the growth of several emerging breeds of cyber-attack, including the increasing popularity of so-called "ransomware" and viruses that are being spread via fake anti-spyware applications. The anti-virus software maker's research arm said in its Web Security Trends Report, issued on May 16, that the growth of "rogue anti-spyware" and the emergence of hackers looking to hold stolen corporate data up for ransom are two of the fastest growing trends in the security threat landscape. Virus rootkits continue to pose one of the most prevalent and challenging obstacles for IT administrators to overcome, according to the study. In these attacks, hackers disguise the malware in programs advertised online as free anti-spyware applications. Once downloaded onto a user's computer, the applications may deliver their own payloads of malicious code or expose affected machines to subsequent attacks. In some cases, the false anti-spyware tools even run fake computer security scans that claim to find existing spyware programs on infected devices. The software then directs the computer's user to a Website where the user is encouraged to purchase a full version of the free application already on the PC. To download report, follow link and click on “Security Trends Report”: http://www.finjan.com/Content.aspx?id=827#SecurityTrendsReport

---

28.2 Scumware

Category 28.2 Scumware

2000-08-28 **spyware unauthorized connection upload scumware**

RISKS 21

Eudora v4 has three settings for functionality: full (paid), free with ads, and limited but without ads. David Sedlock noticed that the latter mode was nonetheless accessing the Eudora site using HTTP connections twice a day without any notification to (or authorization from) the user. Eudora staff dismissed the occurrence as a minor issue because the connections were "really really fast" and did not transfer any private information from the user. Sedlock, however, noted that the unwanted connections could automatically initiate a connection to his ISP, thus incurring per-call costs to him.

Category 28.2 Scumware

2001-04-04 **scumware alteration Web interpretation conversion alteration text HTML**

RISKS 21 36

Marc Roessler reported an interesting effect of using filtering proxies. A colleague of his reported problems in a published text document Roessler had posted on the Web; it turned out that his colleague's WebWasher Version 3.0 for Windows was changing redirected links to direct links. The plaintext file included examples of enquoted HTML, but the proxy filter did not take the file type or quoting into account; in fact, it altered the file type from "text/plain" to "text/html" thus forcing the browser to interpret HTML fragements as instructions.

Category 28.2 Scumware

2001-05-23 **scumware unauthorized modification editing changes invisible data corruption integrity arrogance word processing spreadsheet office software design flaw arrogant public relations dismissive**

RISKS 21 42

Jonathan Arnold reported with outrage to RISKS about yet another scumware feature in MS Office XP. "When you type a hyperlink in FrontPage 2002, Word 2002, Excel 2002, PowerPoint 2002, or Outlook 2002 (using Word as your email editor), the Office application will alter what you've typed, without notifying you or giving you an opportunity to undo the "correction." In fact, in most cases, you can't override the 'correction' at all: you're stuck with FP, Word or Excel's version of what you typed."

Specifically, Microsoft describes as a "feature" the fact that it silently and irremdiably removes double slashes from all hyperlinks typed in its Office XP suite. The descriptor is left as intended, but the underlying hyperlink is modified. Challenged with this bizarre behavior, Microsoft responded essentially that no one should be using double slashes anyway and that its unauthorized changes are in the interest of "cleanliness and consistency."

Quoting Peter Deegan, the correspondent adds, "The company has gone too far in compulsory changes to the link with no warning to the user or any workaround to fix the Autocorrect. Adding injury to insult, there's no documentation on these changes in the help file. Microsoft has declined to provide details of any other compulsory changes made to hyperlinks in Office XP nor have they suggested any workaround for those affected, or some way to switch off this behavior. The Microsoft arrogance shows through: it's not a problem, so why bother fixing it? The fact that Microsoft has declined to detail what changes are arbitrarily made to links makes us even more concerned. Office XP users don't know what compulsory changes will be made to their links. Chances are they'll find out the way I did - the hard way."

Category 28.2 Scumware

2001-06-07 **scumware pop-up advertisements hiding**

RISKS 21 47

Greg Searle reported in RISKS on yet another way of annoying Web users. A company called Fastclick provides code that hides pop-up windows behind the windows already on screen. These pop-ups remain in place and are revealed only after one minimizes or closes the other windows on screen -- by which time it is difficult to determine where the pop-ups came from. The solution, such as it is, is to disable JavaScript; alternatively, if one can locate the offending sites, one can put them on a firewall's or brower's exclusion list.

Category 28.2 *Scumware*

2001-06-07 **scumware HTML URL redirection Web advertising pornography**

RISKS 21 47

Justin Mason provided RISKS readers with an interesting (if distressing) example of scumware. Mr Mason used a free URL-redirection service to provide an easier entry into his Web site, which had a cumbersome URL. Some years later, having forgotten all about the redirection. To his horror, someone who wanted to reach his site reported (and Mr Mason confirmed) that entering the old URL resulted in a number of unclosable windows with advertisements, including pornography.

[MORAL: routinely check all the URLs you have placed with redirection services to be sure that you approve of how your site is being represented to unsuspecting viewers.

Category 28.2 *Scumware*

2001-06-20 **BIOS ROM firmware Internet connection links desktop browser scumware**

RISKS 21 51

Merlyn Kline reported a novel example of scumware to RISKS as follows [identity of "Myrv" not clear]:

Myrv writes: "There is an interesting thread over at DSL Reports discussing Phoenix Technologies new BIOS. This BIOS contains the PhoenixNet Internet Launch System. ILS resides safely within ROM and is activated the first time a user launches a PhoenixNet-enabled PC with a Windows 98 Operating System. When the PhoenixNet ILS detects an Internet connection, it makes contact with the PhoenixNet server and delivers user-selectable services. These services are delivered to the user as hotlinks on the desktop and in the web browser or, as applications that PhoenixNet automatically packages, downloads and installs. It's 3 a.m., do you know who your motherboard's talking to????"

http://slashdot.org/yro/01/06/19/2039216.shtml

Category 28.2 *Scumware*

2001-06-22 **scumware adware junk e-mail spam**

NewsScan

TOOL WRAPS E-MAIL MESSAGES WITH SPAM
Admail, a new technology marketed by Australian online marketing firm Reva Networks, enables advertisers to intercept e-mail messages as they enter the mail server and "wrap" them in advertising content tailored to the recipient's demographic profile. Reva Networks CEO Robert Pickup says the concept has proven more effective than other forms of online advertising. "Because the advertising is embedded within a regular e-mail and not a separate e-mail message from an advertiser, users are more likely to open the message and hence be exposed to the advertising offer." Pickup says he doesn't think consumers will be annoyed by the ads "as long as it's relevant to them." But Australian Consumer Association IT policy officer Charles Britton says he doesn't think that consumers will passively accept advertising with their personal e-mail: "Without some incentive, why would you want advertising in your e-mail?" (ZDNet Australia 22 Jun 2001)
http://dailynews.yahoo.com/h/zd/20010622/tc/tool_feeds_spam_to_your_e-mails_1.html

---

Category 28.2 *Scumware*

2001-06-28 **scumware smart tags Windows XP**

NewsScan

MICROSOFT OFFERS NEW VERSION OF ITS OFFICE SOFTWARE [31 May 2001]
Microsoft today is announcing Office XP, sixth version of the software it introduced ten years, and which now has been integrated with the Internet for interactive information retrieval and collaboration. For example, a word processing feature called "Smart Tags" will allow documents to link automatically to Internet databases, and Microsoft Word will be able to recognize an address, a parcel shipping number, or a flight number, etc., and look up further information about it. Some of these retrieval functions will be free from company Web sites but others (such as legal searches in the Lexis-Nexis database) will cost money. (New York Times 31 May 2001)
http://www.nytimes.com/2001/05/31/technology/31SOFT.html

MICROSOFT PULLS CONTROVERSIAL SMART TAG FEATURE [28 Jun 2001]
Bowing to a wave of criticism, Microsoft says it will kill plans to include a Smart Tag feature in its forthcoming Windows XP operating system. The feature would have allowed Internet Explorer to turn any word on any Web site into a link to Microsoft's own sites and services, or to a site of Microsoft's choosing. The company continues to defend Smart Tags in principle, and plans to work toward including it in a future version of Windows or Internet Explorer, but group VP Jim Allchin said the decision was made to remove the Smart Tags because "we got way more feedback than we ever expected." Although many people view the public reaction against Smart Tags as excessive, Wall Street Journal columnist Walter Mossberg says, "...Microsoft's dominant Internet Explorer browser is like a television set, or a digital printing press, for the Web. Its function is to render -- accurately and neutrally -- all Web pages that follow standard programming... Microsoft has a perfect right to produce and sell its own Web content with its own points of view. But it is just plain wrong for the company to use the browser to seize editorial control and to steal readers from other sites." (Wall Street Journal 28 Jun 2001)
http://interactive.wsj.com/archive/retrieve.cgi?id=SB993679289461737795.djm (sub req'd)

Category 28.2 *Scumware*

2001-07-31 **spyware license usage environment software EULA end-user license agreement contract**

RISKS 21 56

Livestage Pro from Totally Hip Software "phones home" to report via the Internet on its license information, usage and computing environment using a covert http interaction. According to Michael F. Maggard, writing in RISKS, the company stonewalled, refusing to discuss the issue; however, one employee did express surprise in a public discussion group that anyone would object to such a proceeding. He pointed to an explicit clause in the end-user license agreement that specifically allows the company to "electronically verify their serial number."

Category 28.2 *Scumware*

2001-08-29 **scumware adware popup banners overlay advertisements lawsuit**

NewsScan

LEGAL FIGHT OVER POP-UP BANNERS [29 Aug 2001]
The Interactive Advertising Bureau (IAB) is planning a complaint with the Federal Trade Commission against software Gator.com, and Gator has sued IAB in a preemptive legal strike. The IAB is asking the FTC to stop the practice of superimposing new ads over the existing ads of other Web sites. Gator argues that its software -- which generates ads relevant to the particular individuals surfing a Web site -- "is going to revolution the industry. There are a lot of online media sites that are failing right now and it's because their advertising isn't working." IAB president Jeff McFadden says: "What they are doing isn't very smart. It's harmful to Web sites and their advertisers and it's not very fair to consumers." (Washington Post 29 Aug 2001)
http://washingtonpost.com/wp-dyn/articles/A11208-2001Aug29.html

---

Category 28.2 *Scumware*

2001-11-09 **scumware Microsoft Visual Basic programming language undocumented modification unauthorized inconsisten stupid arrogant swine detestable reprehensible disgusting nauseating**

RISKS 21 74

John Sullivan noted yet another example of the questionable design philosophy of programmers and product managers at Microsoft. His report in RISKS demonstrates that Visual Basic (VB6 SP5) alters dates without permission, without notification, and inconsistently.

Part of his report reads, ". . . I'd entered the start date as a literal date of the form #2001-11-08#. . . . When I came back to it today, I noticed it read #11/8/2001#. . . . Retyping it showed that the date was changed in front of my eyes:

#2001-11-08# becomes #11/8/2001# (2001-11-08)
#11/8/2001# becomes #11/8/2001# (2001-11-08)
#8/11/2001# becomes #8/11/2001# (2001-08-11)
#15/11/2001# becomes #11/15/2001# (2001-11-15)

It changes as soon as the cursor left the line. So you type it, check it, find it correct, go off somewhere else, blam! The first has reduced the comprehensibility of the code. The second and third give no feedback that they're not conforming to the current locale. The last two show that VB is not even being consistent in its parsing."

Nick Brown replied in a later RISKS that perhaps the algorithm is as follows:

- Find a number which could only be the month
- Find a number which could only be the day
- If there is ambiguity, assume the user typed the date in mm/dd order

---

Category 28.2 *Scumware*

2001-11-14 **scumware copyright content intellectual property advertising TV commercials moral rights consumers tampering alteration**

NewsScan

TV 'TIME MACHINE' SPARKS CONTROVERSY [14 Nov 2001]
A machine that "squeezes" television programming so that broadcasters can fit in extra commercials is stirring controversy in the industry. The Time Machine is being marketed by Prime Image for $93,000 and so far, 120 have been sold to local stations in the U.S., with another 70 going to stations in Mexico. The patented technology shears seconds off of programming by editing out repetitive video frames in real time. With most TV shows running at 30 frames per second, a missing frame here or there is undetectable to viewers, but the accumulated time enables a station to insert an addition 20- to 30-second commercial. People in the TV industry say there is nothing controversial about using such a device during a local news show, for instance, but the problem arises when the station is airing programming from an outside source, such as a professional sports organization, that has strict limits on local commercials. Many Hollywood execs aren't happy with the Time Machine's ability to tinker with content in order to beef up advertising. "Adding more commercials that take away from content is the wrong direction for the industry to go," says Gary Newman, president of News Corp.'s 20th Century Fox Television. (Wall Street Journal 14 Nov 2001)
http://interactive.wsj.com/articles/SB1005695943407459080.htm (sub req'd)

Category 28.2 *Scumware*

2001-12-06 **scumware autocorrect proper names MS Word XP**

RISKS 21 82

Arnold Weissberg was practically spitting with outrage in his note to RISKS about yet another example of having Microsoft engineers tell the rest of the world how to type:

"I typed my last name into a document. I thought something funny had happened because it came out with one "s." I never misspell my last name. There was a line under the "W". Holding the mouse on this line I got the following choices:
1. Change back to "Weissberg"
2. Stop Automatically Correcting "Weissberg"
3. Control AutoCorrect Options

Now this is, as my grandmother would have said, real chutzpah. Telling me how to spell my own name! Talk about arrogance--what's next, "anglicizing" it? Like, auto correcting it to "Whitehill?" And if I try to change it back will it say, "I'm sorry, Arnold, I can't do that"? I think in this little example we can learn a lot about Microsoft's corporate attitudes toward the rest of the world--that is, no one is smart enough even to be trusted to spell their own name right. Much less choose what software they'd like to use."

[MK notes: Hey, this is progress -- at least you get to turn off the correction!]

Category 28.2 *Scumware*

2001-12-07 **scumware Microsoft Office Windows XP sensitive information debugging memory dump program crash document**

RISKS 21 82

David Farber noted yet another threat to sensitive information from Microsoft Office XP and Windows XP. Writing in RISKS, he contributed the following summary:

PROBLEM: Microsoft Office XP and Internet Explorer version 5 and later are configured to request to send debugging information to Microsoft in the event of a program crash. The debugging information includes a memory dump which may contain all or part of the document being viewed or edited. This debug message potentially could contain sensitive, private information.

PLATFORM:

* Microsoft Office XP
* Microsoft Internet Explorer 5.0 and later
* Windows XP
* Microsoft has indicated that this will be a feature of all new Microsoft products

DAMAGE: Sensitive or private information could inadvertently be sent to Microsoft. Some simple testing of the feature found document information in one message out of three.

SOLUTION: Apply the registry changes listed in this bulletin to disable the automatic sending of debugging information. If you are working with sensitive information and a program asks to send debugging information to Microsoft, you should click Don't Send.

http://www.ciac.org/ciac/bulletins/m-005.shtml

Category 28.2 *Scumware*

2002-01-04 **spyware music-sharing peer-to-peer unauthorized installation implementation supervision QA quality assurance**

NewsScan

USER WEB HABITS TRACKED BY SOME MUSIC-SWAPPING PROGRAMS
The Web surfing habits of people who used the LimeWire, Grokster and KaZaA music-sharing programs were surreptitiously tracked because those programs were linked to an online sweepstakes game called ClickTillUWin, in which players pick numbers and win cash prizes. The company that operates the sweepstakes game says it told outside distributors to get users' permission before installing the software, but in these cases that action was not taken. The three companies have posted new versions of their software without the tracking component, and LimeWire has issued an apology. (AP/USA Today, 4 Jan 2002)
http://www.usatoday.com/life/cyber/tech/2002/01/04/limewire-tracking.htm

---

Category 28.2 *Scumware*

2002-01-11 **scumware Lotus Notes unauthorized undocumented data modification corruption diddling arrogance stupidity criminal negligence design flaw bug error expletive deleted**

RISKS 21 88

Erling Kristiansen posted a note in RISKS discussing undocumented, unannounced data loss in Lotus Notes. The author's examples follow verbatim:

* I printed a mail message before I sent it. Some of the cc: addresses were quietly and permanently removed. (Did anybody say buffer overflow recently? Maybe it is more like buffer truncation, but certainly member of the same family)

* Trying to reply to a mail I received, I discovered that 3 out of the about 10 cc: addresses in the incoming message had been truncated, rendering them invalid. No addresses were lost completely, but the amount of truncation that occurred suggests that a short address might be "truncated into extinction" if it is in the right place in the list of addresses. I checked the original RFC-822 header that is accessible. It was correct.

By the way, correcting the addresses in place and re-sending had a very strange effect: The corrected addresses, and only those, were turned into an X.400-like address with a number of attributes pointing to my local environment. I had to remove and re-type the "sick" addresses to have them accepted.

* I copied and pasted about 100 addresses from a spreadsheet into the bcc: field of a mail. Everything looked OK, the pasted addresses appeared neatly in the address window, I could scroll through them, etc. But the message was only sent to the first address. No warning of any kind appeared that a good hundred addresses had been discarded. I only discovered the error because I had asked for delivery notification, and got very few. Had I not discovered this, only a handful of people would have been invited to a presentation. (there were a few other addressees that had not been pasted in - those worked OK even though some were entered AFTER the skipped addresses).

* Notes allows you to format messages, with facilities more or less equivalent to an HTML editor. If a message is sent outside the Notes domain, ALL formatting is removed, even things like indentation and paragraph numbers. So a nicely formatted message may become rather unreadable, even ambiguous (indentation may imply a lot about the meaning of a text). No warning is given that formatting information is being removed.

The RISKS correspondent concludes, "The RISK of all this is that Notes accepts instructions to do something, does not complain about the input, and then goes ahead and does something else than what could reasonably be expected. You can obviously check for any of these events, but they are rare enough, and different enough, that you don't really know when to expect a problem, and what to look for in order to make sure everything went as expected."

Category 28.2 *Scumware*

2002-01-18 **scumware Microsoft Excel unauthorized undocumented data modification corruption diddling arrogance stupidity criminal negligence design flaw bug error expletive deleted**

RISKS 21 88

Geoffrey Brent, writing in RISKS, identified yet another Microsoft undocumented, unauthorized data modification. If you open two MS-Excel files and copy a cell containing a number and paste it into a cell in the other file, everything works fine. For example, 1.2345 gets copied as 1.2345 regardless of how many figures are showing in the cell. However, if you open file A, copy a number, _close file A_, and then paste the number into file B, you get a value that is identical to what was _visible_ rather than to what was entered in the original cell. Thus in the example above, 1.2345 in the source becomes 1.23 in the destination worksheet. [MK note: I tested this myself in Excel 2000 and it's true.]

Category 28.2 *Scumware*

2002-01-28 **scumwarescumware unauthorized modification editing changes invisible data corruption integrity arrogance word processing spreadsheet office software design flaw arrogant public relations dismissive**

RISKS 21 90

Bear Giles reported that Microsoft Outlook has an erroneous algorithm for recognizing UUENCODED text within the body of a message. The designers incorrectly assumed that any line beginning with the word "begin" must be the start of UUENCODED text. The algorithm does not bother to check for any other evidence that this assumption is correct, with the result that perfectly ordinary text is relegated to an attachment and may easily be lost. In addition, malware writers have already figured out that they can send ordinary text messages and have Outlook obligingly convert embedded malicious code into an attachment _after_ it has gone through a firewall or e-mail filtereven if users don't permit attachments to get through.

Microsoft's breathtakingly arrogant workaround (not solution) for their own design error was to recommend that everyone on the planet either stop using the word "begin" or use the capitalized form "Begin" in all e-mail messages sent to Outlook users or potentially forwarded to Outlook users -- that is, in effect, in all e-mail messages the world over.

Category 28.2 *Scumware*

2002-01-29 **scumware automated spelling correction software**

RISKS 21 90

Automated spelling-correction software mangled several names in the HP annual report; examples include "David and Lucite Packard Foundation" [from "Lucile"], "Edwin van Pronghorns" [from "Bronkhorst], "Eleanor Hewlett Limon" [from "Gimon"], and "Mary Hewlett Gaffe" [from "Jaffe"].
http://www.siliconvalley.com/docs/news/tech/085146.htm

Category 28.2 *Scumware*

2002-02-12 **scumware Google search engine periods removed data modification corruption e-mail address bounce**

RISKS 21 91

Google appears to remove some periods even in e-mail addresses that appear in the summary lines for hits. Robert Marshall reported this problem to RISKS as follows (quoting verbatim):

I was searching for the work e-mail address for a friend using google. Let's say the name was Paul Consultant. Google gave me a hit with the correct company and the web page was such that his e-mail appeared in the google summary. So I cut and pasted it directly without having to visit the company web site. It appeared as PR.Consultant@relations.com.

When the e-mail bounced I investigated and the company web page has the mail as P.R.Consultant@relations.com, as does google's cache. It looks as if google is trying to cut down on the synposis by removing redundant '.'s

Unfortunately they aren't always redundant. Fortunately my e-mail bounced rather than going to an unrelated recipient.

Category 28.2 *Scumware*

2002-03-05 **privacy spyware redirection search engine privacy monitoring surveillance**

RISKS 21 93

Sim IJskes found that even though he reconfigured Netscape browser v6.2 to use GOOGLE instead of the netscape.com search engine, in fact the product shunted his requests through their search engine before passing the search on to GOOGLE. Commented the correspondent, "I guess that Netscape allows you to search other search engines than their own, but still wants to know what you are searching.…"

Category 28.2 *Scumware*

2002-04-25 **P2P peer-to-peer Trojan distributed processing reverse engineering**

Security Wire Digest 4 32

*KAZAA CRITICIZED FOR SECONDARY SOFTWARE
Since peer-to-peer file sharing service KaZaa came under fire for surreptitiously including secondary software with every download, a Russian hacker has created a "KaZaa Lite" version sans a program that allows a third party to tap into a user's computer processing power and storage space. KaZaa owner Sharman Network has not said what actions, if any, it will pursue against Russian programmer "Yuri" and Kazaalite.com, which has processed more than 80,000 downloads since its release earlier this month, according to a published report. Sharman quietly has been installing software in KaZaa downloads that could allow a secondary file-swapping network called "AltNet" to draw upon users' resources for use in distributed computing. KaZaa estimates that about 20 million users have the software installed on their machines. Several media reports have said the secondary software works the same as a Trojan. The company has since changed its user agreement policy.

Category 28.2 *Scumware*

2004-02-13 **slimeware AOL instant message IM software game adware**

NewsScan

SLIMEWARE?

Some AOL subscribers have received messages seeming to be from friends but linked to a humorous Osama bin Laden game that surreptitiously installs another program which in turn broadcasts an ad from the infected computer to all correspondents on its buddy lists. AOL executive Andrew Weinstein calls the software that does this "a particularly slimy form of adware," though the makers of that software, called Buddylinks, insists: "Our games interact with instant messengers by promoting the game among the user's network of buddies. Please understand, our flash games are in no way a virus. We simply combine peer-to-peer, social networking, and instant messaging into one spectacular technology." AOL's Weinstein says, "The one important thing for consumers to know is that they should always execute extreme caution before downloading or installing any program unless they're absolutely sure why they got it." (San Jose Mercury News 13 Feb 2004)

Category 28.2 *Scumware*

2004-08-10 **adware scumware spyware insidious sofware personal computer ISP scan audit**

NewsScan

AUDIT IDENTIFIES TOP ADWARE THREAT

A six-month audit carried out by an ISP and a software company has concluded that CoolWebSearch is one of the top adware threats on the web. The survey was carried out by the Atlanta-based ISP Earthlink and Webroot Software, the latter a company that makes privacy protection software. Slightly over two million scans were carried out during the period January 1 to June 30 this year. A total of over 54 million instances of spyware were found. CoolWebSearch's most common exploit is to hijack a user's homepage and direct it to a paying client's Web site. Damaging CWS variants can pop up so many ads that a computer locks up or crashes. (The Age, 10
Aug 2004) rec'd from John Lamp, Deakin U.

Category 28.2 *Scumware*

2005-11-11 **CD copy protection suspension Sony spyware DRM XCP rootkit installation patch**

DHS IAIP Daily;
http://www.techweb.com/wire/security/173602071;jsessionid=BH
YE2POHHTY0IQSNDBOCKH0CJUMEKJVN

SONY SUSPENDS CD COPY PROTECTION

On Friday, November 10, Sony BMG Music Entertainment announced that it would stop producing CDs with its XCP copy-protection technology. The move came just a day after nearly every major security firm put out alerts that a Trojan horse was using the XCP (eXtended Copy Protection) software to hide malicious files. A wave of lawsuits has been filed or are about to be filed against Sony for installing the hacker-style "rootkit" on users' PCs without their permission. On Thursday, November 9, Sony BMG posted a news release on its Website that linked to a patch download and the site where consumers are to request help with uninstalling the copy-protection software.

Category 28.2 Scumware

2005-12-04 **spyware scumware Sony rootkit XCP security vendors**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/story/0 ,10801,106759,00.html

SONY ROOTKIT PROBLEM RAISES QUESTIONS FOR SECURITY VENDORS

Sony BMG Music Entertainment has been lambasted for shipping its spywarelike XCP software on music CDs over the past year, but an important question has gone largely unanswered: Why didn't security vendors catch the problem sooner? Though one security vendor, Finland's F-Secure Corp., was aware of the problems surrounding Extended Copy Protection (XCP), none of the major anti-spyware or antivirus vendors had any idea that something was amiss, according to representatives from Symantec Corp., McAfee Inc., and Computer Associates International Inc. There were two things about XCP that presented challenges for the big security vendors. The first was Sony's use of rootkit techniques to cloak XCP and make it harder to circumvent its copy-protection capabilities. A second problem is that the software was distributed by a trusted company: Sony. Sony has sold an estimated two million CDs containing the copy-protection software, which used special rootkit techniques to hide itself on PCs. Rootkit software runs at a very low level of the operating system and is designed to be extremely difficult to detect. Ultimately, XCP's cloaking ability was used by hackers to write malicious software, a development that prompted Sony to recall its XCP CDs.

Category 28.2 Scumware

2005-12-06 **Sony BMG CD rootkit spyware scumware EFF computer security fix**

DHS IAIP Daily; http://news.com.com/New+Sony+CD+security+risk+found/2100−100 2_3− 5984764.html?tag=cd.lede

NEW SONY CD SECURITY RISK FOUND

Sony BMG Music Entertainment and the Electronic Frontier Foundation (EFF) digital rights group jointly announced Tuesday, December 6, that they had found, and fixed, a new computer security risk associated with some of the record label's CDs. The danger is associated with copy-protection software included on some Sony discs created by a company called SunnComm Technologies. The vulnerability could allow malicious programmers to gain control of computers that have run the software. The issue affects a different set of CDs than the ones involved in the copy-protection gaffe that led Sony to recall 4.7 million CDs last month. The announcement is the latest result of the detailed scrutiny applied by the technical community to Sony's copy-protected discs, after a string of serious security issues were found to be associated with the label's anti-piracy efforts. Following those revelations, the EFF asked computer security company iSec Partners to study the SunnComm copy protection technology, which Sony said has been distributed with 27 of its CDs in the United States. iSec found the hole announced Tuesday and notified Sony, but news of the risk was not released until SunnComm had created a patch. Sony patch: http://sonybmg.com/mediamax/ List of CDs affected: http://sonybmg.com/mediamax/titles.html

---

Category 28.2 Scumware

2006-04-11 **security risk Web Rebates spyware adware**

DHS IAIP Daily; http://www.it− 23 observer.com/news/6058/web_rebates_steals_conf idential_personal_information/

WEB REBATES SCUMWARE/SPYWARE A SECURITY RISK FOR COMPUTER USERS.

Security experts at MicroWorld Technologies are stating that a new variant of the "WebRebates" program, "Win32.WebRebates.s," is a serious security risk for computer users. WebRebates claims to offer rebates and discounts when purchasing items on Internet, however it's found to be a Spyware, Adware and a security hazard in many ways. This program monitors browser activity and other operations on your PC. It also pesters your computer with annoying pop-ups, apart from clogging your mailbox with spam. WebRebates comes bundled with many software utilities. Once installed, it tries to get additional malware from a series of Websites.

28.3 Keystroke loggers

Category 28.3 *Keystroke loggers*

1997-06-16 **privacy workplace monitoring**

Dow Jones, Wall Street Journal

The Japanese firms that controls the widespread 7-Eleven stores in the US proposed in June to equip their point-of-sale (POS) terminals with sophisticated monitoring software to track the rhythm and types of sales in all its stores — and to force managers to pore over these statistics daily.

Category 28.3 *Keystroke loggers*

2002-06-26 **keylogger Trojan confidentiality eavedropping data leakage espionage organized crime password user ID college university students**

NewsScan

RUSSIAN MOB TARGETS SOME U.S. COLLEGE COMPUTER SYSTEMS
A Russian-born man at Pasadena City College has been arrested as he tried to install keystroke-recording software to capture student credit card information, and Arizona State University officials found that a program had been surreptitiously installed to steal student credit card numbers, passwords, and e-mail. Linking these and other activities to Russian organized crime, the Secret Service and the Education Department have joined in issuing a general alert to American college computer centers. (AP/USA Today 26 Jun 2002)
http://www.usatoday.com/life/cyber/tech/2002/06/26/college-computers.htm

---

Category 28.3 *Keystroke loggers*

2003-02-10 **spying keystroke logger criminal prosecution case Boston College**

NIPC/DHS

February 06, CNET News — Ex-student accused of spying on campus.

A former Boston College student was indicted on Thursday for allegedly installing keystroke-recording software on more than 100 campus computers and accessing databases containing personal information on other students, staff and faculty. The case may be the first criminal prosecution of a person accused of unlawfully installing a key-logging device, which is designed to capture and record what a computer user types, including passwords and other private information. "I am very concerned about (key-logging software) given the enormous number of public access computers at schools, copy shops and libraries," said John Grossman, chief of the Massachusetts attorney general's corruption, fraud and computer crimes division. According to the attorney general's office, Boudreau began to install key-logging software around April 2002 and used intercepted information to add money to a stored-value card used in the campus dining and bookstore system. Boudreau is not, however, accused of misusing credit card numbers or profiting from selling any private information he allegedly gleaned. Universities have grown more worried about the possibility of key-loggers monitoring their systems, with the University of Illinois at Urbana-Champaign warning that the "Secret Service has advised us about several nationwide computer intrusions/hacking incidents." The charges against Boudreau include unauthorized access to a computer system, wiretapping, and breaking into a building at night "with intent to commit a felony." The last charge alone carries a penalty of up to 20 years in state prison.

Category 28.3 *Keystroke loggers*

2003-03-07 **criminal hackers keystroke loggers bank accounts theft**

NewsScan

SUSPECTS STEAL MONEY VIA KEYSTROKE MONITORING SOFTWARE
Two Japanese men were arrested for allegedly hacking into people's bank accounts and stealing $136,000. The men are accused of downloading software that detects the keystrokes made by a computer user and installed it on PCs at Tokyo cybercafés. They then figured out the passwords that five previous customers had used to access their bank accounts online, and transferred a total of $141,000 from those accounts to another bank. One of the men, 27-year-old Goro Nakahashi, then used an alias to withdraw $136,000. If charged with theft, the two could face up to 10 years in prison. According to the Asahi newspaper, the men allegedly tried to use about 100 computers at 13 different Internet cafes around Tokyo. (AP 7 Mar 2003)
http://apnews.excite.com/article/20030307/D7PKA2180.htm

Category 28.3 *Keystroke loggers*

2003-05-12 **Fizzer stealth worm KaZaA file-sharing P2P crackers Vxers anti-virus PC update Europe**

NIPC/DHS

May 12, The Register — Fizzer stealth worm spreads via KaZaA.

An Internet worm called "Fizzer" is spreading through the KaZaA P2P file-sharing network and as an executable file via e-mail. Reuters reported Monday that businesses in Asia were the first to report the attack, followed by reports of tens of thousands of infections in Europe. Fizzer is especially dangerous because it installs a keyboard-logging program that intercepts and records all keyboard strokes in a separate log file. To transmit this information, Fizzer loads a backdoor utility that allows crackers/VXers to control a computer via IRC channels. Additionally, the worm regularly connects with Web page located on the Geocities server from which it attempts to download updated version of its executable modules. In an attempt to foil detection, Fizzer also attempts to shut down an array of widely used anti-virus programs that might be running on a victim's PC. Computer users should keep their anti-virus software updated.

Category 28.3 *Keystroke loggers*

2003-10-10 **hacker security fraud Drexel University investment keystroke**

NewsScan

HACKER CHARGED WITH SECURITIES FRAUD
A 19-year-old student at Drexel University in Pennsylvania is being charged by the Securities & Exchange Commission (SEC) of fraud and identity theft for hacking into someone's investment account and making a complex and illegal trade. The student is accused of using a program called the Beast to monitor every keystroke typed on the target machine, and by doing so was able to obtain the log-in and password for the investor's online brokerage account with TD Waterhouse. (New York Times 10 Oct 2003)

Category 28.3 *Keystroke loggers*

2003-10-10 **spyware covert monitoring eavesdropping keylogger RAT fraud spam law enforcement parents ethics**

NYT
http://www.nytimes.com/2003/10/10/technology/10SPY.html?th=&pagewanted=print&position=

Rick Eaton, founder of TrueActive, altered his monitoring product to remove its "silent deploy" feature, which allowed secret installation of the surveillance software on the target machine via e-mail and without permission. He did so on ethical grounds. In contrast, more than a dozen other keystroke loggers persist in providing facilities for surreptitious installation.

Category 28.3 *Keystroke loggers*

2004-03-24 **first civil wiretapping case California key logger Key Katcher**

NewsScan

WIRETAP CASE FOCUSES ON KEYSTROKE RECORDING DEVICE

A California man has been charged with one count of wiretapping, becoming the first person in the U.S. to be charged with illegally using an electronic device to record someone's keystrokes. Larry Lee Ropp allegedly plugged a "Key Katcher" into the computer of a secretary at the insurance company where he worked. Key Katchers are commercially available and are marketed to parents who want to monitor their children's computer use. However, they are not legal when used on commercial property and when Ropp was fired for violating his company's time-clock policy, he called an employee and asked her to remove what he called a "toy" from the secretary's computer. Ropp was charged with wiretapping after the firm's technology department looked into the matter. A conviction could result in a maximum five-year prison sentence. (Los Angeles Times 24 Mar 2004)

Category 28.3 *Keystroke loggers*

2004-05-11 **hacking eavesdropping keyboards hardware**

DHS IAIP Daily; http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci963348,00.html

May 11, SearchSecurity.com — 'Whispering keyboards' could be next attack trend.

Eavesdroppers can decipher what is typed by simply listening to the sound of a keystroke, according to scientist Dmitri Asonov at this week's IEEE Symposium of Security and Privacy in Oakland, CA. Each key on computer keyboards, telephones and even ATM machines makes a unique sound as each key is depressed and released, according to the paper titled "Keyboard Acoustic Emanations." All that is needed is about $200 worth of microphones and sound processing and PC neural networking software. Today's keyboard, telephone keypads, ATM machines and even door locks have a rubber membrane underneath the keys. "This membrane 11 acts like a drum, and each key hits the drum in a different location and produces a unique frequency or sound that the neural networking software can decipher," said Asonov. Asonov found that by recording the same sound of a keystroke about 30 times and feeding it into a PC running standard neural networking software, he could decipher the keys with an 80% accuracy rate. He was also able to train the software on one keyboard to decipher the keystrokes on any other keyboard of the same make and model. Good sound quality is not required to recognize the acoustic signature or frequency of the key. In fact, Asonov was able to extract the audio captured by a cellular phone and still decipher the signal.

Category 28.3 *Keystroke loggers*

2005-11-28 **report keyloggers programs malicious software rampant Internet download**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1893515,00.asp

MALICIOUS KEYLOGGERS RUN RAMPANT ON NET

Keylogging programs are the epitome of online stealth, and they're also a mushrooming problem on the Internet. Reports of new keylogging programs soared higher this year, as part of a wave of multifunction malware with integrated keylogging features, according to VeriSign Inc.'s security information company iDefense Inc. The programs often evade detection by anti-virus tools and can be difficult to detect once installed, experts warn. More than 6,000 keylogging programs will be released by the end of this year, according to projections by iDefense. That's an increase of 2,000 percent over the last five years, company officials said. Keyloggers have been around for years and are also sold as legitimate applications -- often as monitoring tools for concerned parents or suspicious spouses -- according to Ken Dunham, director of malicious code at iDefense, in Reston, VA. Malicious keyloggers are increasingly part of modular programs that contain Trojan horse, spamming and remote control features, as well, Dunham said. Anti-virus companies have developed signatures that will stop many of those programs before they can be installed, but new programs with unique signatures are readily available from malicious code download sites.

Category 28.3 *Keystroke loggers*

2006-02-08 **keyloggers data leakage data theft fraud scam Trojans bank accounts international criminal hackers arrests**

http://www.theregister.co.uk/2006/02/08/france_keylogs_losses/

RUSSIAN KEYLOGGERS HIT BANK CUSTOMERS: FRENCH BANKS LOSE €1M

John Oates wrote in _The Register_:

"Russian scammers used key logging Trojans to steal more than a €1m from French people accessing online bank accounts. The Trojans were sent by email but were not activated until people accessed their online bank accounts. Then the Trojan forwarded on user names and passwords to the crooks. The thieves then used the details to transfer funds to third party *mule* accounts. The worst individual loss was €40,000. French police were told in November 2004 and the scam lasted 11 months. Arrests have been made in Moscow and St Petersburg and several *Ukrainian masterminds* have also had their collars felt."

Mr Oates pointed to an article in The Guardian at
< http://www.guardian.co.uk/france/story/0,,1703777,00.html >
by Kim Willsher with more details.

Category 28.3 Keystroke loggers

2006-05-15 **keyloggers spyware business enterprise strike Websense study**

DHS IAIP Daily; http://www.techweb.com/article/printableArticle.jhtml;jsessi 23
onid=NYTZFP2AMAGYQQSNDBGCKHSCJUMEKJVN?articleID=187203291
&si te_section=700028

KEYLOGGERS, SPYWARE CONTINUE TO STRIKE ENTERPRISES.

Nearly one in five enterprises have had workers' PCs infected with keyloggers, the worst kind of spyware, a survey released Monday, May 15 said. Keyloggers are a type of spyware, and are used to record keystrokes (and sometimes mouse movements as well) to capture information such as usernames and passwords. They're often planted on consumers' PCs by identity thieves, but are becoming a corporate problem, too. The poll, conducted by Harris Interactive for San Diego-based security vendor Websense, found that 17 percent of IT administrators said that one or more employees had launched a keylogger on their network. In last year's survey, only 12 percent of administrators had acknowledged that keyloggers infected their domains. Bots are also a major problem for corporations, as they are for consumers, the survey showed. Just over a third of administrators (34 percent) were confident that they could keep bots from infecting workers' PCs when those machines weren't connected to the company's network, while almost one in five (19 percent) said that they have had employees' work desktops or laptops hit by a bot.

28.4 Cell/mobile phones/GPS/cameras

Category 28.4 *Cell/mobile phones/GPS/cameras*

1997-02-02 **cellular phone privacy**

PA News

Civil liberties groups in Britain condemned the use of cell phones as "tags" allowing tracking of the carrier without permission.

Category 28.4 *Cell/mobile phones/GPS/cameras*

1997-02-09 **privacy cellular phones**

AAP

In Australia, the chair of the New South Wales Privacy Commission warned that cellular phones emit a tracking signal at least every half hour if they are on; such signals could be used by telecommunications companies or criminal hackers to track the phones. However, a spokesperson for Telstra, the Australian telecommunications company, said that such tracking is extremely difficult and expensive.

Category 28.4 *Cell/mobile phones/GPS/cameras*

1997-08-29 **cellular phone tracing privacy**

RISKS 19 35

British Telecom announced that the new MOSA (Mobile Social Alam) cellular phone will allow determination of its physical location to within 30 feet (about 10 m).

Category 28.4 *Cell/mobile phones/GPS/cameras*

1998-07-17 **privacy cellular phone location geographical monitoring**

EDUPAGE

FOR FBI, MOBILE PHONE ISSUE IS WHERE IT'S AT
Federal Bureau of Investigations director Louis J. Freeh wants the Senate Appropriations Committee to write legislation requiring phone companies to provide law enforcement officers the precise location of cellular phone users suspected of committing a crime. The officers would not even need a court order in the case of an "emergency" (such as suspicion of a felony, pursuit of a fugitive, or danger to human life). Current technology allows phone companies to get location information on any cellular phone that is turned on and operating within the cellular network — even if the user is not actually engaged in a phone call. The FBI plan is opposed both by the telecommunications industry, which says it would cost billions of dollars to implement, and by civil liberties groups, which consider it a dangerous and unconstitutional invasion of privacy. (New York Times 17 Jul 98)

Category 28.4 *Cell/mobile phones/GPS/cameras*

2003-06-17 **prevent theft gps matsushita bicycle**

NewsScan

BIKE HAS GPS TO PREVENT THEFT
An electric bicycle produced by National Bicycle, a Matsushita company, will have a Secom global positioning system (GPS) designed to guard against theft. The battery will simultaneously supply electricity to the bicycle and recharge the portable GPS unit. (Japan Today 17 Jun 2003)

Category 28.4 *Cell/mobile phones/GPS/cameras*

2004-08-18 **cell mobile phone clone tracking device South Korea electronic serial number ESN Find-Friend service**

DHS IAIP Daily;
http://english.chosun.com/w21data/html/news/200408/200408180 039.html

August 18, The Chosum Ilbo (South Korea) — Cloned cell phones used to trace personal locations.

The Ministry of Information and Communication (MIC) in South Korea has said that a total of 1,940 cloned phones were detected since last November. According to the MIC, cloned cell phones might help an unscrupulous person register himself as a friend of a targeted phone owner to trace his whereabouts. Every cell phone has a unique factory-set electronic serial number (ESN) and a cloned phone is one illegally programmed to have the identical ESN to the legitimate phone. After cloning, both the legitimate and the fraudulent phones have the same ESN and phone number, and cellular systems cannot distinguish the cloned cell phone from the legitimate one. This enabled the start of the Find-Friend service, a location-based service (LBS) provided by the nation's mobile operators, which was possible only after being explicitly agreed to by legitimate phone owners. Fraudulent phone holders are able to give their consent to mobile operators.

Category 28.4 *Cell/mobile phones/GPS/cameras*

2004-10-04 **mobile cell phone hacking attack vulnerabilities spying eavesdropping**

DHS IAIP Daily; http://news.bbc.co.uk/1/hi/technology/3712816.stm

October 04, BBC News — Latest mobiles open to attack. The latest generation of mobile phones is vulnerable to hackers, security experts have warned.

The warning was at an international conference on computer security in the Malaysian capital, Kuala Lumpur. According to the meeting's organizer, Dylan Andrew, loopholes in the software could allow hackers to scroll through a phone's address book by remote control and even eavesdrop on conversations. The mobile industry is aware of these security issues, said Sal Viveros, director of wireless security at McAfee. "I don't think people need to be too alarmed, but they should start asking their mobile operators to provide them with protection," he said.

Category 28.4 *Cell/mobile phones/GPS/cameras*

2005-07-11 **Cell phone service New York attack deadly bombs move bombings operation Madrid New Jersey Lincoln Holland tunnelssubway**

DHS IAIP Daily;
http://www.computerworld.com/mobiletopics/mobile/story/0,108
01,103125,00.html

CELL PHONE SERVICE DISABLED IN NEW YORK TUNNELS AFTER LONDON ATTACK

Cellular phone service has been shut off in four busy New York commuter tunnels since last week's deadly blasts in London, officials said Monday, July 11. No specific reason was given for the move, but cell phones have been used to trigger bombs in the past. Cell phone service is disabled in the Holland and Lincoln tunnels that connect Manhattan to New Jersey under the Hudson River, the Midtown Tunnel to the city's Queens borough and the Battery Tunnel to Brooklyn, officials said. The move came immediately after the bombings in London on Thursday, according to a spokesperson for the Port Authority of New York and New Jersey, which oversees operation of the Lincoln and Holland tunnels. In March 2004, bombs in Madrid that killed 191 people on trains were fitted to mobile phones, using the alarms as timers. Police in London have said they believe the subway bombs there were detonated by timers. A spokesperson for the New York Police Department said officials would weigh the benefits of disabled service against allowing cell phone service in the tunnels so the public could report suspicious packages or individuals.

Category 28.4 *Cell/mobile phones/GPS/cameras*

2005-07-11 **FCC ALLTEL Corporation Western Wireless Corporation licenses authorizations applications merger WWC Widgeon Acquisition LLC**

DHS IAIP Daily; http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC−259932 A1.pdf

FCC CONSENTS TO ALLTEL CORPORATION ACQUISITION OF WESTERN WIRELESS CORPORATION LICENSES AND AUTHORIZATIONS

The Federal Communications Commission (FCC) on Monday, July 11, consented to the applications filed in connection with the proposed merger of ALLTEL Corporation and Western Wireless Corporation (WWC) subject to certain conditions. The transactions would transfer the control of licenses held by WWC and its subsidiaries to Widgeon Acquisition LLC, a wholly-owned subsidiary of ALLTEL. The Commission denied all of the petitions filed in opposition to the merger, finding that the merger as conditioned would serve the public interest.

Category 28.4 *Cell/mobile phones/GPS/cameras*

2005-09-19 **data leakage countermeasure photography illicit surreptitious digital camera privacy**

INNOVATION

PHOTO-BLOCKING TECHNOLOGY

Paparazzi, beware! Researchers at Georgia Tech have come up with a way to prevent digital cameras and camcorders from taking surreptitious photos or video. The technology can detect the presence of a digital camera up to 33 feet away and then shoots a targeted beam of light at the lens, neutralizing the recorded image. The neutralizing light continues until the camera lens can no longer be detected. The group has developed a lab prototype consisting of a digital projector with a modified video camera mounted on the top, but team members say they're working on a design that could be commercially manufactured and sold. With the rise in cell phone cameras and other intrusive camera technology, they see the technology as a first step toward ameliorating privacy concerns that are escalating in the face of shrinking camera size, and anticipate that businesses, conferences and exhibit halls with no-photography rules will constitute a ready-made market. (CNet News.com 19 Sep 2005) <http://news.com.com/Crave+privacy+New+tech+knocks+out+digital+cameras/2100-7337_3-5869832.html>

Category 28.4 *Cell/mobile phones/GPS/cameras*

2006-02-05 **study cell phone tracking tools privacy surveillance espionage security threat**

EDUPAGE; http://news.com.com/2100-1039_3-6035317.html 23

CELL PHONES AS TRACKING TOOLS

Companies that use cell phones to track people have seen significant increases in business in the past few years. In Britain, firms such as Followus and Verilocation frequently work with employers who want to keep tabs on staff, despite concerns that the service infringes on individuals' civil rights. Kevin Brown of Followus noted that his company's service requires the consent of those being tracked. Users must agree to having their cell phones tracked, and periodic messages are sent randomly to users reminding them that their movements are being followed. Officials at Verilocation pointed to such events as the bombings in London last summer as times when being able to locate all of your employees is highly valuable. Experts on business processes said being able to track employees can allow companies to provide better service to customers by, for example, letting them know exactly where a technician is and when he will arrive at a customer's home. Officials from Liberty, a civil rights group, were unconvinced, saying that employees' rights in the workplace have been eroded and that there is a significant risk that businesses will misuse tracking data.

Category 28.4 *Cell/mobile phones/GPS/cameras*

2006-03-22 **Motorola phones buffer overflow security dialog spoofing vulnerabilities arbitrary command execution bypass security restrictions sensitive information disclosure**

DHS IAIP Daily; http://www.frsirt.com/english/advisories/2006/1045 23

MOTOROLA PHONES BUFFER OVERFLOW AND SECURITY DIALOG SPOOFING VULNERABILITIES.

Two vulnerabilities have been identified in various Motorola cell phones, which could be exploited by attackers to execute arbitrary commands, bypass security restrictions, and disclose sensitive information. Analysis: The first issue is due to a buffer overflow error when handling an overly long OBEX "setpath()" sent via the OBEX File Transfer service, which could be exploited by an attacker to crash a vulnerable handset or potentially execute arbitrary code via a paired device. The second flaw is due to an input validation error when handling incoming connection to the "Headset Audio Gateway" on Channel 3 from a remote Bluetooth device, which could be exploited by attackers to spoof the device name displayed in security dialogs and convince a user to accept an incoming connection. Affected products: Motorola PEBL U6 and Motorola V600. Solution: The FrSIRT is not aware of any official supplied patch for this issue.

Category 28.4 *Cell/mobile phones/GPS/cameras*

2006-03-29 **spy program cell phone snoop call log text messages F-Secure Trojan label FlexiSpy**

DHS IAIP Daily; 23
http://news.com.com/Spy+program+snoops+on+cell+phones/2100−1 029_3−6055760.html?tag=nefd.top

SPY PROGRAM SNOOPS ON CELL PHONES.

New software, called FlexiSpy, released in March by Bangkok, Thailand-based Vervata, hides on cell phones and captures call logs and text messages. It is being sold as a way to monitor kids and spouses. The data captured is sent to Vervata's servers and is accessible to customers via a special Website. Security company F-Secure has labeled the software a Trojan. "This application installs itself without any kind of indication as to what it is," Jarno Niemela wrote on the Finnish antivirus maker's corporate blog Wednesday, March 29. In addition, FlexiSpy could be used by miscreants as part of malicious software that targets phones, Niemela wrote.

28.5 Serial numbers

Category 28.5 Serial numbers

1999-01-22 **privacy chip serial identifier processor e-commerce**

Washington Post, San Jose Mercury News, New York Times, AP, New York Times 20 19
http://www.nytimes.com/library/tech/99/04/biztech/articles/29chip.html; RISKS

A storm of protest erupted when Intel innocently announced what it thought would be a useful feature: software-accessible microprocessor serial numbers. Apparently unaware that minicomputer and mainframe manufacturers have provided such a feature for decades, privacy activists — including in particular the Electronic Privacy Information Center <http://www.epic.org> — appealed to the FCC to stop what they perceived as a nefarious plan to invade consumer's privacy. Intel's Pentium III chip includes a software-accessible serial number, just like LAN interface cards and many other kinds of processors long used in industry. Civil libertarians protested that such a unique identifier would allow detailed tracking of an individual's usage of the Internet. Bowing to protests, the company later agreed to set the default for this feature to "off." Critics than insisted that the mere availability of the feature would put pressure on consumers to turn it on; as Deirdre Mulligan of the Center for Democracy and Technology said, "If everybody's demanding it, it's going to be hard for a consumer to say no." Later in February, Junkbusters Corp. and EPIC (Electronic Privacy Information Center) appealed to the Federal Trade Commission for a ruling forbidding the chip from being released. The FTC declined to cooperate. The situation was inflamed by the discovery in late February that the software switch could be activated remotely, without permission of the PC owner. In late February, a German magazine, Computer Technology, published reports that the feature could be hacked to change the unique identifier, thus allowing a breach of authenticity by altered computers. Pentium determined that the problem lay in the software it had released.

Category 28.5 Serial numbers

1999-03-08 **privacy confidentiality signature imprint serial number**

BENTON PROJECT; EDUPAGE; AP

MICROSOFT TO RID WINDOWS OF TRACKING NUMBERS
Issue: Privacy
Richard M. Smith, a computer programmer, compares it to a Social Security number being stamped on every document a person creates on a computer operating with the Microsoft Windows 98 operating system. "It" is a unique 32-digit serial number that is generated in the latest version of Windows and planted within electronic documents. It could be used to trace the author's identity. Microsoft officials said they are investigating whether the company is collecting the serial numbers from customers even if they explicitly indicate they didn't want them disclosed. "If it is, it's just a bug," said Robert Bennett, Microsoft's group product manager for Windows. "If it is indeed happening, we'll absolutely fix that." Bennett said Microsoft will create a software tool to let customers remove the Windows number, which he said is meant to help diagnose problems for customers who call with technical problems. Privacy activist Jason Catlett of Junkbusters said, "This is going to be a cleanup job larger than the Exxon Valdez oil spill." [Bug...or feature?] [SOURCE: Washington Post (A8), AUTHOR: Ted Bridis (Associated Press)] <
http://www.washingtonpost.com/wp-srv/business/feed/biztop920897272397.htm>

MICROSOFT RESPONDS TO PRIVACY ISSUE
Reacting to a controversy started when a programmer in Brookline, Mass., discovered Windows 98 generates a unique serial number that is implanted in every electronic document and that can be used to trace the identify of its author, Microsoft said it will create a software tool to allow customers to remove the number, which was created to help support specialists diagnose problems for customers who call with questions. Jason Catlett, who lobbies on privacy issues, says, "This is going to be a cleanup job larger than the Exxon Valdez oil spill. There are billions of tattooed documents out there." (AP 8 Mar 99)

MICROSOFT OFFERS PRIVACY FIX
Microsoft Corp. has two free software programs on its Web site that will strip out the identifying number that could be used to trace the authorship of some electronic documents. One program removes the number from existing documents and the other prevents it from being embedded in new documents. The number feature was included as part of Windows 98, but privacy advocates complain that the feature makes it technically possible for the company to trace documents to a specific computer, even if the author wishes to remain anonymous. Microsoft says the numbers originally were intended to support a feature to link documents over a network, but it was never fully developed. See <
http://officeupdate.microsoft.com/Articles/privacy.htm > (AP 19 Mar 99)

Category 28.5 *Serial numbers*

1999-04-04 **information warfare privacy virus serial number stamp Word**

THE NEW YORK TIMES NEWS SERVICE

As the search for the author of Melissa, generally accepted to be someone calling himself "Vicodin ES," continued, investigators discovered a serial number in the vector document, written with MS-Word. The undocumented serial number not only helped law enforcement catch the perpetrator (30-year-old programmer David L. Smith of Aberdeen, NJ) it also caused a fuss among privacy activists world wide. Amitai Etzioni, a professor at George Washington University and author of _Limits of Privacy_, said, "The No. 1 threat today to privacy is not Big Brother, it's big bucks."

Category 28.5 *Serial numbers*

1999-04-29 **Pentium serial number Trojan diagnostic Intel vulnerability**

New York Times

INTEL GOES TO BATTLE AS ITS EMBEDDED SERIAL NUMBER IS UNMASKED
Intel tried to resolve issues about the controversial serial number embedded in its Pentium III processors by providing software meant to hide the number, but a researcher has discovered that the number can be made visible even with the software. A researcher at Canadian software company Zero-Knowledge Systems found that the serial number could be made visible again without the Pentium III user's knowledge. Zero-Knowledge then placed a program on its Web site to demonstrate the software's flaw to the public. Intel responded to Zero-Knowledge's program earlier this month by telling Symantec, which makes the Norton Antivirus software, that the program was "hostile code." Zero-Knowledge says Symantec's virus warning on its Web site damaged its business, and maintains that Intel should not have used a serial number to protect user security. (New York Times 04/29/99)

28.6 RFID tags

Category 28.6 *RFID tags*

2003-07-21 **surveillance radio frequency RFID GPS Wozniak WiFi**

NewsScan

WOZNET: APPLE COFOUNDER COMES BLAZING BACK
Beginning with an interest in finding a way to track his lost dogs, Apple co-founder Steve Wozniak developed location-monitoring technology using electronic tags and designed to help people keep track of their animals, children or property. The new company, Wheels of Zeus, is touting WozNet as a simple and inexpensive wireless network that uses radio signals and global positioning satellite data to keep track of a cluster of inexpensive tags within a one- or two-mile radius of each base station. Its low-power network will complement rather than compete with other wireless technologies such as radio-frequency I.D. tags used in stores and factories and higher speed Wi-Fi and cellular data networks. WozNet, with data rates of no more than 20,000 bps, will be able to transmit a very small amount of digital information even through environments subject to radio interference, and will be able to location information from global positioning system (GPS) satellites. (New York Times 21 Jul 2003)

Category 28.6 *RFID tags*

2003-07-25 **Intel Alzheimer RFID patient tracking artificial intelligence system**

NewsScan

INTEL, ALZHEIMER'S ASSOCIATION TEAM UP ON PATIENT CARE
Intel has formed a consortium with the Alzheimer's Association to fund research on new ways to improve the care of Alzheimer's patients, such as using a combination of sensors and wireless technologies to monitor the patient, thereby freeing up the caregiver to tackle some chores. "If you are a caregiver, this is really empowering technology," says Eric Dishman, director of proactive research at Intel. Intel says it is also investigating the use of radio frequency identification (RFID) tags on items that the patient uses every day, such as a coffee cup or plate. The tags could track activity patterns for each object, and a link to an artificial intelligence system could generate prompts via the radio or TV on what to do with it (i.e., instructions for making coffee or washing a dish and putting it away). The Everyday Technologies for Alzheimer Care will fund more than $1 million worth of new research. (San Jose Mercury News 25 Jul 2003)

Category 28.6 *RFID tags*

2003-10-03 **tracking books RFID people privacy EFF**

NewsScan

TRACKING LIBRARY BOOKS OR TRACKING PEOPLE?
The Electronic Frontier Foundation (EFF), which concerns itself with civil liberties issues in cyberspace, is expressing dismay over a plan by the the San Francisco Public Library use RFID technology to track books. A RFID (radio frequency identification) chip would be inserted into each library book, and would send out electromagnetic waves that would allow tracking of the book's location. San Francisco's city librarian Susan Hildreth says the RFID devices will help streamline inventory and prevent loss, and explains that tracking people is not the goal; "It will not allow us to track people to their home or any location." Hildreth's response has failed to satisfy Electronic Frontier Foundation Lee Tien, who worries: "We're talking about the imbedding of location trafficking devices into the social fabric." (AP/USA Today 3 Oct 2003)

Category 28.6 *RFID tags*

2004-01-25 **radio frequency identification RFID IBM Philips logistics tracking**

NewsScan

IBM AND PHILIPS TEAM UP ON RFID TAGS

IBM and Philips Electronics are moving ahead on an emerging computer-based logistics system that is expected to help retailers reduce their inventory-tracking costs. Philips will manufacture the RFID (radio frequency identification) tags that can be attached to items ranging from clothes to milk cartons, while IBM will provide the computer services and system. Analysts predict that in a few years' time, RFID tags will come down in price to just a few cents apiece or less, and will be capable of storing information such as a product description, packaging and expiration dates, color and price. Research groups say that excess inventory of consumer goods and retail items valued at $40 billion is in the supply chain at any given time and they estimate that use of advanced tracking systems such as RFID could help reduce theft and excess inventory levels by 25%. According to Applied Business Intelligence, the RFID market could reach $3.1 billion by 2008, while IDC estimates that retail demand alone will be $1.3 billion within four years. (Reuters/CNet News.com 25 Jan 2004)

Category 28.6 *RFID tags*

2004-02-19 **radio frequency ID RFID FDA tags prescription drugs**

NewsScan

FDA CALLS FOR RFID TAGS TO TRACK DRUGS

A report released last week by the U.S. Food and Drug Administration calls RFID (radio frequency identification) tags as the most likely technology to spur "mass serialization" of prescription drugs, which it describes as "assigning a unique number (the electronic product code or EPC) to each pallet, case and package of drugs and then using that number to record information about all transactions involving the product." A unique number would act as an "electronic pedigree," guaranteeing information on the drug's authenticity, where it was intended for sale and whether it was previously dispensed. The agency has presented plans to test and adopt RFID tracking throughout the prescription drug industry, with feasibility studies slated for this year and full scale rollout at the case and pallet level by 2007. Wal-Mart stores plans to get a head start, using RFID tags to track all controlled substance medications dispensed by its pharmacies this year. (Computerworld 19 Feb 2004)

Category 28.6 *RFID tags*

2004-03-02 **currency security features RFID urban myth hoax microwave explode burn**

RISKS; http://www.prisonplanet.com/022904rfidtagsexplode.html 23 24

RFID TAGS IN $20 BILLS? EXPLODING IN MICROWAVES?? WHO KNOWS???

A controversy, ah, exploded in March 2004 when "prisonplanet.com" published an article from two anonymous contributors claiming that new $20 bills from the US Treasury contain an RFID tag positioned in the image of Andrew Jackson's right eye. Carrying a stack of such bills sets of RFID detectors in stores, said the letter; wrapping them in aluminum foil prevented detection. Microwaving the bills in a stack in a microwave caused all the RFIDs to explode.

Skeptics pointed out that the publisher had to back off and write, "We want to make it clear that $20 bills will only 'pop' or 'explode' in certain microwaves." Critics suggested that the image shown on the Web site seems to consist of _old_, not new, $20 bills (that is bills not containing the security features described in < http://www.globalsecurity.org/security/library/news/2003/10/sec-031009-usia02.htm >).

The discussion then devolved into name-calling and insults.

[MK comment: this debacle could have been avoided by running controlled trials with old used $20 bills, old unused $20 bills, new used $20 bills and new unused $20 bills. Microwaving some used and unsused dollar bills might have provided useful information too. Comparing the effects of stacks of such different sorts of bills on RFID detectors would not have exceeded human capabilities either.]

Category 28.6 *RFID tags*

2004-03-05 **radio frequency RFID tags privacy consumer profiling issues**

NewsScan

WILL RFID TAGS TAG BOOKS OR READERS?

Radio frequency identification (RFID) tags — tiny devices that broadcast data about any object in which they're embedded — have been proposed as a way of improving inventory control in San Francisco's library system; however, some critics of RFID technology fear that it will be used as an invasion of the personal privacy of library patrons. Ann Brick of the ACLU says, "Privacy is really the handmaiden of the First Amendment," and Lee Tien of the Electronic Frontier Foundation warns: "Now is the time to seriously worry about the government using RFIDs to track people." But Kathy Lawhun, chief of the city's main library and a proponent of the RFID proposal, suggests that the critics are getting way ahead of themselves: "RFID is simply a chip with an antenna. You can have as little or as much as you want on that chip." (AP/USA Today 5 Mar 2004)

Category 28.6 *RFID tags*

2004-05-03 **RFID ID air travel Transportation Security AuthorityTSA**

DHS IAIP Daily; http://releases.usnewswire.com/GetRelease.asp?id=132−
0503200 4

May 03, U.S. Newswire — TSA announces eight airports participating in Access Control Pilot Program.

Rear Adm. David Stone, Acting Administrator for the Transportation Security Administration (TSA), on Monday, May 3, announced that eight airports have been selected to participate in TSA's Access Control Pilot Program which will test Radio Frequency Identification (RFID) technology, Anti-Piggybacking technology, advanced video surveillance technology and various biometric technologies. The airports are Boise Air Terminal/Gowen Field Airport (BOI), Boise, ID; Miami International Airport (MIA), Miami, FL; Minneapolis-St. Paul International Airport (MSP), Minneapolis, MN; Newark International Airport (EWR), Newark, NJ; Savannah International Airport (SAV), Savannah, GA; Southwest Florida International Airport (RSW), Ft. Myers, FL; T. F. Green State Airport (PVD), Providence, RI; and Tampa International Airport (TPA), Tampa, FL. TSA has developed a two-phase pilot program starting with Phase I, including these initial eight airports testing various off-the-shelf biometric technologies under a variety of real-world operational environments in an effort to provide unbiased evaluations of their suitability of use.

Category 28.6 *RFID tags*

2004-07-02 **radio frequency identification tags job loss unemployment**

NewsScan

RFID COULD COST 4 MILLION JOBS BY 2007

The Yankee Group, a prominent market research firm, is predicting that RFID tags will cost four million U.S. jobs by 2007, throughout numerous industries. (RFID stands for Radio Frequency Identification, a technology embedded for inventory and tracking purposes into products, materials, and shipments.) However, Yankee Group analyst Adam Zabel thinks that most workers who lose their jobs due to increased efficiencies made possible by RFID technology will be able to obtain 'more value-added' positions. (Vnunet 2 Jul 2004)

Category 28.6 *RFID tags*

2004-07-12 **radio frequency identification RFID schoolchildren Japan privacy**

NewsScan

RADIO KIDS IN JAPAN

School officials in the Japanese city of Osaka will soon be using RFID technology to monitor the movements of their pupils. (The acronym stands for radio frequency identification.) The tags, which will be read by readers installed at various key locations throughout a school, will be placed on the children's schoolbags, name tags, or clothing. (CNET 12 Jul 2004)

Category 28.6 *RFID tags*

2004-07-14 **radio frequency identification RFID employees Mexico corruption scanner**

NewsScan

GOT YOU UNDER MY SKIN: RFID USED TO TAG EMPLOYEES

RFID tags have been implanted under the skin of Mexico's top federal prosecutors and investigators to give them quick access to restricted areas inside a new federal anti-crime information center. The chips also could provide more certainty about who accessed sensitive data at any given time. (In the past, the biggest security problem for Mexican law enforcement has been corruption by officials themselves.) The microchip tags lie dormant under the skin until read by an electromagnetic scanner, which uses a technology known as radio frequency identification (RFID) that's now commonly used for inventory control. (San Jose Mercury News 14 Jul 2004)

Category 28.6 *RFID tags*

2004-10-13 **radio frequency identifier implant microchip FDA medical RFID patient pets access control**

NewsScan; http://apnews.excite.com/article/20041013/D85MJ8I83.html

FDA APPROVES MEDICAL MICROCHIPS

The Food and Drug Administration has okayed an implantable radio frequency microchip that can transmit information on a patient's medical history to doctors in the event of an emergency. VeriChips, made by Applied Digital Solutions, are already in use as a way to track wayward pets and livestock, and nearly 200 people working in Mexico's attorney general's office have had the chips implanted in order to access secure areas. The tiny chips, which are embedded under the skin with a syringe, are programmed with a code similar to the UPC codes on retail goods, which releases patient-specific information on such issues as allergies and prior treatments when scanned.

Category 28.6 *RFID tags*

2004-10-14 **RFID radio freqency identifier Vatican books library anti-theft inventory**

NewsScan;
http://www.cnn.com/2004/TECH/10/14/spark.rfid.vatican/index.html

VATICAN TAPS RFID TECHNOLOGY TO TRACK BOOKS

The Vatican Library has tagged about 30,000 of its books with RFID (radio frequency identification) tags since last year, and says plans call for tagging 2 million of the 40- million piece collection in the near future. That would enable the staff to complete the library's annual inventory in less than a day -- a task that previously forced it to close for a whole month. Emilia Di Bernardo, VP of Seret, the company that installed the RFID system, says initially the Vatican staff were interested only in an efficient inventory process. "But we came up with something that is not only an inventory but a way to manage the books. This way staff always know where all the books are." Di Bernardo says it is relatively inexpensive to maintain the system and the technology does not harm the books in any way. "The most expensive part is the tags and the hardware." The RFID tags cost between five and 10 cents each, but Texas Instruments, which manufactures the tags, anticipates the costs coming down. "It's robust and as the price comes down, you will see it being used more and more, including in bus ticketing and concert ticketing," says a TI spokesman.

Category 28.6 *RFID tags*

2004-10-21 **RFID radio freqency identifier passport**

NewsScan; http://www.wired.com/news/privacy/0,1848,65412,00.html

U.S. PASSPORTS GET CHIPPED

Beginning in January, diplomats and U.S. State Department employees will be issued passports containing embedded RFID chips that will contain the individual's name, address, date and place of birth, and a digital photo. Ordinary citizens applying for new passports will get the high-tech version starting in the spring. Civil liberties advocates have called the new passports a "privacy horror," and point out that even if the data were encrypted (and it's not), it would still be very easy to steal. "If 180 countries have access to the technology for reading this thing, whether or not it is encrypted, from a security standpoint, that is a very leaky system," says Electronic Frontier Foundation attorney Lee Tien. "Strictly from a technology standpoint, any reader system, even with security, that was so widely deployed and accessible to so many people worldwide will be subject to some very interesting compromises." Meanwhile, a travel privacy expert says that in addition to identity thieves, commercial travel companies, including hotels, will capture the data when people check in or exchange currency. Intel RFID expert Roy Want says those fears are overblown, but acknowledges some theft is possible: "In principle someone could rig up a reader, perhaps in a doorway you are forcing people to go through. You could read some of these tags some of the time."

Category 28.6 *RFID tags*

2004-10-21 **privacy VeriChip consumers Dixon RFID radio frequency identifier**

NewsScan; http://www.christiansciencemonitor.com/2004/1021/p13s01-stct.html

DESCENT FROM PRIVACY: A 'SLIPPERY SLOPE'

Pam Dixon, executive director of the World Privacy Forum, warns: "Most consumers don't fully understand the tradeoffs they're making with privacy." As an example, she argues that the potential widespread use of the VeriChip -- a tiny radio transmitter inserted under a person's skin -- is "a nightmare situation" for privacy, because at first workers might be induced to wear the devices simply to get high-security jobs but that eventually the transmitters would be much more broadly required: "All of a sudden it becomes mandatory for certain classes of people. I just see this as an extremely slippery slope."(Christian Science Monitor 21 Oct 2004)

Category 28.6 *RFID tags*

2004-11-19 **RFID radio freqency identifier FDA medical surgery SurgiChip identification patient quality assurance error avoidance**

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/10226986.htm

MAKE INCISION HERE: RFID TAG USED IN SURGERY

The U.S. Food and Drug Administration has approved use of radio frequency ID (RFID) tags to ensure that physicians perform the right surgery on the right patient. Manufactured by SurgiChip Inc., the radio tag is encoded with the patient's name and the site, type, and date of the surgery; the patient helps stick the adhesive-backed tag near the site of the surgery and workers in the hospital's operating room scan the tag to compare that information with the patient's chart. (AP/San Jose Merury News 19 Nov 2004)

Category 28.6 *RFID tags*

2005-02-10 **RFID radio freqency identifier elementary school ACLU track surveillance privacy civil liberties**

NewsScan; http://apnews.excite.com/article/20050210/D885RJD81.html

CONTROVERSIAL USE OF RFID TECHNOLOGY IN ELEMENTARY SCHOOL

Brittan Elementary School in rural Sutter, California, is requiring students to wear radio frequency identification (RFID) badges that can track their movements in order to simplify attendance-taking, curtail vandalism, and improve student safety. But civil libertarians are alarmed, and ACLU representative Nicole Ozer warns, "If this school doesn't stand up, then other schools might adopt it. You might be a small community, but you are one of the first communities to use this technology." Angry parent Michael Cantrall, who alerted the ACLU to the school's decision to use RFID technology, which is also used to track merchandise, says: "There is a way to make kids safer without making them feel like a piece of inventory. Are we trying to bring them up with respect and trust, or tell them that you can't trust anyone, you are always going to be monitored, and someone is always going to be watching you?" Each student is required to wear identification cards around their necks with their picture, name and grade and a wireless transmitter that beams their ID number to a teacher's handheld computer when the child passes under an antenna posted above a classroom door. But the IDs have been welcomed by some parents, such as one who notes: "This is not Mayberry. This is Sutter, California. Bad things can happen here." (AP 10 Feb 2005)

* * *

NO RFID TAGS FOR SCHOOL KIDS -- AT LEAST FOR NOW

The InCom company, which developed Radio Frequency Identification (RFID) tags to monitor the whereabouts of school children, has pulled out of a deal with Brittain Elementary School in Sutter, California. School principal Earnie Graham says, "I'm disappointed… I think I let my staff down. Nobody on this campus knows every student." Dawn Cantrall, the parent who objected to the system and brought the ACLU in to stop its implementation, remains skeptical: "I'm not convinced it's over. I'm happy for now that kids are not being tagged, but I'm still fighting to keep it out of our school system. It has to stop here." The system was conceived as a way of simplifying attendance-taking, reducing vandalism, and keeping students safe. (San Francisco Chronicle 16 Feb 2005)

http://sfgate.com/cgi-bin/article.cgi?file=/n/a/2005/02/16/financial/f075453S34.DTL

Category 28.6 *RFID tags*

2005-02-11 **radio frequency identification tag RFID school children monitoring surveillance tracking**

RISKS; http://www.msnbc.msn.com/id/6448213/did/6942751/ 23 71

RFID TAGGING ELEMENTARY SCHOOL CHILDREN

Peter Coffin and Peter Neumann summarized a new application for RFID tags:

The only grade school in Sutter, California is requiring students to wear radio frequency identification badges that can track their every move. Some parents are outraged, fearing it will rob their children of privacy. The badges introduced at Brittan Elementary School on 18 Jan 2005 rely on the same radio frequency and scanner technology that companies use to track livestock and product inventory.

While similar devices are being tested at several schools in Japan so parents can know when their children arrive and leave, Brittan appears to be the first U.S. school district to embrace such a monitoring system.

Civil libertarians hope to keep it that way.

I trust no one reading RISKS has any troubles imagining many ways to foil this system. "Karen, I wanna ditch. Carry my tag in your backpack?"

Category 28.6 *RFID tags*

2005-08-02 **identification authentication I&A Social Security Number SSN card RFID radio frequency identification device identity theft legislation proposal Congress**

RISKS 23 96

MISSING THE POINT: RFID TAGS IN SOCIAL SECURITY CARDS

Geoff Kuenning analyzed a misguided application of RFID tags:

I just received an e-mail from my Congressman, David Dreier, touting his efforts to put RFID chips in Social Security cards. Dreier, never noted for clear thinking, writes:

>There is a common sense solution to thwarting identity theft and the fraudulent use of Social Security cards: the cards must be made counterfeit-proof… H.R. 98…improves the integrity of the Social Security card by adding a digitized photo of the cardholder. These Smart Cards will also contain a unique electronic encryption code that will allow employers to verify each applicant's work eligibility prior to hiring. Smart Cards will decrease Social Security information theft and prevent illegal immigrants from using fake or stolen Social Security information to get a job.<

Note that HR 98 doesn't do anything to actually address identity theft, which isn't performed using Social Security cards in the first place. Sensible measures, like making the Social Security Number self-checking, decoupling it from identification, and penalizing corporations who fail to protect SSNs or who misuse them, are notably absent. Instead we have yet another case of technology as a panacea.

But in the current hysterical climate, and with the popular fascination with overhyped technology, I have no doubt that the bill will pass. I also have no doubt that it will have no effect on its true target, illegal immigration, since it will be easy to find low-paid insiders to help forge the "impossible to forge" cards.

Category 28.6 RFID tags

2006-03-15 **RFID security computer virus infection paper terrorism evade scanners**

DHS IAIP Daily; 23
http://www.nytimes.com/2006/03/15/technology/15tag.html?ex=1
300078800&en=24f421ff24864376&ei=5090&partner=rssuserland&em c=rss

STUDY SAYS CHIPS IN ID TAGS ARE VULNERABLE TO VIRUSES.

A group of European computer researchers have demonstrated that it is possible to insert a software virus into radio frequency identification tags (RFIDs), part of a microchip-based tracking technology in growing use in commercial and security applications. In a paper entitled, "Is Your Cat Infected With a Computer Virus?," to be presented Wednesday, March 15, at an academic computing conference in Pisa, Italy, the researchers plan to demonstrate how it is possible to infect a tiny portion of memory in the chip, which can hold as little as 128 characters of information. Until now, most computer security experts have discounted the possibility of using RFID chips to spread a computer virus because of the tiny amount of memory on the chips. Ultimately, by their research, they have introduced a series of worrisome prospects, including the ability of terrorists and smugglers to evade airport luggage scanning systems that will use RFID tags in the future.

29 Sociology of cyberspace

Category 29 *Sociology of cyberspace*

2004-07-31 **weblog blog Internet writing Webpage disintermediation business information security customer partner sharing**

NewsScan

BUSINESS BLOGGING GOES MAINSTREAM

Major technology companies such as Microsoft and IBM are endorsing blogging as a means of enhancing companies' communications channels while at the same time eyeing them as potential profit-boosters. At a recent conference held at the University of California Berkeley's Haas Business
School, IBM Almaden Research Center director James Spohrer outlined his company's plans for integrating blogging into its employee communication strategies: "It's about decreasing social space between employees, and increasing the amount of knowledge shared between people." An example might contain some of an individual's educational background and work experience, as well as information on product development strategies that colleagues and customers can access around the clock. This sharing of information could spur feedback on efforts to produce new products and improve business processes, said Spohrer. Meanwhile, some analysts are looking at the marketing potential inherent in blogging. "Blogs are a way to put a human face on the company," because of the continuous interaction and relationships that employees can develop with blog-readers, says Forrester Research analyst Charlene Li. (Reuters 31 Jul 2004)

29.1 Addiction, games & violence

Category 29.1 *Addiction, games & violence*

1998-01-06 **Internet addiction dependency**

EDUPAGE

In Eustis, FL, the LifeStream Behavior Center counseling group began a program in January to help Internet addicts. In February, research published in the _CyberPsychology and Behavior_ journal suggested that college students are particularly at risk for such psychological dependence.

Category 29.1 *Addiction, games & violence*

1998-08-30 **Internet culture psychology depression false wrong**

EDUPAGE

The NSF funded a $1.5M study over two years at Carnegie Mellon University to understand the effects of Internet usage on users. Their startling finding was that increased Internet usage (e-mail, chat rooms, newsgroups and so on) decreased social interactions in the real world and caused an increase in depression. This study was severely criticized on methodological grounds within a week of its publication; one problem was the small sample size (169) and doubts about the applicability of the data drawn from a non-random sample in a single city, Pittsburgh.

Category 29.1 *Addiction, games & violence*

1998-09-15 **e-commerce research sociology psychology**

EDUPAGE

Scientists at a meeting sponsored by the NSF strongly advocated further fundamental research into the social effects of e-commerce.

Category 29.1 *Addiction, games & violence*

1998-12-14 **Internet addiction women depression**

Reuters

According to a study of 445 Internet users by the British psychologists Drs Helen Petrie and David Gunn of the University of Hertfordshire, "Women seemed to be more addicted to the Net than men were. They showed more positive feelings about using the Net and higher usage of the Net than men." The results were presented to the December meeting of the British Psychological Society in London. "Addicted" people spent an average of about 55 hours a week surfing, compared with self-described non-addicts, who spent half that amount (about 28 hours a week). Although the study did show a correlation between measures of depression and the amount of use of the Net, it was not possible from this study to ascertain the existence of a causal link; possibly depressed people liked to use the Net more or possibly using the Net more resulted in depressing people.

Category 29.1 *Addiction, games & violence*

1999-02-03 **virtual reality sickness neurological damage perception VR**

EE Times via CMP News via PointCast

Michigan State University researchers found measurable neurological effects from prolonged exposure to virtual reality systems. Doctors using VR systems to gain information about a patient's anatomical details during knee surgery took 10 minutes to adapt to the slight spatial displacement of the image from the real knee; however, the distorting neuromuscular coordination effects of the head-mounted display units lasted 30 minutes after the doctors removed the VR rig.

Category 29.1 *Addiction, games & violence*

1999-02-20 **Internet stalker harrassment junk e-mail fantasy violence**

Guardian (UK)

A survey by Novell in Britain revealed that "58% of men and 41% of women who use the Internet have been persistently stalked on it." An article in the Guardian newspaper by Sara Hall reported that the problem is exacerbated by the large number of new users who do not know enough to conceal personal information in public forums on the Net. Secondly, the large number of users means that the tiny percentage of weirdoes now constitute a significant number of people who harass others.

Category 29.1 *Addiction, games & violence*

1999-03-15 **computer ethics government program proposal**

AP

In March, Janet Reno encouraged government and industry to work on teaching ethical behavior in cyberspace. [I call it integrating cyberspace into children's — and our own — moral universe.]

Category 29.1 *Addiction, games & violence*

1999-04-03 **virus writers sociology psychology studies motivation**

NEW YORK TIMES NEWS SERVICE

Sarah Gordon, a respected anti-virus researcher working for IBM, commented that malicious code is all over the Net: "It's like candy - a child can get these, a 12-year-old can get these. It's trivial," she said. "All you do is download it to a computer, click on it, and there you go." Evidence supports the view that a growing number of virus writers and distributors are juveniles. On the other hand, some virus writers protest what they describe as simplistic generalizations. One fool going by the pseudonym "Attitude Adjuster" wrote, "The idea that all of us out here are malicious teen-agers is quite a fallacy. There are those of us who still exist in the community who write viruses because it's fun. We don't give our viruses to the public and nobody gets hurt."

Category 29.1 *Addiction, games & violence*

1999-09-27 **geek nerd computer fanatic hacker syndrome psychology**

LA Times

Gary Chapman published an interesting article in the LA Times suggesting that some fanatical users of computers calling themselves "geeks" or "nerds" (or maybe "hacker") may in fact have symptoms of clinical syndromes similar to some forms of autism. Specifically, writes the author, "Unlike classic autism, which often involves mental retardation and a lack of verbal skills, Asperger's syndrome is at the `high functional' end of the spectrum of autistic behavior, experts say. People with Asperger's syndrome have normal or above-average IQs and may even display savantism, or exceptional abilities in a specific skill. What they lack is human empathy, a deficiency sometimes called `mind-blindness,' which shows up as a distinct inability to read routine human nonverbal cues of attitude such as kindness, anger or love. Asperger's syndrome patients, who usually develop their traits at a young age, often have these tendencies: excellent rote memory; fascination with fantasy worlds and arcane facts; facility with math and science; physical awkwardness or clumsiness and sometimes an unusual gait; hyperactivity but with an ability to focus on interesting problems for hours at a time; poor social understanding; hyper-verbal activity but without the ability to make contextual connections in conversations; and an appearance of insensitivity and eccentricity. They are commonly victims of teasing in school. And, apparently, some can do well in the computer world." However, some experts in the field claim that such interpretations are bunk, pointing out that most Asperger's Syndrome kids are severely debilitated.

Category 29.1 *Addiction, games & violence*

2000-03-01 **cybersex addiction syndrome habit**

NewsScan, New York Times http://www.nytimes.com/aponline/a/AP-Online-Sex.html

Psychologists from Stanford and Duquesne universities have published an article in the journal Sexual Addiction and Compulsivity claiming that at least 100,000 users are cybersex compulsives who spend more than 11 hours a week visiting X-rated Web sites and chat rooms. The study concludes: "This is a hidden public health hazard exploding, in part, because very few are recognizing it as such or taking it seriously." The researchers believe that cybersex compulsives have difficulty maintaining normal relationships with others. (AP/New York Times 1 Mar 2000)

Category 29.1 *Addiction, games & violence*

2000-09-19 **allergy toxic computer equipment plastic contamination**

NewsScan, TechServer http://www.techserver.com/noframes/story/0,2294,500259402-500399748-502393843-0,00.html

Chemicals from computer screens can provoke allergies, according to a Swedish study published . . . [18 Sep] in the journal Environmental Science and Technology. Researchers from Stockholm University say the chemical compound triphenyl phosphate, a flame retardant widely used in the plastic of video monitors and computers, can cause allergic reactions such as itching, nasal congestion and headaches. The problem arises when the temperature of the screen or video monitor begins to rise, says the study's lead author. "We have focused our interest on this compound since it has been proven to be a contact allergen to man and due to the fact that a number of workers in Sweden have acquired health problems related to computer work." Significant levels of the compound were found in more than half of the 18 computer brands tested by researchers, who recommend lots of ventilation to alleviate the problem. (Agence France Presse/Nando Times 19 Sep 2000)

Category 29.1 *Addiction, games & violence*

2000-10-02 **socioeconomic factors digital divide availability bandwidth access knowledge skills**

NewsScan

As many as 50 million U.S. adults are at risk for becoming functionally illiterate in the coming years because they're technologically deprived, according to a Gartner Group study. "The Internet will soon be so pervasive that not having access to the technology or not knowing how to use it will be the equivalent of not knowing how to read or write," . . . [said] Gartner CEO Michael Fleisher. The report confirms the existence of a "digital divide" that denies 65% of "lower socioeconomic-status" Americans access to the Internet, compared with only 17% in the top income bracket. But beyond simple access, a second "experience gap" separates people knowledgeable enough to tap the benefits of the Internet from those who are not. Meanwhile, a third divide is developing between those with high-speed, broadband access and those stuck with straight dialup accounts. "As broadband access reaches higher penetration rates, we can expect to see a gap in broadband adoption that mirrors today's gaps in (personal computer) ownership. This will be the equivalent of having the moderate and upper classes in IMAX theaters while the underprivileged are still watching silent movies," says Fleisher. (Reuters/MSNBC 2 Oct 2000)

Category 29.1 *Addiction, games & violence*

2001-06-07 **information overload study coping**

NewsScan

INFORMATION OVERLOAD IS A STATE OF MIND
A new study titled "The Next Big Thing" found surprising anecdotal evidence that people who receive the greatest volume of electronic information reported a greater ability to cope, while the group that feels the most overwhelmed has the least amount of data to deal with. "We went into the survey expecting to find people were really struggling. We were surprised to find they were thriving," says the study's publisher, Josh Clark. "Anecdotally, there are people out there who are feeling overwhelmed, but practice makes perfect. The people who are most comfortable practice dealing with high volumes of information, and they are coping beautifully." The study's authors caution that because their response group was predominantly male with 42% working in the technology sector, its results cannot be extrapolated to the entire U.S. population. Nevertheless, the comparatively high response rates for the study mean the results are meaningful, and the results bear out what previous studies and empirical evidence has shown -- that simplicity is the key to success in the technology age. (Newsbytes 7 Jun 2001)
http://www.newsbytes.com/news/01/166615.html

Category 29.1 *Addiction, games & violence*

2001-07-22 **Internet cyberspace culture games children effects benefits harm obsession addiction**

NewsScan

COMPUTER GAMES BOOST KIDS' ABILITIES
Computer games can boost children's coordination and ability to concentrate, putting them on a par in those categories with top-level athletes, according to a study by the UK government's Economic and Social Research Council. "People who play games regularly seem to develop a mental state that we have seen before only in serious athletes or professionals such as astronauts, whose life depends on concentration and coordination," says Jo Bryce, who led the research. "Their minds and bodies work together much better than those of most other people." Bryce found that although a minority of gamers become obsessive, the majority have a healthy mix of other interests and varied social lives. "Our subjects were averaging about 18 hours a week on computer games, which sounds a lot, but they were spending similar amounts of time reading and doing sport or socializing," says Jason Rutter of the Center for Research on Innovation and Competition at Manchester University. A recent study by Britain's Home Office also showed that those who regularly played computer games when young were more likely to be intelligent, to attend a university, and to get a better-than-average job. (The Sunday-Times 22 Jul 2001)
http://www.sunday-times.co.uk/news/pages/sti/2001/07/22/stinwenws03005.html

---

Category 29.1 *Addiction, games & violence*

2001-07-23 **psychology depression loneliness Internet user profile research study**

NewsScan

SOME ARE HAPPY SURFERS, SOME ARE SAD
A new study by Carnegie Mellon University psychologist Robert Kraut, who claimed three years ago that Internet use led to depression, says that Internet use can no longer be correlated with depression or loneliness but can add to the stress people feel (as "just another thing on their to-do list"). Kraut 's research has convinced him that the Internet deepens the prevailing mood of both extroverts (who become livelier) and introverts (who become lonelier the more time they spend online, and look to the Internet less for social contact than for entertainment). The study findings are unsurprising to Vanderbilt University psychologist and e-commerce expert Donna Hoffman, who says that people are "going to use computers in a predictable way, based on the kind of person they are." (USA Today 23 Jul 2001)
http://www.usatoday.com/life/cyber/tech/2001-07-23-web-depression-study.htm

---

Category 29.1 *Addiction, games & violence*

2002-02-26 **online sex cybersex addiction survey**

NewsScan

ADDICTED TO "ADULT" SITES
An online survey by the San Jose Marital and Sexuality Centre reports that 10% of the 7,037 individuals responding to the survey say they are addicted to cybersex. Other data: Neilsen/NetRatings figures indicate that there were 27.5 million U.S. visitors to adult-oriented sites last month; of that number, 72% were men and 28% women. (USA Today 25 Feb 2002)
http://www.usatoday.com/life/cyber/tech/2002/02/26/cybersex.htm

---

Category 29.1 *Addiction, games & violence*

2002-07-01 **electronic auction fanatics fans addicts enthusiasts groupies**

NewsScan

EBAY BELIEVERS IN LOVE WITH MEG
Online auctioneer eBay now has 50,000 million customers, a great many of whom don't think of themselves as customers at all, but as entrepreneurs, pioneers, and friends. They honor Pierre Omidyar, who founded the company in 1995, and are in love with Meg Whiman, eBay's billionaire chief executive officer. Marketing professor Eugene Fram of Rochester Institute of Technology explains: "These are innovation junkies -- like the people who used to follow the Grateful Dead around the country. Every day, fifty thousand new people participate in eBay auctions, and the company insists that, despite the fears of skeptics, eBay will never let its search for corporate customers interfere with its commitment to individual buyers and sellers, who built the company's success and who continue to generate excitement for its mission." At a recent convention of 5,500 eBay lovers, one eBay junkie enthused: "It's like a reunion of people you've never met." (USA Today 30 Jun 2002)
http://www.usatoday.com/life/cyber/2002/07/01/ebay.htm

Category 29.1 *Addiction, games & violence*

2002-08-23 **Internet addiction survey study**

NewsScan

ONE IN FOUR U.S. WORKERS ADDICTED TO THE NET
Twenty-five percent of U.S. employees report that they are addicted to going online, according to a survey conducted by Websense, although only 8% of companies polled report any knowledge of workplace Internet addiction. According the report, these workers spend more than one entire workday each week accessing non-work-related Web sites. The top five types of sites labeled most addictive were: shopping, news, pornography, gambling and online auctions. The study reports that while 78% of workplaces have installed filters to prevent employees from accessing pornography while at work, only 47% block access to gambling sites. Employers are generally reluctant to block access to news sites, with only 4% reporting they had done so. (Nua Internet Surveys 22 Aug 2002)

Category 29.1 *Addiction, games & violence*

2002-09-03 **sociology pathology games role-playing online harassment anti-social behavior**

NewsScan

GRIEFERS RELISH THE DARK SIDE OF CAMELOT
Griefers — online game players who focus on the indiscriminate slaughter and ridicule of other gamers — have caught the attention of game makers such as Sony, Microsoft and Electronic Arts, who worry that these bad sports will jeopardize the rise of online games by scaring away customers willing to spend $10 to $14 a month to subscribe to the online gaming experience offered by titles such as "EverQuest" and "Dark Ages of Camelot." These games offer players rich, immersive, fantasy worlds where they can acquire virtual jobs, adopt pets, marry and own property. Rather than a shining city on a hill, however, the online Camelot has quickly descended into anarchy, where stealing, killing, taunting and other forms of bullying are used to torment novice players. For a griefer, this is what it's all about — not the killing, but the misery they inflict afterward. "Griefers feed on the negative reactions of the people they kill," says one self-proclaimed bully. "There's nothing sweeter than when you kill someone and they spout insults at you for hours. That's when you know you got him. It sounds really cruel, but it's fun." And while game makers have tried to isolate anti-social behavior by setting up safe zones where players can't be harmed and filters that reject obscene and graphic names, the griefers continually find ingenious ways to get around them. The result is a cat-and-mouse game that has become tremendously costly for game developers at the same time they are planning to significantly expand their online offerings. "We're trying to take a whole new generation of players online who have never been there before," says the director of content services for Microsoft's Xbox. "We want to make sure everyone has a good experience." The griefer's response? "Everybody needs a bad guy." (Los Angeles Times 2 Sep 2002)

Category 29.1 *Addiction, games & violence*

2002-09-24 **Internet addiction work policies acceptable use survey**

NewsScan

NEWS SITES SERVE UP 'ADDICTIVE' CONTENT
Workers who surf on the job report that they visit online news sites more often than pornography, gambling, or even online auction sites, and that they consider news one of the most addictive types of content available on the Web, according to a survey by Websense. "Initially we saw the most abuse in pornography and gambling sites, now we are seeing more time spent on shopping and news sites," says Websense CTO Harold Kester. Twenty-three percent of those surveyed cited news as the most addictive Web content, compared with 24% who chose shopping, 18% who picked pornography, 8% for gambling and 6% for online auctions. Meanwhile, employers don't seem too perturbed over their workers' penchant for current events. Sixty-seven percent said there were no restrictions in the office on reading news online. That compared with 37% who allowed access to shopping and auction sites, and a slim 2% who didn't mind if their employees visited gambling and porn sites while on the clock. Workers reported spending 8.3 hours a week — 20% of their worktime — on Internet sites that had no relation to their jobs, and most said they would rather give up coffee than the Internet. (Reuters/CNN.com 23 Sep 2002)

Category 29.1 *Addiction, games & violence*

2003-02-12 **computer game psychology sociology community**

NewsScan

COMPUTER GAMES ARE GOOD FOR YOU
Playing computer games can be beneficial, say researchers studying the complex social interactions inherent in the popular online multiplayer shoot-em-up Counter-Strike. Professor Talmadge Wright and colleagues at Loyola University in Chicago say that Counter-Strike is much more than just racking up "kills," with the strategies and tactics used by many regular players approaching the complexity of those used in chess. And although much of the banter reflects the typical trashtalk of teenage boys, it's a mistake to dismiss the gamers as misguided misanthropes. "The most common emotion when people are playing is laughter," says Wright. In fact, games like Counter-Strike that rely on trust and cooperation give rise to strong communities and friendships, he adds. "It gives people an option of actively participating in some kind of fantasy role they could not do in real life that allows them to play with their own feelings. It is an area that's bricked off from everyday life that you can enter and leave at will. It offers you a way to play with things you may be scared of in a safe way where there are very few consequences." For these reasons the games are good for players, says Wright, who suggests that many studies of game-playing have been skewed by hidden agendas. "There's a cultural motif that underlies the critiques that go on around this, the idea of mindless activity is given short shrift in culture where productivity is given the highest praise." (BBC News 12 Feb 2003)
http://news.bbc.co.uk/1/hi/technology/2744449.stm

Category 29.1 *Addiction, games & violence*

2003-02-24 **data recovery disk drive crash psychological counselling**

NewsScan

PSYCHOLOGICAL HELP FOR COMPUTER MELTDOWN VICTIMS
Here's the latest in data recovery services — DriveSavers, a technology firm that specializes in recovering data from even the most devastated computer system, employs a full-time crisis counselor to help customers work through their trauma. "People get upset — very, very upset," says Kelly Chessin. "They yell. They cry. They need someone to listen to them and let them vent. That's what I'm here for." When customers go berserk on the phone, Chessin steps in and tries to help them calm down before an engineer comes on the line to discuss the technical aspects of the problem. Chessin says her experience working for a suicide hot line is invaluable in helping distraught customers deal with data disaster. "It's similar. But when people call a hot line, you need to help them find their own solutions. Now I can offer solutions to people's problems." Another difference? People who seek help from DriveSavers frequently call Chessin back to thank her for being there. "That's really nice," she says. (San Francisco Chronicle 23 Feb 2003)

Category 29.1 *Addiction, games & violence*

2003-03-04 **text messaging children spelling**

NewsScan

TEXT MESSAGE ESSAY BEWILDERS BRITISH TEACHER
A 13-year-old's "How I Spent My Summer Vacation" essay proved to be almost indecipherable to her poor teacher. "I could not believe what I was seeing. The page was riddled with hieroglyphics, many of which I simply could not translate," the teacher told the Daily Telegraph newspaper. The girl's essay began: "My summr hols wr CWOT. B4, we used 2go2 NY 2C my bro, his GF & thr 3 :- kids FTF. ILNY, it's a gr8 plc." For those who had trouble reading that, here's a translation: "My summer holidays were a complete waste of time. Before, we used to go to New York to see my brother, his girlfriend and their three screaming kids face to face. I love New York. It's a great place." The text messaging craze is partially to blame for a decline in grammar and written English abilities, says Judith Gillespie of the Scottish Parent Teacher Council. "Pupils think orally and write phonetically." (Reuters/CNN 3 Mar 2003)

Category 29.1 *Addiction, games & violence*

2003-03-17 **spell checker software errors dependence**

NewsScan

BEWARE THE SPELLCHECKER
A study at the University of Pittsburgh reveals that the ubiquitous spellchecker software may be doing as much harm as good, when it comes to writing. In the study, 33 undergraduate students were asked to proofread a one-page business letter — half of them using Microsoft Word, with its spell- and grammar-checking features and the other half using only their brains. Without the software, students with higher SAT verbal scores made, on average, five errors, compared with 12.3 errors made by students with lower scores. However, using the software, the two groups made about the same number of errors — 16 vs. 17. Dennis Galletta, a professor of information systems at the Katz Business School, says people have come to rely on spellchecking software too completely. "It's not a software problem, it's a behavior problem." (AP 14 Mar 2003)
http://apnews.excite.com/article/20030314/D7POQ7R80.htm

Category 29.1 *Addiction, games & violence*

2004-04-28 **Internet addiction usage monitoring employee usage IT addition**

NewsScan

COFFEE CAN WAIT -- GIVE ME MY NET!

Given the choice between going online or enjoying a morning cup of coffee, almost half of workers polled (49%) say they'd forgo the java, according to a survey by Websense. But the response signals trouble ahead for employers, who fear that productivity is suffering as a result of workers' Net addiction. While 51% of employees surveyed said they spent only about two hours a week on personal Web surfing, IT managers pegged the number at a far higher six-plus hours a week. IT managers also expressed concern over network security when employees took their laptops home with them. "Some employees take their laptops home and use their own time to download a movie. They may access a site where there's spyware or a virus and then they bring their laptop back to work and don't realize they've exposed people on their network," says Kian Saneii, VP of marketing at Websense. (CNet News.com 28 Apr 2004)

Category 29.1 *Addiction, games & violence*

2004-07-08 **Iraq war image picture JPEG online news newpapers graphic viewership Americans US**

NewsScan

AMERICANS FLOCK TO GRAPHIC WAR IMAGES ONLINE

About one in four American Internet users sought out graphic war images that were deemed too gruesome to display in conventional media such as newspapers and television, according to new research by the Pew Internet Project. The results were drawn from a telephone survey conducted between May 14 and June 17 -- a period that encompassed such disturbing events as the murder and dismemberment of American contract workers in Fallujah, the exposure of prisoner abuse at Abu Ghraib, and the capture and beheading of U.S. civilian Nicholas Berg. Survey respondents reported mixed feelings after viewing the images -- 51% said they felt they'd made a good decision to access the images, but a third said they wished they hadn't seen them. "Millions of Internet users want to be able to view the graphic war images and they see the Internet as an alternative source of news and information from traditional media. But many who do venture outside the traditional and familiar standards of the mainstream news organizations to look at the images online end up feeling very uncomfortable," says report co-author Deborah Fallows. Women in particular seemed more troubled over the entire issue of graphic online images, while younger adult Internet users tended to approve their availability. (Pew Internet Project News Release 8 Jul 2004)

Category 29.1 *Addiction, games & violence*

2004-08-02 **cyber life trend academia college university student lifestyle Internet IM surfing laptop brain information storage retrieval**

NewsScan

JUST A MINUTE -- MY BRAIN IS BOOTING UP

Increasingly, college students are toting their laptops to class and using them as retrieval mechanisms for information they haven't yet managed to store in their carbon-based brain cells. The phenomenon was predicted 40 years ago by Marshall McLuhan, who suggested that people's senses were extending outside of their bodies, in the way a book was an extension of the eye and a car was the extension of a foot. Internet researcher Sherry Turkle has documented this latest evolutionary trend in her book "Life on the Screen" where she describes a typical college student's study habits -- the text book is open, the CNN news ticker is flickering across the TV screen, the headphones are pumping out the latest alternative rock, and the student's fielding IM messages as he/she surfs the Web. "Real life is just one more window," says one multitasking student. (CNN.com 2 Aug 2004)

Category 29.1 *Addiction, games & violence*

2004-08-04 **conscripts Finland army military draft Internet addiction unfit serve**

NewsScan

FINLAND DISMISSING 'NET-ADDICTED' CONSCRIPTS

A growing number of conscripts have to be dismissed from Finland's armed forces every year due to an Internet addiction that makes them unsuited for service. A Finnish official says: "It's an increasing problem. More and more young people are always on the Internet day and night. They
get up around noon and have neither friends nor hobbies. When they get into the army, it's a shock to them." There are no specific figures and the military has yet to give the condition a proper dismissal code in its health records. (The Age, 4 Aug 2004) Rec'd from J Lamp

---

Category 29.1 *Addiction, games & violence*

2004-08-07 **sociology cyberspace psychology disorder Website Internet e-commerce marketing**

NewsScan

A SICK TRADE

The phenomenon of weborexics first became apparent about three years ago with the emergence of so-called pro-ano, or pro-anorexia, Web sites. But they've taken a sinister turn, with several sites cashing in by selling pro-ano merchandise, including teddy bears, "ana" bracelets and tank tops with slogans such as "nothing eaten, nothing gained." Pro-anos are one of the more disturbing online communities because of their promotion of anorexia as a lifestyle choice and badge of honor. The Web sites typically contain a weight-loss weblog, a how-to guide with tips on starving and purging, and "trigger pictures" of thin celebrities. Many of the homepages and forums have been disabled but a plethora of sites can still be easily found. Anorexics can now go online and for between $3 and $25 buy a red-beaded "ana" bracelet -- a symbol of solidarity that identifies them to the rest of the community. The bracelets are designed to help anorexics resist their hunger by being worn on the hand used to eat with. (The Age 7 Aug 2004) rec'd from John Lamp, Deakin U.

Category 29.1 *Addiction, games & violence*

2004-08-09 **technology syndrome Internet e-mail cell phone PDA Britain**

NewsScan

TECHNOLOGY CAUSING 'FRANTIC LIFE SYNDROME'

Working women in the U.K. think new technology makes their lives even more hectic, according to a new report. The advent of mobile phones and e-mail have left women feeling under greater pressure to juggle work and home commitments, leaving less time for themselves. As a result, a growing number of career women are suffering from what has been dubbed "frantic life syndrome." Research conducted for Good Housekeeping magazine found 30% of working females had regularly been driven to exhaustion by work and home commitments. The problem is even more acute for those living in London, where the figure rises to 47%. Some of the biggest gripes are on the subject
of technology designed to make life easier. (The Age 9 Aug 2004) Rec'd from J Lamp

---

Category 29.1 *Addiction, games & violence*

2004-08-13 **technology addiction family life children kids study sruvey**

NewsScan

TECHNOLOGY KEEPS U.K. KIDS AWAY FROM FAMILY LIFE

British children are interacting less and less with their families and spending more time in their bedrooms watching television or playing computer games, according to a study published on Friday. Three-quarters of Britain's 11-14 year-olds have a television in their bedroom, almost two-thirds a DVD player or video recorder, and a quarter have a computer in their room, market research firm MINTEL said. Two-thirds of those surveyed said they played computer games in their rooms, and one in three said they only ever played the games alone. "Many of today's children now seem to be
experiencing greater isolation from family life," MINTEL consumer analyst Jenny Catlin said. "Sadly, it does seem that in many cases modern technology has now replaced the family unit, so that everyone does whatever they want, when they want, even if it means doing it on their own." (The
Age, 13 Aug 2004) rec'd from John Lamp, Deakin U.

Category 29.1 *Addiction, games & violence*

2004-12-09 **sociology virtual addiction Greenfield chats instant messaging games hyperstimulation children adolescents teenagers**

NewsScan; http://www.latimes.com/technology/ats-ap_technology10dec09

GET UNPLUGGED

Enough is enough, say experts who think young people need to get a life beyond the Internet. Psychologists Michelle Weill and Larry Rosen write, "It's like being lost in space. You get lost in the world of the Internet, games or multiple instant-message chats." Dave Greenfield, another psychologist specializing in high-tech issues argues: "Until technology gets 'stupid simple,' equivalent to turning on a light or a television set, it's going to eat time and energy. Do I have the right adapter? Or the right battery? Or cable?" Noting that many people buy the latest high-tech gizmos whether they need them or not, Greenfield says: "It points to a larger theme in our culture -- that new things are good and better, and that more is better, and faster is better. And that's not always the case." He's the author of a book called "Virtual Addiction." (AP/Los Angeles Times 9 Dec 2004)

Category 29.1 *Addiction, games & violence*

2004-12-16 **Illinnois videogames crime rental sell**

NewsScan; http://www.latimes.com/technology/la-na-videogame16dec16

ILLINOIS LEGISLATION TO REGULATE OVER-THE-TOP VIDEOGAMES

Illinois may be the first state in the country to regulate the sale and rental of violent and "adult" videogames, including ones such as "Grand Theft Auto: San Andreas," where players kill cops, steal cars, solicit prostitutes and then beat them to get their money back. Two bills being promoted by Illinois Gov. Rod Blagojevich would make it a crime for retailers to rent or sell such violent or sexually graphic material to minors. The videogame industry seems ready to shrug off the governor's proposals, and a spokesman for the Video Software Dealers Association says, "Every time there's a major new release, or a new release of technology, you see new attempts to regulate this industry." (Los Angeles Times 16 Dec 2004)

Category 29.1 *Addiction, games & violence*

2005-09-27 **virus plague cyber-terrorism role-playing game malware infection bug quality assurance QA testing patch vandals**

http://www.securityfocus.com/print/news/11330

GOOD GRIEF: GAMING VANDALS AS CYBER-TERRORISTS

The vandals called _griefers_ who infest computer-based role-playing games took advantage of a new feature called "corrupted blood" in the popular World of Warcraft game community. The feature was originally supposed to be limited to characters in a specific dungeon but the griefers teleported the infected characters into cities and infected pets. As a result, entire cities were depopulated as the plague spread from character to character. The Blizzard Entertainment programmers running the game -- presumably the equivalents of gods -- issued patches that shut down the pandemics. Robert Lemos, writing in SecurityFocus, quoted a game-playing security consultant, Brian Martin, as saying, "Giving it the ability to propagate at all beyond a limited environment definitely reminds us that self-propagating code is likely to bite us in the ass without careful consideration and planning. . . . This also underscores the fact that adequate testing is a requirement for software, as this--and thousands of other bugs--would have easily been discovered and hopefully fixed had the testing been more thorough."

29.2 Cyberdating & cybersex

Category 29.2 *Cyberdating & cybersex*

2002-12-11 **Internet browsing searching male chauvinism sexism**

NewsScan

BATTLE OF THE SEXES MOVES TO CYBERSPACE
A survey conducted by search engine AltaVista reveals that male chauvinism is alive and well on the Internet, with 80% of men polled claiming to be better at Web surfing than their female counterparts. Men also admit to being backseat drivers, interfering with their partners while they try to surf the Web, and of those who experienced the impatience and frustration of "Net rage," two-thirds were men. "As information has become such a valuable commodity, it's not surprising that men have transferred their traditional hunter-gatherer role to hunting for information on the Web," says Open University psychologist Dr. Adam Joinson, who adds it's unlikely that men actually are better at Web surfing than women. "I'd be surprised if men's self-perceived superiority is grounded in fact." (BBC News 11 Dec 200)
http://news.bbc.co.uk/1/hi/technology/2562601.stm

Category 29.2 *Cyberdating & cybersex*

2005-01-11 **Internet sociology anonymity role-playing psychology addiction fantasy reality**

NewsScan; http://www.nytimes.com/2005/01/11/health/psychology/11secr.html

'ON THE INTERNET, NO ONE KNOWS YOU'RE A DOG'

Psychologists believe that secret role-playing may be good or bad, depending on the circumstances. Harvard psychology professor Daniel M. Wegner says: "In a very deep sense, you don't have a self unless you have a secret, and we all have moments throughout our lives when we feel we're losing ourselves in our social group, or work or marriage, and it feels good to grab for a secret, or some subterfuge, to reassert our identity as somebody apart." The Internet is famous for accommodating people with multiple personalities, and MIT sociologist and author Sherry Turkle says, "It used to be you'd go away for the summer and be someone else, go away to camp and be someone else, or maybe to Europe and be someone else" -- whereas now many people now use online interactive games to set up families they wish they had or to play out alternative versions of their own lives. "I think what people are doing on the Internet now has deep psychological meaning in terms of how they're using identities to express problems and potentially solve them in what is a relatively consequencefree zone." In further defense of secret lives, New York clinical psychiatrist Jay S. Kwawer says, "Contrary to what many people assume, quite often a secret life can bring a more lively, more intimate, more energized part of themselves out of the dark." (New York Times 11 Jan 2005)

Category 29.2 *Cyberdating & cybersex*

2005-02-07 **anonymity Internet romance chat room**

NewsScan; http://theage.com.au/articles/2005/02/07/1107625114716.html

A MODERN VALENTINE'S DAY FABLE

A budding romance between a Jordanian man and woman turned into an ugly public divorce when the couple found out that they were in fact man and wife, state media reported on Sunday. Separated for several months, boredom and chance briefly reunited Bakr Melhem and his wife Sanaa in an internet chat room, the official Petra news agency said. Bakr, who passed himself off as Adnan, fell head over heels for Sanaa, who signed off as Jamila (beautiful) and described herself as a cultured, unmarried woman -- a devout Muslim whose hobby was reading, Petra said. Cyberlove blossomed between the pair for three months and soon they were making wedding plans. To pledge their troth in person, they agreed to meet in the flesh near a bus depot in the town of Zarqa, northeast of Amman. The shock of finding out their true identities was too much for the pair. Upon seeing Sanaa-alias-Jamila, Bakr-alias- Adnan turned white and screamed at the top of his lungs: "You are divorced, divorced, divorced" -- the traditional manner of officially ending a marriage in Islam. "You are a liar," Sanaa retorted before fainting, the agency said. (The Age 7 Feb 2005)

Category 29.2 Cyberdating & cybersex

2005-03-14 **Internet increase gambling college students poker tournaments**

EDUPAGE; http://www.nytimes.com/2005/03/14/education/14gamble.html

INTERNET FUELS GAMBLING AMONG COLLEGE STUDENTS

Gambling is seeing a significant upsurge among college students in the United States, a trend many attribute to the combination of television coverage of glitzy poker tournaments and the availability of gambling Web sites. Poker tournaments are showing up on campuses including Columbia University and the University of North Carolina, with waiting lists of students hoping to participate. A poker society at the University of Pennsylvania receives hundreds of responses during the first 30 minutes after a tournament is announced, according to the group's president. Some students, such as Princeton University senior Michael Sandberg, have made large amounts of money--in the past six months, Sandberg has won $30,000 in Atlantic City and another $90,000 playing cards online--and have come to regard gambling as an attractive and lucrative career option. Keith S. Whyte, executive director of the National Council on Problem Gambling, commented that university administrators are not working to raise awareness of the risks of gambling, nor are they offering resources for how to get help, which they do for issues such as substance abuse or date rape. New York Times, 14 March 2005 (registration req'd)

29.3 Digital divide

Category 29.3 *Digital divide*

2002-07-05 **digital divide international Linux personal computer PC Internet**

NewsScan

INDIA'S CHEAP NEW HANDHELD "SIMPUTER"
India's new "Simputer" -- a handheld computer whose name was chosen to suggest that it is simple, inexpensive, and multilingual -- will cost between 10,500 to 23,000 rupees ($214-469), in a country where the average per capita income is about $450. Using a Linux operating system, the device will have applications for voicemail, text-to-speech translation, and Internet access, and will be powered by an Intel StrongARM processor and two AA batteries. Random-access memory options will be 32 or 64 megabytes. The Simputer was designed by engineers at Encore Software and professors from the Indian Institute of Science in Bangalore, and will be marketed through a few large Indian technology companies. (Reuters/San Jose Mercury News 5 Jul 2002)
http://www.siliconvalley.com/mld/siliconvalley/3605609

Category 29.3 *Digital divide*

2002-07-18 **digital divide children access power international**

NewsScan

WHEN YOU COME TO A DIGITAL DIVIDE, LEAP OVER IT
And how do you do leap over the digital divide? By concentrating not so much on computer literacy -- but rather on computer power. In 1993, with money from Intel, MIT Media Lab professor Mitchel Resnick helped establish the first site of what is now an international network of 50 Computer Clubhouses, which are places where boys and girls 8 to 18 can "really feel in charge of the technology." Resnick says, "Access is not enough. Access is just a starting point. It's not about playing games, but about making your own games. It's not about surfing the Web, but it's about making your own Web pages. It's not just about downloading MP3 music files, but doing your own music composition." The clubhouse network has a $32 million commitment from Intel through 2005, in addition to hardware, software and services donated from Adobe, Macromedia, HP, Autodesk, and other companies. The network extends throughout the world, and includes such countries as Ireland, Israel, India, Germany, the Netherlands, and the Philippines. (New York Times 18 Jul 2002)

Category 29.3 *Digital divide*

2002-07-23 **digital divide international usage survey study**

NewsScan

CHINA IS NO. 3 IN INTERNET USERS
Exceptionally strong growth in Internet use over the past year has vaulted China to the No. 3 position in the world in terms of online population numbers. A 72% increase since last year translates to 45 million Chinese citizens now logging on regularly, even as the government still struggles with how to control subversive content. Only the U.S. and Japan have more citizens online, according to a report from the China Internet Network Information Center, an industry group funded by the Information Industry Ministry. The average Chinese user spends eight hours and 20 minutes online each week, and while Internet formerly was concentrated among academics, 68% of current users do not have college degrees. "The Internet is now coming closer to common people," says the People's Daily newspaper. (AP 23 Jul 2002)
http://apnews.excite.com/article/20020723/D7KUIAUG1.htm

Category 29.3 *Digital divide*

2002-08-27 **digital divide international access**

NewsScan

HINDI CHATBOT OPENS INTERNET TO MILLIONS
Computer science students in India have developed an interactive software program fluent in Hindi that could demystify computers for millions of Indian citizens. "The good thing about Deepti [the program] is that it is suitable for the Indian environment," says Ritvik Sahajpal, one of the students who worked on the program. "Deepti speaks in Hindi and since the majority of the people in India are computer illiterate and don't speak English, this feature is really great." The students say Deepti could be used to make government services more accessible, or it could be linked with touchscreen technology so that people with little or no knowledge of computers could use Internet kiosks. (BBC News 27 Aug 2002)
http://news.bbc.co.uk/1/hi/technology/2209775.stm

Category 29.3 *Digital divide*

2002-09-04 **digital divide international technology telecommunications Internet Africa report**

NewsScan

NewsScan editors John Gehl and Suzanne Douglas published an interesting report from their special correspondent Wilcliff Sakala, who is based in Zambia, on information technology in Africa. Some highlights:

* Africa is progressing on the road to integrate Information and Communication Technologies.

* In East Africa, the IT market value is set to expand at a compound annual growth rate (CAGR) of 21 per cent between 2000 and 2004.

* Tanzania will lead the growth rate in East Africa, with a forecast 28 per cent ($135 million) CAGR by 2004.

* Uganda will follow, registering a 25 per cent CAGR in the same period, totaling $63 million.

* Since 1991, telephone penetration in Least Developed Countries (LDCs) has risen from 0.3 to 1.1 per 100 people.

* Nigeria is drastically expanding its telecommunications infrastructure with the development of a more democratic government.

* Zimbabwe's three cellular providers have a subscriber base of more than 300,000, and the private operators have more lines than the State's fixed phone network.

* South Africa has the largest number of Internet subscribers in Africa, accounting for more than 80 per cent of the continent's estimated 2.6 million Internet users.

* Poverty presents another big challenge towards efforts to provide communication facilities to the majority of people in Africa. Innovative products include pre-paid packages, and phone shops that services previously under-serviced high-density and rural areas.

* Since 2000, Tunisia's mobile penetration has more than tripled, recording 4.01 per cent at the end of 2001 from 1.2 per cent. Meantime, mobile phone subscribers rose from 119,075 in 2000 to 404,202 by March, 2002.

* In Kenya, it is the tourism and non-traditional sectors, such as horticulture, that are driving e-commerce. A 1999 study by Kenya Association of Tour Operators showed that 10 per cent of membership had an Internet presence and conducted business on-line.

Category 29.3 *Digital divide*

2002-09-24 **broadband cable access digital divide ISP Internet service provider survey**

NewsScan

BROADBAND'S AVAILABLE, BUT HAS FEW TAKERS
Almost every U.S. household has potential access to a high-speed Internet connection, but only 10% subscribe to such a service, lower than the rate in Taiwan, South Korea, Hong Kong or Canada. About half of U.S. families have some type of Internet access at home. A report from the U.S. Commerce Department's Office of Technology Policy cites a need for more compelling content in order to boost the adoption of broadband: "New applications and services that consumers want and businesses need will provide the tipping point for broadband demand and usage." The report credits Napster, along with PCs, CD-ROM writers and larger hard drives, for promoting the use of broadband access. Along with lack of content, the report says the relatively high cost of high-speed access is another obstacle to wider usage. Broadband access costs about $50 a month vs. $20 a month for dialup connections. An August 2002 Yankee Group survey indicated that more than 70% of dialup users cited cost as the main barrier toward upgrading to faster access. (AP 23 Sep 2002)
http://apnews.excite.com/article/20020923/D7M7GVS00.htm

Category 29.3 *Digital divide*

2003-01-07 **online polls digital divide bias non-random sampling**

NewsScan

ONLINE POLLS REFLECT CONSERVATIVE OUTLOOK
While both Democrats and Republicans were likely to turn to the Internet as a source of news and political information during last fall's midterm elections, Republicans were much more likely to register their views in online polls, according to a study by the Pew Internet and American Life project. Nearly half of the Republicans who went online in search of election news said they liked to participate in online polls, compared with 23% of Democrats. The bottom line is that Web sites operating online polls should take those results with a grain of salt, says Lee Rainie, director of the Pew project. "They very much skew toward more conservative views. People who rely on Internet polls are relying on a false indicator." (Wired.com 6 Jan 2003)
http://www.wired.com/news/politics/0,1283,57093,00.html

Category 29.3 *Digital divide*

2003-03-19 **digital divide accessibility Internet**

NewsScan

MORE UNDERSERVED CHILDREN ARE GETTING ONLINE
Almost two-thirds of American children between the ages of 2 and 17 logged onto the Net last year, with a whopping 205% increase among African-American children, according to a new report from the Corporation for Public Broadcasting. The disparities between higher and lower income children still exist, but the study found that 58% of African American children and 50% of Hispanic children now use the Internet from some location — either home, school or the local library. The study, based on a series of surveys conducted last year by technology market research firm Grunwald Associates, also found that digital media use among children ages 6-17 is now approaching parity with television viewing. According to the report, children spend 3.1 hours per day watching TV and 2.9 hours a day surfing the Web, playing video games or using the computer for non-Internet activities. Among teenagers, computer use actually outstrips TV viewing — 3.5 hours vs. 3.1 hours per day. An electronic version of the report "Connected to the Future" is available at cpb.org/ed/resources/connected. (Corporation for Public Broadcasting 19 Mar 2003)

Category 29.3 *Digital divide*

2003-04-17 **Internet usage evasion elderly digital divide**

NewsScan

PEW STUDY OF INTERNET EVADERS
A study by the Pew Internet and American Life Project has found that 42 % of American adults are not connected to the Internet, even though two out of three of those people have relatives or close friends who do. In addition, the study's authors label as "Net Evaders" 20% of the nonusers who live in Internet-connected homes where other relatives go online. And then there's a category of "Net Dropouts" to characterize the 17% of nonusers who tried the Net and didn't like it. The director of the Pew project says of the Net Dropouts: "Some grew disillusioned with the online world. They decided it was just a time swamp, or they never found what they wanted." [They have our full sympathies. If the poor wretches never found NewsScan, who can blame them for jumping ship?] (New York Times 17 Apr 2003)

Category 29.3 *Digital divide*

2003-06-26 **Wi-Fi poorer nations wireless internet**

NewsScan

WIRELESS GIVES POORER NATIONS CHANCE TO CATCH UP…
In a speech prepared for a UN conference on the social implications of wireless communications technologies, UN Secretary-General Kofi Annan declared that wireless Internet access has "a key role to play everywhere, but especially in developing countries and countries with economies in transition… It is precisely in places where no infrastructure exists that Wi-Fi can be particularly effective, helping countries to leapfrog generations of telecommunications technology and infrastructure and empower their people." (Reuters 26 Jun 2003)

Category 29.3 *Digital divide*

2003-07-15 **MIT search engine poor countries e-mail connectivity**

NewsScan

A SEARCH ENGINE FOR THE WORLD'S POOR
Researchers at MIT are designing a search engine geared to the needs of computer users in the world's disadvantaged countries, most of whom have only sporadic access to the Web at what are often less-than-optimal bandwidths. "Let us assume you are in Malawi," says professor Saman Amarasinghe of MIT's Laboratory for Computer Science, "and the computer lab does not have access to the telephone line all the time. If you want to find some new information about malaria, you are prompted with a message that says 'we are going to send a query through e-mail, is it OK?'. At night, when the phone line is available, the teacher can dial out and send the queries." The request is routed to computers at MIT, which then perform the search and filter the results, choosing the most relevant. These results are then sent back to the computer in Malawi. "Next morning the teacher can connect, download that e-mail and when the students arrive, they can browse through those pages the way they would if they had full Internet connectivity." Amarasinghe says most search engines are geared toward Western users who are cash-rich but time-poor. "The idea is that developing countries are willing to pay in time for knowledge. In the West when we surf we want the information in the next two seconds. We are not willing to wait." (BBC News 15 Jul 2003)

Category 29.3 *Digital divide*

2003-12-19 **internet illiteracy language non-english population technology**

NewsScan

GLOBAL INTERNET USE LIMITED BY LANGUAGE, ILLITERACY
According to the International Telecommunication Union, about 70% of the world's Internet users live in countries that make up only 16% of the world's population — statistics that reinforce complaints aired at last week's U.N World Summit on the Information Society that despite the Internet's global reach, most of the material is inaccessible to the vast non-English-speaking population of the world. And while international development efforts have included linking villages and schools in developing nations to the Internet, once people are connected, there must be compelling information available in native languages and in accordance with local customs. "Getting the technology into people's hands is one thing. Getting people to use it is key," says Daniel Wagner, director of the University of Pennsylvania's International Literacy Institute. The solution involves more than just translating Web sites into other languages. To address the problem of population illiteracy, South Africa is developing speech recognition, text-to-speech and other voice technologies, starting with Zulu. Bulgaria, South Korea and other countries are producing government sites in native languages. And the Canadian government is looking at adapting its internal search engine to include materials in Inuktitut, the Inuit language, as well as French and English. "The point is to produce more content that is useful," says Bernardo Sorj, an advisor to Brazilian urban assistance group Viva Rio. "If people go on the Internet and do not find good content for themselves, then they go to pornography." (AP 19 Dec 2003)

Category 29.3 *Digital divide*

2004-02-19 **Internet rural usage technology cyberspace**

DHS IAIP Daily;
http://www.cnn.com/2004/TECH/02/18/hln.wired.rural.internet/ index.html

February 19, CNN — Rural Internet use on the rise.

More rural Americans are surfing through cyberspace than ever before. Fifty-two percent of rural adults were connected in 2003, up from 41 percent in 2000. Despite the growth, rural users still lag more than 10 percentage points behind their urban and suburban counterparts, according to the latest report from the Pew Internet and American Life Project, "Rural Areas and the Internet." Why the gap? First, it's typically easier to get online in urban and suburban communities, and users have more choices when it comes to accessing the Internet. Other factors include lower income levels and the fact that rural users are often older than urban and suburban users. The majority of the analysis from the "Rural Areas and the Internet" report came from random phone surveys conducted between March and August 2003. The report is availalble online:
http://www.pewinternet.org/

Category 29.3 *Digital divide*

2004-04-28 **IT industry workers age old people skill set changing**

NewsScan

RULES TO CHANGE IN 'YOUNG MAN'S' IT GAME

A new report by Australia's Swinburne University researchers has highlighted the under-representation of older people working in the IT industry, with figures showing that workers aged 45 years and over made up only 23% of the IT workforce in 2001. The study shows that only 5% of IT workers were aged between 55 and 64 (compared with 21% in the business and property services industry), and that younger males were the most likely group to work full-time in permanent employment, while women aged over 45 years were the least likely. Libby Brooke of Swinburne thinks that the dramatic drop-off in the number of people in the IT industry after the age of 45 could be attributable to a range of issues (including the recent soft jobs market and the "constantly changing skills base" within the IT industry) and says that the main question is: "How can older workers continue to be skilled and supported in the workplace?" (The Age, 28 Apr 2004)

Category 29.3 *Digital divide*

2004-07-25 **computer usage minimum age study debate technology proliferation**

NewsScan

COMPUTER KIDS: HOW YOUNG IS TOO YOUNG?

There's a growing debate about whether children should be exposed to technology when they are still infants. Author Jane M. Healy opposes the practice and says, "Mental ability is gained from manipulating the three-dimensional world at that age and managing your own mind and not
having it managed by an electronic machine"; she recommends that kids stay off computers until age 7. David Elkind, professor of child development at Tufts University, has similar concerns: "Children miss out on all these basic learning experiences if they are so attuned to the virtual world." But other scholars hold the opposite view: Yong Zhao, a professor of educational psychology at Michigan State University, bought his daughter an iMac before she turned 1 and allowed her to simply bang on the keyboard to learn how the banging led to changes on the screen. And still other technology experts say the right answer lies somewhere in the middle of those two positions. Peter
Grunwald, whose consulting firm specializes in kids and technology, says: "Kids need a good balance in their lives and a mix of experiences"; his position is that computers can help kids develop hand-eye coordination and other skills, but shouldn't be used as robotic baby-sitters that shield a
child from the real world. (AP 25 Jul 2004)

Category 29.3 *Digital divide*

2004-10-28 **survey politics Internet digital divide sociology diversity**

NewsScan; http://www.pewinternet.org/

INTERNET BROADENS VOTERS' POLITICAL HORIZONS

More than 40% of U.S. Internet users have gotten news and information about this year's presidential campaign online, and 31% of broadband users now cite the Net as their primary source of campaign news -- about the same number as those who rely on newspapers (35%). And while some pundits had expressed concern that wider use of the Internet would result in a decreased exposure to viewpoints that conflict with users', it turns out that Internet users have a greater overall exposure to political arguments, including those that challenge their preferences. "People are using the Internet to broaden their political horizons, not narrow them," says Kelly Garret, coauthor of a new report from the Pew Internet & American Life Project. "Use of the Internet doesn't necessarily diminish partisanship, or even zealotry. But it does expose online Americans to more points of view, and, on balance, that is a good thing." One surprise coming out of the survey -- about 20% of Americans say they actually prefer news sources that challenge their point of view, and nearly 10% are *more* aware of arguments that oppose their candidate than arguments in favor. (Pew Internet & American Life Project 28 Oct 2004)

Category 29.3 *Digital divide*

2005-02-24 **World Bank digital divide organization United Nations World Summit Information Security democracies poverty mobile phones**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=7731166

WORLD BANK SAYS DIGITAL DIVIDE CLOSING FAST

The World Bank has released a report contending that the digital divide is closing fast, putting the organization at odds with the United Nations (U.N.), which asserts that the divide is a problem that still needs to be addressed. The U.N. is hosting the World Summit on the Information Society in Geneva, where attendees are expected to call for increased funding to provide access for poorer countries to digital technologies. The U.N. believes that increasing such access will help poorer countries build stable democracies and deal with problems such as poverty. The World Bank cited statistics, however, that seem to contradict the need for ongoing funding to shrink the divide. The group's report said, for example, that in 2002, Africa had 59 million fixed-line or mobile phones, far more than some other estimates. The report also said half the world's population now have access to a fixed-line phone and 77 percent have access to a mobile phone.

Category 29.3 *Digital divide*

2005-06-15 **Internet access rural India villages World Bank thin client technology bridge digital divide**

EDUPAGE; http://www.nytimes.com/2005/06/16/technology/16compute.html

BRINGING THE INTERNET TO RURAL INDIA

As many as 5,000 villages in rural India may soon be connected to the Internet, thanks to efforts of an international group of companies and organizations, including the World Bank. Many rural Indians do not have easy access to business or government functions, and the project is designed to fill that gap for villages with more than 5,000 residents in the Indian state of Karnataka. The computer centers or kiosks will connect to the Internet either through wired networks or by satellite and will have between 5 and 10 "thin client" computers. In addition to the World Bank, partners in the project include Comat Technologies, an Indian Internet service provider; ICICI Bank, a commercial bank in India; and California-based Wyse Technology, maker of computer terminal equipment. New York Times, 15 June 2005 (registration req'd)

Category 29.3 *Digital divide*

2006-04-26 **digital divide shrink IBM _The Economist_ study worldwide**

EDUPAGE; http://news.com.com/2100-1034_3-6065240.html 23

DIGITAL DIVIDE SHRINKING

According to a study conducted by IBM and "The Economist" magazine, although the digital divide remains considerable for some countries, the gaps are shrinking. The study assessed both availability and use of technology in 68 countries and assigned each an "e-readiness" score on a scale of 1 to 10. The gap from the top of the list (Denmark, 9.00) to the bottom (Azerbaijan, 2.92) is indeed significant, but in certain regions of China and India, connectivity rivals that of developed nations, according to Peter Korsten, European director at IBM's Institute for Business Value. The study noted that nearly every country's score improved from last year but that countries nearer the bottom of the list saw greater gains than those in the upper tiers, indicating a shrinking digital divide overall. Beyond the issue of connectivity lies the question of what efforts each country makes to use technology. As Korsten said, "It's up to governments to take advantage with education and other initiatives."

29.4 Online & electronic voting

Category 29.4 Online & electronic voting

2000-01-18 **internet online voting study report state government task force**

California State Government http://www.ss.ca.gov/executive/ivote/

The California Internet Voting Task Force issued its "Report on the Feasibility of Internet Voting." A key section from the Executive Summary: "
The implementation of Internet voting would allow increased access to the voting process for millions of potential voters who do not regularly participate in our elections. However, technological threats to the security, integrity and secrecy of Internet ballots are significant. The possibility of "Virus" and "Trojan Horse" software attacks on home and office computers used for voting is very real and, although they are preventable, could result in a number of problems ranging from a denial of service to the submission of electronically altered ballots.

Despite these challenges, it is technologically possible to utilize the Internet to develop an additional method of voting that would be at least as secure from vote-tampering as the current absentee ballot process in California. At this time, it would not be legally, practically or fiscally feasible to develop a comprehensive remote Internet voting system that would completely replace the current paper process used for voter registration, voting, and the collection of initiative, referendum and recall petition signatures."

Category 29.4 Online & electronic voting

2000-09-21 **online voting fraud contest TV show**

RISKS, Australian Broadcast Corp. 21 06
http://www.abc.net.au/mediawatch/transcripts/s181183.htm

The Australian Broadcasting Corporation found strong indications of voting fraud when it allowed online voting for the popularity of amateur videos on a TV show. The leading contender received five times more votes than any other contestant despite the fact that her videos were despised by the professional judges.

Category 29.4 Online & electronic voting

2000-10-20 **electronic voting workshop**

RISKS 21 10

The Internet Policy Institute (IPI) held a workshop on October 11 & 12, 2000 to examine the issues associated with conducting public elections via computer networks. Sponsored by the National Science Foundation (NSF) and chaired by C.D. Mote, Jr., president of the University of Maryland, this workshop was in response to a request by the White House to study the feasibility of Internet voting. Avi Rubin participated in the workshop and wrote in RISKS:

"Panels were held discussing issues such what e-voting means, whether or not e-voting would improve accessibility, whether it would widen the digital divide, and whether more people would vote. On the technical side, there were panels about the security requirements, the current state of security on desktops as related to voting.

The mandate was to cover the following issues:

* How to ensure the security and reliability of the voting process;
* How to protect the privacy of voters;
* How to authenticate voter identity;
* How to achieve broad and equitable access to online voting systems;
* How to assess the impact of online voting on representative democracy and community; and
* How to ensure that online voting systems are convenient, flexible, and cost-effective."

Category 29.4 Online & electronic voting

2000-10-26 **online voting security prediction**

NewsScan, Associated Press, San Jose Mercury News
http://www.mercurycenter.com/svtech/news/breaking/ap/docs/564217l.htm

Concerned about issues of security, confidentiality and ease of use, election officials are being extremely cautious about letting citizens use the Internet to cast their votes: in the coming elections fewer than 200 people will be eligible to vote from their PCs. Maine secretary of state Dan Gwadosky sums up the current situation this way: "Online voting is inevitable. It just won't happen on Internet time." (AP/San Jose Mercury news 26 Oct 2000)

Category 29.4 Online & electronic voting

2000-11-07 **voting computers proprietary software Trojans QA quality assurance open source fraud**

RISKS 21 10

Douglas W. Jones, the chair of the Iowa State Board of Examiners for Voting Machines and Electronic Voting Systems, wrote an essay for RISKS in which he expressed concern over the growing use of proprietary software for voting machines and other forms of electronically-mediated voting. He pointed out that such software makes it much easier to insert Trojan code than, say, open-source software.

He ended his essay as follows: "The time has come for computer professionals to press for a change to the guidelines for voting machines, asking that all software included in such machines be either open source, available for public inspection, or at least open to inspection by a third party independent testing authority. There are no technical obstacles to this! Linux, Free BSD and several other fully functional operating systems are available and will run on the hardware currently being incorporated into modern voting machines!

But, this is not the end of the problem! How do you prove, after the fact, that the software in the voting machine is the software that was approved by the board of examiners and tested by the independent testing authority? No modern machine I'm aware of makes any real effort to allow this proof, although several vendors do promise to put a copy of their source code in the hands of an escrow agency in case a question arises".

Category 29.4 Online & electronic voting

2000-11-08 **online voting problems satire funny**

RISKS 21 11

Lauren Weinstein's "Reality Reset" <http://www.vortex.com/reality > included a hilarious satirical "interview" with "Paddy Mastoid. . . . president of trust-us-not-to-badly-screw-up-your-vote.com, a firm promoting Internet voting systems." In this spoof, Weinstein, Co-Founder of PFIR (People For Internet Responsibility, < http://www.pfir.org >) and Moderator of the Privacy Forum < http://www.vortex.com >, ably reviews many of the vulnerabilities to hacking that online voting systems present.

Category 29.4 Online & electronic voting

2000-11-14 **online voting predictions**

NewsScan, USA Today http://www.usatoday.com/life/cyber/tech/cti797.htm

Some technology chief executives are predicting that Web-based voting will be in place by the time of our next presidential election, and one of them argues: "You can trade stock online. There's plenty of technology to implement Internet voting." But Jim Cannavino of the security firm CyberSafe says "I haven't seen us move fast on any of these things," and doesn't think the Internet voting will happen until 2050, because it will take that long for government leaders to understand the system well enough to believe in its validity." (USA Today 13 Nov 2000)

Category 29.4 Online & electronic voting

2000-12-12 **electronic voting security testing challenges contests**

RISKS 21 14

In a manifesto published in the IP distribution list and on the RISKS Forum, eminent computer scientists Peter Neumann (SRI), Rebecca Mercuri (Bryn Mawr), and Lauren Weinstein (PFIR, Privacy Forum) attacked the practice of putting proprietary electronic voting systems out for random attacks as a method of evaluating their level of security. "In fact, using such "tests" as any sort of validation technique runs contrary to long-established computer and engineering verification practices, and makes a mockery of the rigorous design and testing that is required of systems that are to be deemed secure through extensive and methodical processes (e.g., to gain certification under the ISO Common Criteria or its predecessors TCSEC/ITSEC)."

Category 29.4 Online & electronic voting

2000-12-13 **online voting**

RISKS 21 15

Fred Cohen analyzed the security issues in online voting in a paper published in the RISKS Forum. Having listed ten necessary properties for a trustable election process, he noted, "At this point in time, and for the foreseeable future, computerized and particularly Internet-based voting machines and networked voting systems do not, and will not, fulfill the majority of these requirements." He went on to list ten specific objections to online voting systems in today's technical environment.

Category 29.4 Online & electronic voting

2000-12-15 **online voting research study project**

NewsScan, San Jose Mercury News
http://www.mercurycenter.com/svtech/news/breaking/merc/docs/010800.htm

[In December, a] team of political scientists, engineers, and design experts from the Massachusetts Institute of Technology and the California Institute of Technology . . .[announced that they would] undertake a study of existing voting technology and create a plan to improve it. Caltech president David Baltimore said it is "embarrassing to America when technology fails and it puts democracy to such a test as we have seen in the last month," and his counterpart MIT president Charles Vest promised that, "to a large extent, the problem that the country has ... a technological solution." (AP/San Jose Mercury News 15 Dec 2000)

Category 29.4 Online & electronic voting

2000-12-19 **online voting automated teller machines ATM ABM**

RISKS 21 15

David Jefferson wrote a thoughtful analysis of proposals for using automated teller machines (ATMs) for voting. Although such machines are often equipped with security measures, Jefferson showed major disadvantages that preclude using them for elections. In summary, his objections to using the ATM networks for voting were as follows:
* Private voting, like absentee balloting, is subject to voter intimidation, coercion and vote-selling;
* Voter authentication is problematical, since vote-sharing (voting by proxy) is illegal;
* Reliability of electronic voting using banking networks would be problematic;
* Independent oversight by election officials would be complicated if the privately-owned ATM networks were used for voting;
* The security of the banking networks would be equally compromised if election officials had access to financial systems;
* It is unthinkable that banks would turn over complete control of their systems to public officials even for a single day, let alone for the time required "to build, debug and certify such a system. . . ."
Therefore, concludes Jefferson, "the suggestion to use the ATM network for voting is a complete nonstarter."

Category 29.4 Online & electronic voting

2001-01-11 **online voting technology**

NewsScan

TECH ALLIANCE TO DEVELOP NEW VOTING SYSTEM
Unisys, Microsoft, and Dell will jointly work on a project to create a new voting system that will integrate all election processes, from voter registration to ballot counting, and avoid the confusion and uncertainty experienced in the recent U.S. presidential elections. (Reuters/San Jose Mercury News 11 Jan 2001)
http://www.mercurycenter.com/svtech/news/breaking/reuters/docs/833061l.htm

---

Category 29.4 Online & electronic voting

2001-03-16 **online elections voting problems report analysis**

RISKS 21 28

Terry Carroll summarized in RISKS a recent report on online voting. "The National Science Foundation recently released a study that it commissioned from the Internet Policy Institute on problems associated with Internet voting. The NSF's press release on the study may be found at < http://www.nsf.gov/od/lpa/news/press/01/pr0118.htm>. The IPI has a page devoted to the study (including a link to the report itself) at <http://www.internetpolicy.org/research/results.html>."

According to Carroll, "The NSF highlights the following findings with respect to the feasibility of Internet voting:
- Poll site Internet voting systems offer some benefits and could be responsibly deployed within the next several election cycles;
- The next step beyond poll-site voting would be to deploy kiosk voting terminals in non-traditional public voting sites;
- Remote Internet voting systems pose significant risk and should not be used in public elections until substantial technical and social science issues are addressed; and
- Internet-based voter registration poses significant risk to the integrity of the voting process, and should not be implemented for the foreseeable future.

Another item in the same issue of the RISKS Digest noted an amusing glitch in an online election. Sarr Blumson reported, "The college I attended is running the election for alumni appointed trustee with a Web voting option through election.com. So I went to cast my vote, and got in response:

Microsoft OLE DB Provider for SQL Server error '80040e14'

The log file for database 'electnet' is full. Back up the transaction log for the database to free up some log space.
/dartmouth2001/confirmation.asp, line 92

It's happened twice. It let me vote successfully a few hours later; I'm assuming/hoping it only recorded my vote once. . . ."

Category 29.4 Online & electronic voting

2001-03-29 **online Internet voting standards**

RISKS 21 33

David Marston reported on a move by The Organization for the Advancement of Structured Information Standards (OASIS, http://www.oasis-open.org) to address online voting by developing standards. He provided the following excerpt from published documents on that site:

"A new OASIS technical committee is being formed. The Election and Voter Services Committee has been proposed by Gregg McGilvray, election.com (chair); Oliver Bell, Microsoft; and Ed McLaughlin, Accenture.

Purpose: To develop a standard for the structured interchange of data among hardware, software, and service providers who engage in any aspect of providing election or voter services to public or private organizations. The services performed for such elections include but are not limited to voter role/membership maintenance (new voter registration, membership and dues collection, change of address tracking, etc.), citizen/membership credentialing, redistricting, requests for absentee/expatriate ballots, election calendaring, logistics management (polling place management), election notification, ballot delivery and tabulation, election results reporting and demographics.

Implementation: The standard under development by election.com, Inc. will be made available for review and revision and can be expanded upon as necessary. A phased approach will be used to implement the standard due to the number of aspects being considered by the standard."

Category 29.4 *Online & electronic voting*

2001-11-10 **online voting election paper ballots QA quality assurance failure programmer dishonesty**

RISKS 21 74

In San Bernardino County, an election was screwed up by an untested and faulty computer program. The responsible programmer falsely claimed to have run quality assurance tests; his buggy program ignored some votes, reversed the meaning of votes on other cards, and even counted zero votes in one precinct. Geoff Kuenning, reporting for RISKS, quoted a significant passage from the Los Angeles Times: "County officials said the good news is that using a card-counting system means that ballots are still around to be recounted. If the same error had occurred with an electronic voting system, there would be no paper record . . . ."

Commentators responded to RISKS with the obvious remark that a programmer should never be the only person to test his or her own code. Others suggested that the programmers managers should have been fired for allowing such sloppy procedures.

Category 29.4 *Online & electronic voting*

2001-12-03 **online voting risks internation laws agreements regulations principles legal analaysis**

RISKS 21 81

Lucas B. Kruijswijk published an analysis of several national constitutions and International law with respect to online voting. He wrote in his introduction, "After some research I made the conclusion that some kinds of voting are indeed violating International Law. This means that there is a risk that a judge may forbid some kind of voting methods, making the investment worthless."

Category 29.4 *Online & electronic voting*

2002-01-09 **cybercourt Internet connection legal system vulnerabilities interception man-in-the-middle attack confidentiality reliability availability integrity data diddling**

NewsScan

MICHIGAN GOVERNOR ESTABLISHES CYBERCOURT
Michigan Governor John Engler has signed into law a bill to create a virtual state court -- the first to operate in the U.S., according to Matt Resch, an Engler spokesman. A cybercourt exists at the College of William and Mary in Virginia, but isn't operational, says Resch. The court won't have a jury and will handle only business disputes involving at least $25,000. District or circuit court judges will be assigned for three-year terms and will be specially trained to use the system. "In a world where we can go from idea to IPO at warp speed, we need a connected court that can keep up," says Engler. (AP 9 Jan 2002) http://apnews.excite.com/article/20020109/D7GU9I300.html

---

Category 29.4 *Online & electronic voting*

2002-01-19 **Web voting fraud ballot stuffing automation reliability**

RISKS 21 87

News reports about an unscientific poll about preferences between Java and Microsoft's .NET indicated that some Microsoft employees were "trying to vote repeatedly, including automated voting."

MORAL: don't trust the results of Web-based polls that use self-selected respondents and weak anti-fraud controls.

Category 29.4 Online & electronic voting

2002-01-26 **online court proceedings judgements Web**

RISKS 21 89

Tony Ford summarized a new official self-service litigation system available in England & Wales in a brief article in RISKS (quoted verbatim below):

Today's Daily Telegraph (a quality UK broadsheet newspaper) carries a *potentially* disturbing report describing a new service, "Money Claim Online", whereby individuals and law firms (solicitors) can issue most simple legal proceedings (where a sum less than UK pounds 100,000 is claimed, = USD 140K)) and enforce judgments via a Web browser. The new service has been set up without publicity by the Lord Chancellor's Department, which runs the courts system in England and Wales. It seems that the system is accessible to the public now, although it has not been officially launched.

People using the service are (oddly) referred to as "customers" .... and there is a Customer Help Desk ...

The newspaper report is also viewable at this Daily Telegraph link on-line:
http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2002/01/26/nsue26.xml&sSheet=/news/2002/01/26/ixhome.html

The service can be seen on-line at: https://www.moneyclaim.gov.uk/csmco/index.html

No details are apparent of what measures are taken to validate the identity of the claiming party or prevent other gross miscarriages of justice .... but it would appear that the potential exists for significant trouble .... even though the site warns that "vexatious litigants" are not allowed to us it (these are people who have abused the litigation system in the past to such an extent that they have been declared "vexatious litigants", restricting their ability freely to issue legal proceedings).

PS: I am a lawyer myself, although I don't practise in this area .. but do work in-house for a large IT company ... these comments are offered purely in a personal capacity.

Category 29.4 Online & electronic voting

2002-01-30 **online voting touchscreen COTS insider fraud penetration intrusion audit trail tampering data diddling QA quality assurance**

RISKS 21 90

David E. Price reported that "officials in Florida's Miami-Dade County have approved a $24.5 million contract to replace the county's punch-card voting system with touchscreen equipment, in time for Nov 2002. The touchscreen machines make it impossible to vote for more than one candidate in each race, known as overvoting, and alert voters if they fail to select any candidate, or undervote. Two other counties that were at the heart of the controversy -- Palm Beach and Broward -- also plan to use touchscreens."

Peter G. Neumann added, "And as we have noted here before, today's touchscreen systems provide essentially ZERO hard evidence that your vote is counted as cast, and not for someone else or for no one. With just a little insider fraud, what a remarkable opportunity for rigging elections!"

A couple of weeks later, Alan Brain added the following concise commentary:

"The risks for vote-rigging on COTS systems [include]:

a) Someone tweaks the BIOS of the voting machines. b) Someone tweaks the OS of the voting machines. c) Someone tweaks the applications code d) Someone tweaks the compiler.

a) Can best be dealt with via physical security only - have non-flashable BIOSes, and disallow unauthorised access.

The rest require both a publicly available Open Source codebase, and physical security to make sure that what you think is on the machine, actually is. And that the right OS has been installed, and the right compiler used."

He added, "Conversely, if the voting is being done with machines where the OS, Applications Sourcecode and Compiler aren't Open Source, then security is problematic."

Category 29.4 Online & electronic voting

2002-02-20 **onnline voting fraud countermeasures COTS commercial off-the-shelf software**

RISKS 21 92 FF

The RISKS Forum was the locus of a vigorous discussion of online voting hazards. The following collates contributions from various contributors:

[Alan Brain] The risks for vote-rigging on COTS systems [include]:

a) Someone tweaks the BIOS of the voting machines.
b) Someone tweaks the OS of the voting machines.
c) Someone tweaks the applications code
d) Someone tweaks the compiler.
e) Someone tweaks the compiler of the compiler of the …. [Mike Nelson]

a) Can best be dealt with via physical security only - have non-flashable BIOSes, and disallow unauthorised access.

The rest require both a publicly available Open Source codebase, and physical security to make sure that what you think is on the machine, actually is. And that the right OS has been installed, and the right compiler used.

[Lee Barstow] With physical access to voting machines and/or the software used to control them, the only sure way to provide security is a paper record.

Especially with OpenSource software, it becomes possible to recompile (and hence alter) any electronic-only record. Closed Source software isn't any better - it lacks public accountability and scrutiny. Someone could always create a new ROM, OS, or software image if given sufficient knowledge, bypassing any security system that has been put in place.

So: Print an OCR paper record when the voter finishes his vote. He gets to check the paper copy and put it in a standard secured voting box. The best parts are:

(a) Since it's printed on demand, only the voter's candidate appears on the printout - the voter sees only who or what he voted for, or that he made no vote, and can easily check the paper before dropping it in the box.

(b) Using OCR, independent auditing becomes easy. The auditor needs little in the way of custom hardware or software to do the job; they only need to tweak their OCR readers. Auditors could be chosen by mutual agreement of the candidates after the vote is completed (and only if a candidate determines he wants to have a recount), removing any temptation to bribe the auditing firm.

Category 29.4 Online & electronic voting

2002-04-22 **online Web voting UK browsers identification authentication I&A interception**

RISKS 22 04

In the English boroughs of Crewe & Nantwich in Cheshire, a couple of wards experimented with Web-based voting. The security measures consisted of sending two separate "secret codes" by two postal mailings to registered voters, who would then have to use either MS-IE or Netscape Navigator -- but only in the Windows versions. No other operating system versions need apply.

[MK comment: Hmm, talk about the digital divide…]

Category 29.4 Online & electronic voting

2002-04-29 **online voting fraud criminal hackers penetration tampering corruption interference**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A64981-2002Apr29.html

VIVENDI SUSPECTS ELECTRONIC VOTE FRAUD
Vivendi Universal, the Paris-based media giant, is calling for a criminal investigation of suspected fraud by unnamed computer hackers during a shareholders vote by Internet last week. Vivendi thinks the vote tampering "could have been carried out by a small team armed with a transmitter-receiver and detailed knowledge of the procedures and technical protocols of electronic voting." (AP/Washington Post 29 Apr 2002)

Category 29.4 *Online & electronic voting*

2002-05-16 **online voting corporations companies industry postage Web**

NewsScan

TREND TOWARD ELECTRONIC VOTING
More and more companies are allowing shareholders the option of Internet voting, motivated as much by reductions in postage costs as anything else. Mary Ann Butera of ADP Investor Communication Services says an Internet vote costs a company only about 3 cents, compared to a paper proxy which costs a company 34 cents. "It doesn't sound like much, because you're talking about pennies. When you multiply that over thousands of investors, it does add up." And of course there's the matter of pride of being on top of technology developments. Tom Newston of EquiServe notes: "A small company that only has hundreds of shareholders, or a few thousand shareholders, may not see the cost savings as a big number. But at the same time, they may want to be thought of as a forward-thinking, cutting-edge company." In the U.S., 85% use "traditional" voting methods: 70% of proxy voters mail their votes and 15% use the phone. (Tampa Tribune/San Jose Mercury News 15 May 2002)
http://www.siliconvalley.com/mld/siliconvalley/3271361.htm

Category 29.4 *Online & electronic voting*

2003-01-22 **online Internet election voting**

NewsScan

INTERNET ELECTION
The tiny village of Anieres, Switzerland, made Swiss history by holding that country's first legally binding [online] election. The 323 citizens who cast their votes by Internet were required to type in a series of security codes and their date and place of birth. An additional 370 Anieres residents voted by mail, and 48 actually went to the polls. (AP/Chicago Sun-Times 20 Jan 2003)
http://www.suntimes.com/output/news/cst-nws-net20.html

Category 29.4 Online & electronic voting

2003-01-28 **electronic voting analysis flaws problems resources**

http://www.nwfusion.com/newsletters/sec/2003/0127sec1.html

E-Voting (1): Not Ready Yet

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Electronic voting has been proposed in a number of precincts in the USA. One of the most extensive archives of discussions about this issue is the RISKS FORUM DIGEST edited by Peter G. Neumann of SRI Intl. Entering "vote" as a keyword in the search engine available through at < http://catless.ncl.ac.uk/Risks/ > brings up 303 entries starting with Volume 1 Number 1 [henceforth notated as "v(n)" for the volume and number] in 1985; additional articles can be found using other related keywords such as "voting" and "election."

One of the most recent contributions comes from Jonathan Kamens, writing in RISKS 22(39) (23 Nov 2002). He describes a system that allows a voter to mark a paper ballot and then feed it in through an electronic reader. Kamens points out that the card-reading voting system proposed for Boston MA has fundamental problems:

* There is no way for a voter to verify that the system is correctly registering the voter's choices on the ballot.

* If the card reader indicates that a card has not successfully been registered, a voter can be given a second card -- but the invalid one goes straight into a locked ballot box. If there's a recount, someone could get both their ballots counted.

In general, e-voting systems can include any or all of the following functions, each requiring increasing degrees of security:

* Automatic reading and tallying of votes made on paper ballots;

* Accepting votes using electronic input devices such as electric pens, touch-screens, and keyboards;

* Remote voting at a distance.

E-voting systems need to include at least the following security characteristics:

1) Remote voting requires identification, authentication and authorization PLUS guarantees of complete privacy as well as measures to prevent fraudulent exclusion of valid voters and fraudulent acceptance of repeated votes by individuals.

2) Electronic data entry should include all the measures developed in the last 40 years of data processing to reduce the likelihood of user error; such measures include

a) feedback to the user to be sure that what was entered was what was recorded;

b) error checking and alerts to prevent obvious blunders such as voting for two people for the same position if that is not permitted;

c) provision of overrides so that voters can deliberately spoil their ballot if that's what they want to do;

3) Fail-safe redundancy so that no single point of failure or even widespread denial-of-service attacks could wipe out voter's intentions;

4) Cryptographically strong local and remote audit trails to keep multiple independent records of all votes; such files could include checksums that are calculated using the preceding record's checksum as input to the hashing algorithm (to reduce the ease of fraudulent tampering with the records).

One of the most serious questions raised about e-voting is independent of security: it's the issue of equal access. Will widespread e-voting lead to increased disparity between the voting patterns of richer and poorer people among the electorate? Will e-voting be yet another example of what has been called the "digital divide?"

* * *

In the next article in this two-part sequence, I will look at some detailed analyses of e-voting with special attention to security.

* * *

For further reading:

Bonsor, K. (2002). How E-Voting Will Work. < http://www.howstuffworks.com/e-voting.htm/printable >

Burke, L. (2000). Report says E-Voting Is Unsafe. < http://www.wired.com/news/politics/0,1283,37504,00.html >

Cranor, E. (1996). Electronic Voting: Computerized polls may save money, protect privacy. _ACM Crossroads Student Magazine_ < http://www.acm.org/crossroads/xrds2-4/voting.html >

Digital Divide Network < http://www.digitaldividenetwork.org/content/sections/index.cfm >

Election.com – The Global Election Company < http://www.election.com/us/index.htm >

Electronic Frontier Foundation "E-voting" Archive < http://www.eff.org/Activism/E-voting/ >

Category 29.4 Online & electronic voting

2003-01-30 **electronic voting analysis flaws problems resources**

http://www.nwfusion.com/newsletters/sec/2003/0127sec2.html

E-Voting (2): Security Analyses

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In the first of these two short articles, I've been introducing e-voting. In this part, I summarize some key analyses of the security issues surrounding remote voting via the Internet.

In a July 2002 article posted on the BBC Web site, commentator Bill Thompson comments on a recent Green Paper proposal by Robin Cook, Leader of the House of Commons. Cook includes two methods for increasing the involvement of the public in government decision-making: "For the government, the two strands that make up e-democracy are ways to enhance participation (e-participation) and electronic voting (e-voting)." Thompson argues that the vulnerabilities of any e-voting system built in the next few years should preclude any use of such insecure technology. He writes that the consequences of fraud would be so serious that large amounts of investment would be profitable if they swayed the direction of an election. For example, "If we all use trusted processors then why not set up a production line to manufacture your own hacked chips? It would only cost a few tens of millions of euros. If all code has to be signed by some digital authority, why not spend a few million bribing the senior staff?"

A much longer and more detailed analysis of e-voting is from the respected scientist Avi Rubin of AT&T Labs. Rubin neatly summarizes the issues as follows [I have added the asterisks as bullets and slightly changed the punctuation]: "There are many aspects of elections besides security that bring this type of voting into question. The primary ones are

* coercibility – the danger that outside of a public polling place, a voter could be coerced into voting for a particular candidate.

* vote selling – the opportunity for voters to sell their vote.

* vote solicitation – the danger that outside of a public polling place, it is much more difficult to control vote solicitation by political parties at the time of voting.

* registration – the issue of whether or not to allow online registration, and if so, how to control the level of fraud."

Rubin then analyses the voting platform, the communications infrastructure, social engineering, and specialized devices (by which he means "tamper-resistant devices, such as smart cards." He discusses in some detail how programmatic attacks (viruses, worms, denial-of-service [DoS] attacks) could easily alter election results. Just imagine the consequences of, say, carefully-written Trojan horse programs, targeted DoS attacks on particular precincts on election day; Rubin writes, "In some close campaigns, even an untargeted attack that changes the vote by one percentage point could sway the election." According to the notes in the source HTML for the document, that sentence was written a few weeks before the contested US presidential election of 2002. I strongly recommend Dr Rubin's paper as foundation reading for anyone interested in e-voting.

Finally, I direct your attention to the immensely valuable annotated bibliography on electronic voting prepared by Rebecca Mercuri, PhD, Professor of Computer Science at Bryn Mawr College. Dr Mercuri has a distinguished record of contributions to the technical analysis of electronic voting; her Web site (see below) has many pages of news, essays, pointers to other e-voting sites, lists of her own and other scholarly works on the subject, and even pointers to e-voting humor.

* * *

I hope that these two short articles will increase readers' interest in the trustworthiness of e-voting and that some of you will be able to contribute to a more informed discussion of this critically important issue in the future of representative democracy. I'm sure that I will be hearing from e-voting technology vendors clamoring for attention; if possible, I'll write a follow-up column with some of their remarks.

* * *

For further reading:

Legon, J. (2002). Electronic elections: What about security? Voters put touch screens to the test. < http://www.cnn.com/2002/TECH/ptech/11/05/touch.screen/ >
[Note to avoid ambiguity: the string /11/ in this URL uses the numeral "one"]

Mercuri, R. (2002). Electronic Voting. < http://www.notablesoftware.com/evote.html >

Rubin, A. (2000). Security Considerations for Remote Electronic Voting over the Internet. < http://avirubin.com/e-voting.security.html >

Thompson, B. (2002). Why e-voting is a bad idea. < http://news.bbc.co.uk/1/hi/sci/tech/2135911.stm >
[Note to avoid ambiguity: the string /1/ in this URL uses the lowercase form of the letter "L"]

Category 29.4 *Online & electronic voting*

2003-02-03 **electronic e-voting security risk debate**

NIPC/DHS

January 30, SecurityFocus — E-voting security debate.

Some respected computer scientists and security experts in California's Silicon Valley say the risks posed by malicious hackers, equipment failure or subtle programming errors make fully-electronic voting systems a bad idea. "There's no voter-validated record, so Trojan horses or accidents can happen without any evidence that anything has gone wrong," correctly," says Peter Neumann, a scientist at SRI International, a non-profit research institute. Electronic voting systems usually featuring touch screens and simple ATM-like interfaces. By some estimates one out of five votes were cast electronically last November. The systems are not connected to the Internet; instead, voters' ballots are typically stored on an internal hard drive until the polls close. Then they're copied a portable disk or a non-volatile memory card and taken to a central counting facility. It's the paperless nature of the transaction that bothers critics. "The problem is that…it's really up to the company that wrote the software to say that there were no errors or deliberate tampering that interfered with the vote," says David Dill, a computer science professor at Stanford University. The computer scientists say they'd be happier, but not convinced, if companies making the electronic voting systems released their code for public review. On Friday they are going to attempt to persuade Santa Clara County to embrace a system in which electronic voting stations print a hard copy of the voter's ballot. The voter can then review the printout before manually depositing it in a ballot box.

Category 29.4 *Online & electronic voting*

2003-02-24 **online voting**

NewsScan

LORRIE CRANOR ON INTERNET VOTING
In an interview with John Gehl for the ACM online weekly publication Ubiquity, Dr. Lorrie Faith Cranor of ATT Labs-Research, an expert on technology policy issues, says: "I am afraid that Internet voting will be a reality, and I think it's a bad idea, which surprises people. Usually people think that because I have done Internet voting work, I must be excited that Internet voting is progressing. It's one of those things that the more you know about, the less you like it." What does she dislike about Internet voting? "For one thing, there are huge security risks, especially when people are talking about Internet voting from home or from work as opposed to, say, going to a polling place that happens to be connected to the Internet. That's no fun. If we have to go to the polling place it really doesn't matter if it's connected to the Internet or whatever because we still had to go to a polling place. So when people, especially in the press, talk about Internet voting they're talking about voting from anywhere; from home in your pajamas is the classic example. That means voting over the existing insecure Internet using the existing insecure computers in my house that might have viruses or mis-installed software on them. I think that it is really dangerous, especially in elections where there's something really important at stake." (Ubiquity Feb 2003)
http://www.acm.org/ubiquity/interviews/l_cranor_2.html

Category 29.4 *Online & electronic voting*

2003-07-12 **e-voting security experiment 2004**

NewsScan

INTERNET VOTING IN 2004
The Secure Electronic Registration and Voting Experiment, which involved only 84 voters in 2000, is set to balloon next year when as many as 100,000 citizens in the military and living abroad will have the option of casting their votes via the Internet. The Pentagon-run SERVE program will be limited to eligible voters from South Carolina and Hawaii, as well as residents from selected counties in Arkansas, Florida, Minnesota, North Carolina, Ohio, Pennsylvania, Utah and Washington. If the test proves successful, the $22-million program could be expanded to include 6 million voters in the military and their dependents, as well as nonmilitary citizens living abroad. Some observers have voiced security concerns over electronic voting, however. "It wouldn't take much for some smart hacker to send around a virus that lays in wait for someone to issue a vote," says a project manager for the Center for Public Integrity. Meanwhile, Polli Brunelli, director of the Pentagon's Federal Voting Assistance Program, says her office is taking unprecedented security measures to ensure system integrity. "With this population, we have made the casting of the Internet ballot as safe, if not safer, than with the mail-in ballots. If we reach a point where things are vulnerable and we can't guard against that, we won't go forward." (AP 12 Jul 2003)

Category 29.4 *Online & electronic voting*

2003-07-24 **impersonation e-voting software flaw election system**

NewsScan

SERIOUS FLAWS IN ELECTRONIC VOTING SYSTEMS
Johns Hopkins University experts say that high-tech voting machine software from Diebold Election Systems has flaws that would let voters cast extra votes and allow poll workers to alter ballots secretly. Aviel D. Rubin, technical director of the Information Security Institute at Johns Hopkins, led a team that examined the Diebold software, which has about 33,000 voting machines operating in the United States. Adam Stubblefield, a colleague of Rubin's, said that "practically anyone in the country — from a teenager on up — could produce these smart cards that could allow someone to vote as many times as they like." Diebold has not seen the Institute's report and would not comment on it in detail, but a company spokesman said: "We're constantly improving it so the technology we have 10 years from now will be better than what we have today. We're always open to anything that can improve our systems." Peter G. Neumann, an expert in computer security at SRI International, said the Diebold code was "just the tip of the iceberg" of problems with electronic voting systems. [Side note: see the interview of Peter Neumann by John Gehl in the archives of the ACM online publication Ubiquity: [http://www.acm.org/ubiquity/interviews/p_neumann_3.html.] (New York Times 24 Jul 2003)

Category 29.4 *Online & electronic voting*

2003-09-11 **electronic voting glitch faulty system fraud Diebold Election Systems Inc.**

NewsScan

DEBATE OVER ELECTRONIC VOTING
During California's March 2002 primary, absentee vote tallies from one county seem to have been sent to an Internet site operated by Diebold Election Systems Inc., the company that manufactured the voting machines used in the election. Activist critics of electronic voting systems say the glitch is new evidence that the technology is intrinsically faulty, but Diebold executive Deborah Seiler says that Diebold engineers may have published the results as part of a test performed days, weeks or months after the county primary (regardless of the time stamp shown): "These activists don't understand what they're looking at." Seiler insists that the company has a system of checks and balances to safeguard against fraud, but that explanation doesn't satisfy Kim Alexander, president of the California Voter Foundation, who charges: "In our quest to deliver faster, more accurate election results, we've left the voting process wide open to new forms of attack and mismanagement." (AP/San Jose Mercury News 11 Sep 2003)

Category 29.4 *Online & electronic voting*

2003-09-12 **voting internet poll tax dean al sharpton howard vote**

NewsScan

SHARPTON CALLS INTERNET VOTING A 'HIGH-TECH POLL TAX'
Democratic presidential candidate Al Sharpton has protested a Democratic Party plan that would, for the first time, allow Internet voting in Michigan's presidential caucus — and is challenging front-runner Howard Dean to stand with him. Sharpton wrote to Dean: "Perhaps it is due to the fact you governed a state with virtually no people of color living within its borders that you are unaware that this is a racially biased proposal." (Vermont is nearly 98% white.) A Dean spokesman said that Dean supports the concept of Internet voting or anything that will people to the polls "as long as it's coupled with the need to insure access to African Americans and others when it might not be available." Calling the scheme a "high-tech poll tax," Sharpton explained: "A grandmother in a housing development is going to have to go downstairs and walk five blocks to vote. Who do you think is going to get more of the vote? Democracy is about equal access. This is not equal access. It really is a high-tech poll tax." (AP/USA Today 12 Sep 2003)

Category 29.4 *Online & electronic voting*

2003-11-03 **electronic e-voting Ireland Irish Labour Party suspension flaws**

RISKS; http://www.labour.ie/press/detail.tmpl?SKU=20031103143251 23 1

Irish Labour Party urges suspension of e-voting until flaws addressed

Eamon Gilmore TD, a spokesman for the Irish Labour Party, said in a press release that the party "has called for the suspension of plans to extend electronic voting until the e-voting system has been changed." The decision resulted from a study of electronic voting systems by two IT experts in the Labour Party. Deputy Gilmore said that this report "identifies a number of major flaws and deficiencies in the electronic voting system…" He lists the major defects in local electronic voting systems. He points out that many of these defects are caused by electronic voting's lack of transparency--a voter "is expected to have blind trust in the technology." Then Depute Gilmore lists some of the Labour Party's proposals to reform local electronic voting. He ends, "It is essential for continuing confidence in the electoral system that the proposed electronic voting be changed. The Government should suspend plans for the extension of electronic voting until the reforms proposed by the Labour Party have been implemented."

Category 29.4 *Online & electronic voting*

2003-11-04 **electronic voting information leakage hacker stanford diebold e-mail servers machines**

NewsScan

ELECTRONIC VOTING DISPUTE
The Electronic Frontier Foundation and Stanford University's Cyberlaw Clinic are suing Diebold Inc., a manufacturer of electronic voting machines, to stop it from issuing threats to groups that publish company documents leaked by a hacker; the hacker broke into Diebold's servers in March (using an employee's ID) and copied thousands of company announcements and internal e-mails. The intruder e-mailed the data to voting activists, some of whom published stories on their Web logs denouncing Diebold. A California advisory panel has refused to certify new Diebold voting machines, pending a determination of whether uncertified software and hardware was used in a recent election. (AP/Los Angeles Times 4 Nov 2003)

Category 29.4 *Online & electronic voting*

2003-11-04 **electronic e-voting California Wired.com uncertified software issue Diebold Election Systems**

RISKS; http://www.wired.com/news/politics/0,1283,61068,00.html 23 1

California Halts E-Vote Certification

Kim Zetter reported in Wired.com that California was stalling the "certification process for new voting machines manufactured by Diebold Election Systems." Marc Carrel, assistant secretary of state of policy and planning, said that his office had received "disconcerting information" about uncertified software running in Deibold touch-screen voting machines in one California county; Secretary of State spokesman Douglas Stone said the matter concerned Alameda county. In a follow-up article in RISKS, contributor David E. Ross noted that the security risks with e-voting in Alameda county were graver than previously thought. He says: "The security of Diebold's touch-screen voting system is so weak that someone outside of Alameda County's election office (someone working for Diebold) had access to make unauthorized changes to the vote-counting software."

Category 29.4 *Online & electronic voting*

2003-11-08 **electronic e-voting mechanical voting risks**

RISKS; http://www.washingtonpost.com/wp-dyn/articles/A1397-2003Nov5.html 23 1

A new risk for electronic voting

Jeremy Epstein wrote a summary of electronic voting risks he observed (quoting his RISKS article):

The RISKS of electronic voting have been discussed often enough in this forum that I won't repeat them further (cf. Rebecca Mercuri's piece in RISKS-22.96). Last week's election in Fairfax County (Virginia) had a new risk I haven't seen covered before. They use WinVote machines, made by Advanced Voting Solutions of Frisco, Tex. These are essentially Windows laptops with a touchscreen and an 802.11 wireless net. (More about that in another RISKS article one of these days.) Seems that during the election, at least eight of the machines failed (out of almost 1000 in use county-wide), and were taken out of the polling places to a central repair facility, and then brought back after some form of "repair" was made (a reboot at the polling place did not solve the problem). The seals were broken, but the voting officials in the precincts were told to resume using them. The result was a lawsuit by the Republican party seeking to invalidate the votes from those machines. There aren't enough votes at stake that it would change any of the election results. Of course, the real problem is that without any sort of physical (paper) record, it's impossible to prove what really happened when the machines were being "repaired". In addition, the "hi tech" vote counting (which was supposed to occur by uploading the results from every precinct to a central computer over a dial-up line) overloaded the servers, and "More than half of precinct officials resorted to the old-fashioned telephone to call in their numbers or even drove the results to headquarters, elections officials said. A handful of precincts went back to paper ballots." The only thing that's surprising here is that the election officials were surprised. See
http://www.washingtonpost.com/wp-dyn/articles/A1397-2003Nov5. html

---

Category 29.4 Online & electronic voting

2003-11-09 **electronic voting machines proprietary source code secret touch-screen ballot fraud**

NYT
http://www.nytimes.com/2003/11/09/business/yourmoney/09vote.html?th=&pagewanted=print&position=

Walden O'Dell wrote a letter in mid-August 2003 to 100 wealthy friends inviting them to a Republican fund-raiser. He included the line, "I am committed to helping Ohio deliver its electoral votes to the president next year." Unfortunately, Mr O'Dell is also the CEO of the Diebold company, makers of paperless voting machines. A political storm has erupted over these machines, which have no independent audit trail or means of convincing a voter that his or her vote is being recorded accurately. Accusations of bias led Mr O'Dell to protest in September 2003, "I'm not doing anything wrong or complicated, but it obviously did leave me open to the criticism I've received."

Category 29.4 Online & electronic voting

2003-11-12 **electronic e-voting glitch error flaw anomalous result Boone County**

RISKS; http://yro.slashdot.org/article.pl?sid=03/11/12/1320208 23 3

Astonishing electronic voting "glitch"

Steve Summit writes that in Boone County 19,000 people were registered to vote. In the first week of November 2003, only 5,352 votes were claimed to have been recorded. However, MicroVote's e-voting software turned up 144,000 votes for that election. Summit asks, "With yet another mistake, does anyone still trust closed-source electronic voting?" Peter Neumann adds: "It's interesting to wonder what might have happened if the initial inaccurate result had not been so glaringly obvious …" In a follow-up article, contributor Martin Ward thinks, while admitting to his paranoia, that ""someone" is testing to see just how big a "glitch" they can get away with, while at the same time getting the punters accustomed to regular "glitches" in e-voting software (just as MS has got people accustomed to desktops which regularly crash, freeze or scramble documents)."

Category 29.4 Online & electronic voting

2003-11-13 **electronic e-voting report Congressional Research Service CRS direct recording DRE**

RISKS; http://www.epic.org/privacy/voting/crsreport.pdf 23 3

Report raises more questions about voting machines

In a report entitled, "Election Reform and Electronic Voting Systems: Analysis of Security Issues," the Congressional Research Service (CRS) examines threats to direction recording electronic (DRE) voting machines. This report states, "at least some current DREs clearly exhibit security vulnerabilities. Those vulnerabilities pose potential … risks to the integrity of elections." In addition to noting vulnerabilities in DREs, this report lists proposals to plug those holes and improve security. For example, it suggests "requiring voter-verifiable paper print-outs of vote selection for voters to review."

Category 29.4 Online & electronic voting

2003-11-13 **electronic e-voting confirmation failure integrity**

RISKS; http://finance.lycos.com/home/news/story.asp?story=36422485 23 3

The computer is ALWAYS right

Charles Lamb talks about an e-voting failure in Southington, CT: the town was testing an e-voting system that produced vote-confirmation chits. Avante International's Vote-Trakker machine was run in parallel to a traditional election process. But whenever a voter's confirmation printout didn't match her actual vote the registrar did nothing to correct the vote.

Category 29.4 *Online & electronic voting*

2003-11-13 **electronic e-voting California Diebold software changes**

RISKS; http://www.ss.ca.gov/executive/press_releases/2003/03_100.pdf 23 3

More on Diebold installing uncertified software in California

Peter Neumann discusses an article in the LA Times about Diebold's Accuvote touchscreen voting machines. The article was titled, "Secretary of State Orders Audit of All Counties' Voting Systems: Review of upgraded touchscreen software leads to discovery that two registrars installed it without state's OK." In this article, LA Registrar Conny McCormack says that registrars had long been making changes to their counties' voting system software without state approval. He adds that California Secretary of State Kevin Kelley had known this all along. In this case, Peter Neumann worries about weak Federal Election Commission e-voting standards. He also fears the possibility of Trojan Horse code being inserted in secret changes to e-voting software as in the above case. In a follow-up article, contributor Lillie Coney noted that California Secretary of State Kevin Shelley could ban Diebold selling voting machines in California altogether.

Category 29.4 *Online & electronic voting*

2003-11-18 **EFF Electronic Frontier Foundation Diebold leaked documents security problems**

NewsScan

ELECTRONIC VOTING LAWSUIT

The Electronic Frontier Foundation, a civil liberties advocacy group, says it fears legal threats from Diebold Inc., the maker of electronic voting systems. Diebold has asked a U.S. district court in San Jose to bar Diebold from sending cease-and-desist letters to activists who have published links to leaked documents about alleged security problems with the company's equipment. Diebold's response is that the company has never had an intention to stifle intent to free speech or place onerous burdens on Internet service providers, but that it strenuously objects to the "wholesale reproduction" by activists of 13,000 pages of internal, proprietary documents. Diebold's attorney argues: "The plaintiffs advocate an open-source code system for elections code. These materials were intended to be secret and private and proprietary." (AP/Washington Post 18 Nov 2003)

Category 29.4 *Online & electronic voting*

2003-11-20 **voting online internet democrats dean clark michigan poor blacks portesting**

NewsScan

MICHIGAN DEMS WANT INTERNET VOTING

Democrats in Michigan want to increase turnout in their presidential caucus by allowing Internet voting. All of front-runner Howard Dean's opponents except Wesley Clark are protesting the plan, saying that Internet voting puts blacks and the poor at a disadvantage by making access difficult. Under the plan, registered Michigan Democrats who want to vote by mail or Internet will request an absentee ballot from the state party ahead of time; they will then be sent a ballot that can either be returned by mail or used to obtain a code that will allow voting by Internet. Donna Brazile, former Gore strategist, says that with improvements that have bee made to the Internet voting system, "the access argument sort of melts away." (AP/USA Today 20 Nov 2003)

Category 29.4 *Online & electronic voting*

2003-11-21 **electronic e-voting California paper audit trail voter receipts**

RISKS; http://www.wired.com/news/evote/0,2645,61334,00.html 23 4

California to require voting machine receipts and stricter auditing

Steve Bellovin observes that California's Secretary of State Kevin Shelley mandated a "voter verified paper audit trail" for all voting machines in the state by the year 2006. Bellovin adds: "He [Secretary of State Kevin Shelley] also introduced stricter requirements for testing and auditing the software used for both recording and tabulating votes." Peter Neumann responds to this action by the California SoS: "CA SoS Shelley has apparently taken the recommendations of some of the members of his review panel seriously, in light of recent strange events previously recorded here."

Category 29.4 *Online & electronic voting*

2003-11-25 **worm virus Nachi Diebold Automatic Teller Machines ATM Windows XP embedded**

RISKS; http://www.theregister.co.uk/content/55/34175. html 23 4

Diebold ATMs hit by Nachi worm

Steve Summit writes about Diebold ATM running Windows XP Embedded becoming infected by the Nachi worm. Even though the ATMs were not on the public Internet, the worm is thought to have penetrated firewalls to reach private internets. Commenting that this incident was part of a larger trend, Steve Summit worries about "critical functions" being "implemented using less-than-rugged components such as "consumer grade" operating systems." In a follow-up article, contributor Lillie Coney quotes some security experts' reactions to the above incident. For example, Bruce Schneier said: "Specific purpose machines, like microwave ovens and until now ATM machines, never got viruses. Now that they are using a general purpose operating system, Diebold should expect a lot more of this in the future." Steve Grzymkowski, a senior product marketing manager at Diebold was paraphrased: "Diebold switched from using IBM's OS/2 on its ATMs because banks were requesting Windows." In a different article, contributor Drew Dean describes a scenario in which "[I]t's both faster and cheaper for the bank's data center to remotely patch the ATMs from a central location." So he maintains that solving ATM-worm-infection problem by gravely limiting ATM network connectivity will negatively affect manageability, and introduce new threats. Tim Panton disagrees with Drew Dean's angle on ATM patching. Panton feels that ATMs--unlike "fully autonomous systems, like weather stations or unmanned space craft"--require human contact for replenishing cash. Therefore, forcing only remote ATM patching is not the best practice.

Category 29.4 *Online & electronic voting*

2003-12-01 **Diebold voting machines leaked documents EFF Electronic Frontier Foundation forum public discussion internet security holes**

NewsScan

DIEBOLD BACKS OFF — AT LEAST FOR AWHILE

After considerable controversy, the Diebold company, which makes electronic voting machines, has agreed not to sue voting rights advocates who published leaked documents about alleged security breaches on their machines. Dozens of students, computer scientists and Internet service providers were sent cease-and-desist letters and threatened with law suits Electronic Frontier Foundation attorney Wendy Seltzer says, "This is a huge victory that shows we have weapons on our side to protect free speech from overbearing copyright laws so that the Internet remains a forum for public discussion. We're trying to hammer home that you can't go around making idle threats that aren't backed up by the law." But a Diebold executive says the company will continue to monitor the online proliferation of the leaked documents, and may file lawsuits against others who publish the data.(AP/USA Today 1 Dec 2003)

Category 29.4 *Online & electronic voting*

2003-12-03 **electronic e-voting issues discussion paper trail voter**

RISKS 23 6

Voter-verified breadcrumb trail?

Contributor Dave Brunberg vents, "Why not just admit that e-voting cannot be made secure without adding in so much complexity that it becomes prohibitively expensive or self-defeating?" He opines that although a paper printout of an e-ballot is a necessary step in e-voting security, it could be "a serious insecurity of the false-sense-of-security type." He goes on to raise some still-unanswered questions about e-voting security, such as: "What guarantee is there that no alterations occurred between the touchscreen station and the recording station?", "Once you get out of the actual voting station and the printer, what, if anything, guarantees that votes aren't swapped or dropped?", "And, for areas where physical intimidation may be a factor, how can the voter be assured of anonymous voting when the printer spits out the name of their selections for anyone to see?" Peter Neumann responds to Dave Brunberg in three points. First, he says that paper ballots, not e-ballots, should be the ballots actually counted. E-ballots could "appease the media only for an UNOFFICIAL PRELIMINARY count." Second, he feels that the appearance of discrepancy between paper- and e-ballots from a voting machine should result in the deactivation of that voting machine "for the duration of the election." Third, he affirms that Brunberg's question of why we need e-voting machines at all is valid. In a following article, William Ehrich points out that a paper trail for e-voting is much like having "the voter simply mark the piece of paper with a felt marker." He recommends using paper ballots and electronic-ballot-counting machines. He concludes that using computers where they're not requisite "can do more harm than good." In another article, contributor Russ Cooper attempts to answer the question, "Why have electronic voting machines at all?" He feels that remote electronic voting may encourage greater voter participation: it takes lesser time to cast an e-ballot from one's own home than to do the same by visiting a polling station. In a different article, Finn Poschman refutes Russ Cooper's argument. He says that the costs of "achieving a reasonably fair and verifiable e-vote-from-home" are heavy while the benefits are few. Sander Tekelenburg has a different rebuttal to Russ Cooper: "Voting from the privacy of your home would make it even easier for people to force each other to vote for candidate x than the 'regular' abuse within the sacrecy of the home that's already happening on a grand scale. A public voting station, with secret voting, avoids that RISK."

Category 29.4 *Online & electronic voting*

2003-12-08 **secure voting machines sufficient enough intrusion hackers**

NewsScan

SECURITY CONCERNS ABOUT VOTING MACHINES
Diebold and other companies that make electronic voting machines are joining forces to make the case that electronic voting technology is sufficiently secure to withstand intrusion by hackers. A number of computer experts have argued that the new machines have security problems, and that they should be equipped to provide companion paper records for auditing purposes. Paper printers could add $500 to the cost of each machine. (Washington Post 8 Dec 2003)

Category 29.4 *Online & electronic voting*

2003-12-15 **electronic e-voting companies felons employment**

RISKS; http://www.bayarea.com/mld/mercurynews/news/local/7507193.htm 23 7

Convicted felons worked for electronic voting companies

Contributor Susan Marie Weber writes about voter advocate Bev Harris' allegation of five ex-felons working at a subsidiary of electric voting company Diebold Inc. One felon, for example, programmer Jeffrey Dean, had "served time in a Washington correctional facility for stealing money and tampering with computer files in a scheme that "involved a high degree of sophistication and planning."" A bill to tighten voting company hiring standards was being introduced in January 2004 by Senator Barbara Boxer (D-California).

Category 29.4 *Online & electronic voting*

2003-12-26 **electronic e-voting principles Australia procedure**

RISKS 23 10

Elections Down Under

Responding to discussions in RISKS about e-voting in the United States, Peter Williams outlines how elections are conducted in Australia: Elections are managed by the AEC, an independent federal organization affiliated with no political party. All balloting is done by hand--voters rank the candidates in order of preference. Though ballots are hand-counted, the results are available within a few hours of an election. Voting is mandatory for everyone over age 18, and any adult not voting is fined. Peter Williams also lists his suggestions for computerized voting system. First, he says that the "specifications, source code, test procedures and results" of a computer-voting system should be freely available for public scrutiny. Second, he suggests using secure, well-configured, minimalist operating systems to run the voting software. Next, he recommends a voter paper trail that is also available to election officials to verify electronic votes. Finally, he suggests extensive logging and auditing to so that results can be checked "confidently". In a follow-up article, Mark Newton clarifies the mandatory-voting-if-over-18 aspect of Australian elections. Newton points out that voting in Australia is not compulsory. However, it is compulsory to register to vote if you're over 18 and to show up at a polling station during elections. At the polling station, after checking yourself off for attending, you can choose to either vote or not vote. In another follow-up article, contributor Eric Ulevik corrects some misinformation in earlier posts about the Australian electoral system. Ulevik observes that "[S]imply getting your name checked off and leaving," like Mark Newton had written, "may result in the Electoral Commission staff recording a failure to vote." This, in the Australian state of New South Wales, would cost you a $120 fine. If you refuse to pay this fine you could lose your driver's license. Because avoiding elections altogther in Australia carries penalties, if you don't want to vote there, Eric Ulevik suggests casting a "'donkey' vote." He casts his 'donkey' vote by giving his "preference by order on the ballot (which is determined randomly)." Ulevik concludes: "The clear risk here is that attempting to enforce democratic principles increases the influence of random chance on the final results."

Category 29.4 *Online & electronic voting*

2003-12-30 **electronic e-voting encryption software break-in intrusion**

RISKS; http://www.msnbc.msn.com/id/3825143 23 10

VoteHere reports computer break-in

An article on MSNBC.com said that federal authorities were investigation a network intrusion at VoteHere, a secure e-voting company. VoteHere's founder Jim Adler thought that the intrusion may have been politically motivated. The MSNBC article noted: "Adler's revelation came amid a deepening debate over e-voting and its vulnerability to election fraud -- and a controversy over surreptitious methods to get information about how e-voting software works." RISKS moderator Peter Neumann added that VoteHere later knew who the intruder was. In a follow-up article, contributor Rebecca Mercuri questions VoteHere's trustworthiness as a secure e-voting system maker in the wake of such a network intrusion: "VoteHere is selling an Internet voting product but they apparently aren't capable of protecting their own network from attack and their sensitive files from theft." As a result of the VoteHere network break-in, Mercuri says she actually feels better that VoteHere's proprietary source code could be examined by the intruder and his "pals".

Category 29.4 *Online & electronic voting*

2004-01-01 **electronic voting hardware operating system reliability question**

RISKS 23 11

ELECTRONIC VOTING: COMPUTER RELIABILITY ASPECTS

Contributor Bob Axtell describes a reliability-testing project he performed to ask about e-voting machine reliability. Axtell tested 50 CPUs and two Windows operating systems over a three-month period. His project's findings showed Windows to be too unreliable for a financial service application. Axtell demands, "Why is it that my financial client saw fit to verify hardware security, yet States don't seem to see a need…"

Category 29.4 *Online & electronic voting*

2004-01-15 **online electronic Internet poll voters politicians Senate Republican Conference**

RISKS; 23 13
http://atrios.blogspot.com/2004_01_11_atrios_archive.html#107414565730750569

ONLINE POLL RIGGING

Contributor Keith C. Ivey writes about a case of online poll rigging by the Senate Republican Conference. When results about a poll about the capture of Saddam Hussein didn't go as expected, the recorded answers to the poll question were interchanged in secret. Ivey asks, "If politicians are willing to tamper with something as insignificant as a Web poll, how much more tempting is it to tamper with the results of a real election?"

Category 29.4 *Online & electronic voting*

2004-01-21 **electronic Internet voting criticised COTs**

NewsScan

INTERNET VOTING DISPUTE

An Internet-voting program written for the Pentagon by Accenture eDemocracy Services for use by men and women serving overseas is being fiercely criticized by security experts Avi Rubin of Johns Hopkins University and retired IBM researcher Barbara Simons. Rubin says, "It's not possible to create a secure voting system with off-the-shelf PCs using Microsoft Windows and the current Internet. History has shown that when people have the opportunity to tamper with an election they do." On the other side of the issue, R. Michael Alvarez, co-director of the CalTech-MIT Voting Technology Project says: "The chance of a security threat has to be weighed against the knowledge gained and the improved voting access for those people. There's a widespread perception that Internet voting is going to happen at some time. As scientists, we'd like to lay out some kind of rational path that leads from punch cards and lever machines to that logical future." (Washington Post 21 Jan 2004)

Category 29.4 *Online & electronic voting*

2004-01-23 **electronic e-voting discourage analysis hacking fraud error quality assurance**

NIPC/DHS; http://www.gcn.com/vol1_no1/security/24681−1.html

January 22, Government Computer News — Security analysts recommend scrapping online voting plans.

A group of security analysts who have evaluated Department of Defense (DoD) plans for an online voting pilot have recommended that the plan be scrapped because its security cannot be ensured. The analysts concluded "Internet voting presents far too many opportunities for hackers or even terrorists to interfere with fair and accurate voting." The DoD, however, said it has no intention of stopping the program. "Security was our Number One priority when we started on this concept," DoD spokesman Glenn Flood said. The Secure Electronic Registration and Voting Experiment (SERVE) is a DoD program being operated by the Federal Voting Assistance Program (FVAP) to ease absentee voting procedures for U.S. citizens living or serving overseas. A 10-member Security Peer Review Group put together by FVAP evaluated the system. A minority report was issued by four members of the group. The report said inherent flaws in proprietary software, the Internet and PCs from which votes would be cast make the process too risky to be used in a real election. Threats include insider flaws, denial-of-service attacks, spoofing attacks, and malicious code. Flood said weaknesses in the Internet infrastructure were taken into account in designing SERVE.

Category 29.4 *Online & electronic voting*

2004-01-30 **electronic online voting citizens abroad disapproved politics**

NewsScan

BIPARTISAN COALITION GIVES THUMBS DOWN TO INTERNET VOTING

Politics makes for strange bedfellows, demonstrated by the pairing up of both the Republican and Democratic party organizations for U.S. citizens living abroad against the Pentagon's Federal Voting Assistance Program, which is sponsoring a $22-million Internet voting experiment. The leaders of Republicans Abroad and Democrats Abroad have joined forces with the Association of Americans Resident Overseas, American Citizens Abroad and the Federation of American Women's Clubs Overseas in an appeal to Congress and Defense Secretary Donald Rumsfeld to stop the program now. "We've heard so much about the doubtful security of online voting, so we're concerned that we're going too fast," says the U.S. liaison for the women's clubs. "One day this might be absolutely wonderful. In the meantime, we might find ourselves with a kind of a super-2000 disaster, and people will think online voting will never be possible." The trial program is open to all overseas residents from 50 counties that have signed up with the Pentagon, but it suffered a setback last week when computer security experts released a report detailing the inherent vulnerabilities in the system what would leave it wide open to hacking. (Washington Post 30 Jan 2004)

Category 29.4 *Online & electronic voting*

2004-02-06 **electronic e-voting election Pentagon cancel security concern**

NewsScan

PENTAGON CANCELS E-VOTING PLANS

Because of security concerns, the Department of Defense has canceled plans to use an electronic voting system that would have been used by Americans overseas to cast their votes next November; the system is called Secure Electronic Registration and Voting Experiment (SERVE). Deputy Defense Secretary Paul D. Wolfowitz said in a memo: "The department has decided not to use SERVE in the November 2004 elections. We made this decision in view of the inability to ensure legitimacy of votes, thereby bringing into doubt the integrity of the election results." Wolfowitz goes on to say that the system will continue to be used for testing and development purposes. Meg T. McLaughlin, president of Accenture eDemocracy Services, says the decision to continue testing the system will provide "an opportunity to demonstrate that the Internet is viable, valuable and secure enough to use for filing absentee ballots. We are confident that sending absentee ballots via the Internet is just as secure and reliable as sending them by mail." (New York Times 6 Feb 2004)

Category 29.4 Online & electronic voting

2004-02-10 **electronic voting analysis flaws problems resources**

http://www.nwfusion.com/newsletters/sec/2004/0209sec1.html

Securing Vote Tallies

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Vermont has a tiny population; we have about 600,000 people in the entire state. Because of this small population, people here have many ways of becoming involved in civic affairs. Our state house in Montpelier (the smallest state capital city in the US, with 8,000 people) is open to the public, as are committee meetings. State officials such as the governor often walk about in town where ordinary citizens can chat with them in a friendly and very personal way.

I was recently invited to address the Government Operations Committee as they discussed a pending bill which would require any wholly electronic voting mechanism to be equipped with a means of producing a paper ballot that could be inspected by the voter and which would then be stored safely for official recounts. Given the importance of safeguarding the vote in our nation, I thought it might interest readers to step outside the confines of network security for a moment to consider the security implications of wholly electronic voting.

Today, there are three different forms of voting in place in use in the USA (I won't discuss remote, Internet-based voting in this column): one can mark a piece of paper by hand and have it read by people; one can mark a piece of paper by hand or machine and have it read by an optical-mark reader which tallies the results automatically; or one can use a wholly-electronic system with an input device such as a touch-sensitive screen which stores the results in a database and produces automatic tallies.

Normally, paper ballots, whether read by people or tallied by machines, are stored in sealed containers and can be opened with a court order in cases of judicially-approved recounts when election results are challenged.

In Vermont, the Secretary of State's office allows optical-mark readers to be used for elections; only one such machine is required per voting location, most of which have at most a few thousand voters registered per location. However, most locations still use manual counting of ballots under the supervision of representatives of the various political parties involved in the election.

In my testimony before the Government Operations Committee, I stressed the following points:

* Any system of vote counting that relies on completely proprietary (secret) programs is potentially vulnerable to abuse. The underlying computer programs controlling how marks on ballots are counted in Vermont are proprietary (they are owned by Diebold Corporation), but the technicians who prepare the configuration tables relating a position on a ballot to a particular name work for an independent consultancy in Massachusetts and their configuration tables are open for inspection.

* Every optical tabulator is tested to see if it reads ballots correctly before the election begins.

* Passing a law that allows the Secretary of State to order a random check on the accuracy of machine tallies in any voting district will help prevent systematic fraud. The tallies in a manual recount must match the machine tallies to within an acceptable error rate (to allow for the inherent difference between machine tallies and human counting methods: machine reject incorrectly-marked ballots whereas people can agree on the intention of the voter).

* Wholly-computer-based voting systems have far more vulnerabilities to tampering than optical-mark sensors. We know that even companies such as Microsoft have allowed Easter Eggs (unauthorized, undocumented code such as flight simulators) to escape quality assurance and be delivered to customers in software such as MS-Excel. We know that microprocessors have been tampered with to cheat clients and evade testing (e.g., gas pump meters in the Los Angeles district were designed to overcharge customers by 10% -- unless they noticed one- or five-gallon deliveries, which were the volumes typically used by inspectors when checking accuracy). We know that production code has been profoundly flawed for years without being caught (e.g., the Colorado lottery's not-very-random-number generator that produced only numbers from zero to eight but never any nines). We know that data stored in databases without careful attention to chained cryptographic checksums involving timestamps, sequence numbers and the previous record's checksum can be modified to misrepresent election results.

* For all these reasons, we should resist the use of wholly-computerized voting machines until there is software that is entirely open to inspection.

* Any wholly-electronic voting machine should be required to produce a paper ballot showing the voter's choices for inspection by that voter (only). The voter should then be required to place the ballot in a ballot box for use in judicial recounts and random testing of the accuracy of the computerized voting system.

* * *

For further reading:

Background paper on all aspects of electronic voting < http://lorrie.cranor.org/voting/hotlist.html >
White Paper on the use of receipts in voting < http://www.vreceipt.com/article.pdf >
Dangers of proprietary code in voting machines < http://www.blackboxvoting.org >

See also several articles and press releases about electronic voting on the Electronic Frontier Foundation Web site at < http://www.eff.org >
and reports on the activist Web site < http://www.verifiedvoting.org >.

Category 29.4 *Online & electronic voting*

2004-02-15 **e-voting machine errors election invalidated**

RISKS 23 19

MISSISSIPPI VOIDS NOVEMBER 2003 E-VOTE ELECTION FOR ERRORS

Rebecca Mercuri contributed a report on the failure of WINnVote touchscreen voting machines in Hinds County, Mississippi in the November 2003 election. "Poll workers had trouble starting the machines, some of the machines overheated and had to be taken out of service, poll workers were scrambling to find enough paper ballots, and many voters left with polls without voting because of the long delays. " As a result of the SNAFU, the Mississippi Ssenate ordered a new election.

Category 29.4 *Online & electronic voting*

2004-02-25 **e-voting physical security tampering fraud hacking**

RISKS 23 20

PHYSICAL SECURITY OF ELECTRONIC VOTING TERMINALS

Tobin Fricke reported in RISKS on sloppy security for e-voting equipment: "A cart of Diebold electronic voting machines was delivered today to the common room of this Berkeley, CA boarding house, which will be a polling place on Tuesday's primary election. The machines are on a cart which is wrapped in plastic wrap (the same as the stuff we use in the kitchen). A few cable locks (bicycle locks, it seems) provide the appearance of physical security, but they aren't threaded through each machine. Moreover, someone fiddling with the cable locks, I am told, announced after less than a minute of fiddling that he had found the three-digit combination to be the same small integer repeated three times.

One wonders whether paper ballots would be handled differently, how the terminals are stored between elections, what checks are done for tampering before the use of the terminals, and what physical security features are built into them."

Category 29.4 *Online & electronic voting*

2004-03-02 **e-voting failures bootup delays disenfranchisement**

RISKS 23 25

E-VOTING FAILURES IN CALIFORNIA

A posting in RISKS 23.25 reported a number of e-voting failures in California for local elections. All of the reported problems involved systems refusing to boot. Voters were turned away, sometimes several times, and told to try again later in the day. Some of these would find it difficult to get back to their home precincts after work in time to vote.

Category 29.4 *Online & electronic voting*

2004-03-02 **electronic e-voting touch screen voting machine issues political**

NewsScan

TOUCHY (AND UNCLEAR) SUBJECT

Supporters of the new touch-screen voting machines promise paperless elections cheaper and faster to administer, but there are plenty of skeptics. David Jefferson, a computer scientist at the Lawrence Livermore National Laboratory, warns: "Once a ballot is cast, you can't pull it back out. After the fact, you cannot recover from problems. It's not like a financial system, where you can take reasonable risks; in voting, you just can't." MIT computer science professor Ted Selker, more optimistic about the machines, says: "There are things that are scary that don't happen. And the versions of the software have been such that somebody with nefarious goals would be as confused as the rest of us if they tried." CalTech political scientist R. Michael Alvarez agrees with Selker, but adds: "The issue of voting systems has gotten very politicized in the last year. The overriding issue now is that there's an enormous amount of uncertainty election administrators have about what technological change is happening and what's going to be permitted under the law, and it's not entirely clear that we're going to have the technology to meet the requirements that have been put out there." (Los Angeles Times 2 Mar 2004)

Category 29.4 *Online & electronic voting*

2004-03-03 **electronic online e-voting glitches elections frozen screens malfunctions**

NewsScan

ELECTRONIC VOTING SUFFERS GLITCHES

Voters in California, Georgia and Maryland reported problems with their attempts to cast electronic ballots, citing a frustrating mix of frozen screens, encoder problems and other malfunctions that caused delays of up to two hours and forced some voters to travel to other polling sites to cast old-fashioned paper ballots. Election officials blamed improperly trained poll workers, but critics say Tuesday's experience is just a harbinger of worse things to come next fall, when at least 50 million voters — almost half of the expected voter turnout — will use touch-screen voting systems. "Unless Congress deals with this problem immediately by requiring voting machines to produce a paper record voters can verify, we're going to have more of these occurrences each time we have an election, including this November," says New Jersey Rep. Rush Holt. "The only question is, how long it will take before voters lose faith in a system that they thought was being fixed?" (AP 3 Mar 2004)

Category 29.4 *Online & electronic voting*

2004-03-30 **electronic e-voting Pentagon test end**

NewsScan

PENTAGON ENDS TEST OF INTERNET VOTING

The U.S. Department of Defense has decided to terminate its $22 million pilot project designed to test Internet voting for 100,000 American military personnel and civilians living overseas. Because of concerns about the security of online voting, the department had already decided not to allow Internet ballots to be counted in the presidential election, and has now decided to scrap the whole project — at least for the discernible future. A Pentagon spokesman says: "It's not that it's never going to go in test mode. It's that right now we're not going to do it. We have to step back and look at everything that we've done for two or three years in this thing. But right now we're not going forward." (AP/Washington Post 30 Mar 2004)

Category 29.4 Online & electronic voting

2004-04-13 **electronic voting**

http://www.dissidentvoice.org/April2004/Landes0413.htm

As the battle over voting machines rages across the country, the U.S. Commission on Civil Rights met on 9 Apr 2004, to examine the "Integrity, Security and Accessibility in the Nation's Readiness to Vote." Two scientists and four representatives of civil rights organizations were invited to brief the Commission.

But, before the panelists had a chance to share their views, three Republican commissioners and one (notably conservative) Independent commissioner walked out, ostensibly over a personnel dispute. But, others are not so sure.

It appears that voting technology is a topic that the Republican leadership wants to tightly control. It is without doubt that Republicans own most of the companies that manufacture, sell, and service voting machines. And President Bush and the Republican Congress appear determined to control and limit oversight of the elections industry. The Bush Administration has stacked the Election Assistance Commission with supporters of paperless voting technology, while the National Institute of Standards and Technology's (NIST) got walloped with a $22 million budget cut in fiscal 2004, which means that NIST will have to cut back substantially on its cyber security work, as well as completely stop all work on voting technology for the Help America Vote Act.

Category 29.4 Online & electronic voting

2004-04-22 **e-voting electronic paper backups battery failure Marlyland lawsuit lose**

NewsScan

MD. GROUP DEMANDS PAPER BACKUP FOR E-VOTES

A voter advocacy group in Maryland is suing that state's Board of Elections to prevent the use of touch-screen voting machines until a paper record is installed as auditable backup for the system. At present, the state's Diebold voting machines are not set up to produce a paper record of each individual vote. Linda H. Lamone, the state elections administrator, says that paper records are unnecessary because the Diebold system is equipped to preserve votes in its memory: "It's stored in two different locations. If we have battery failure, it still doesn't lose votes." She also said: "It's going to be next to impossible for anyone to gain access to manipulate the election. If anyone tries it, we're going to put them in jail." (Washington Post 22 Apr 2004)

Category 29.4 Online & electronic voting

2004-04-22 **India e-voting general elections largest democracy save trees**

NewsScan

INDIA IMPLEMENTS E-VOTING

For decades, millions of illiterate Indians voted by pressing their thumbprints on ballot cards. This year, they'll just press a button -- and so will everyone else. India's general elections, which began Tuesday, are set to make the world's largest democracy also the world's largest user of computerized voting machines. This year, in a staggered vote that runs through May 10, India's 660 million registered voters will be able to exercise their franchise on one of approximately 1 million computerized voting machines in an electronic, ballot-less election. The change in India is having a deep impact on politics. Supporters say it's also good for the environment in a country trying to save its vanishing forests. More than 8,000 tons of paper, made from approximately 16 million trees, has been used to print ballots for past federal elections. (The Australian 22 Apr 2004)

Category 29.4 Online & electronic voting

2004-04-22 **e-voting paperless Diebold touch-screen security errors**

NewsScan

CALIFORNIA PANEL NIXES DIEBOLD VOTING MACHINES

California's Voting Systems and Procedures Panel has recommended discontinuing the use of 15,000 its Diebold touch-screen voting machines, saying that the systems had malfunctioned in the state's March primary election in March and caused many voters in San Diego County to be turned away. (AP/USA Today 22 Apr 2004)

Category 29.4 Online & electronic voting

2004-04-24 **electronic e-voting legislators wary Diebold concern**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/articles/A38997−2004Apr 24.html

April 24, Associated Press — Legislators wary of electronic voting.

Computer scientists have long criticized touchscreen voting machines as not being much more reliable than home computers, which can crash, malfunction and fall prey to hackers and viruses. Now, a series of failures in primaries across the nation has shaken confidence in the technology installed at thousands of precincts. At least 20 states have introduced legislation requiring a paper record of every vote cast. On Thursday, April 22, a California panel unanimously recommended banning a Diebold Inc. paperless touchscreen model. Secretary of State Kevin Shelley, who said Diebold glitches "jeopardized the outcome" of the March 2 primary, has until April 30 to decide whether to decertify Diebold and possibly other touchscreen terminals in California. The bipartisan U.S. Election Assistance Commission, formed in January to develop technical standards for electronic voting, will conduct a May 5 public hearing in Washington, DC. Computer scientists say paperless systems made by Sequoia Voting Systems Inc. and other competitors also expose elections to malicious attack, software glitches and mechanical errors that could delete or alter millions of ballots.

Category 29.4 Online & electronic voting

2004-04-29 **Diebold electronic paperless voting machines vulnerabilities hacking perversion distortion election**

http://www.nytimes.com/2004/05/03/technology/03vote.html?th=&pagewanted=print&position=

Professor Aviel Rubin, Technical Director of the Information Security Institute of Johns Hopkins University, demonstrated the vulnerability of paperless electronic voting systems to hacking in a classroom demonstration in April. As John Schwartz of the New York Times wrote, "The fix was in, and it was devilishly hard to detect. Software within electronic voting machines had been corrupted with malicious code squirreled away in images on the touch screen. When activated with a specific series of voting choices, the rogue program would tip the results of a precinct toward a certain candidate. Then the program would disappear without a trace."

Professor Rubin published an analysis of 49,000 lines of the bold voting machine code in July 2003. the security implications were grim, as he and his colleagues wrote: "Our analysis shows that this voting system is far below even the most minimal security standards applicable in other contexts. We conclude that, as a society, we must carefully consider the risks inherent in electronic voting, as it places our very democracy at risk." in a report on his experience as an election scrutineer, he wrote, "I started realizing that some of the attacks described in our initial paper were actually quite unrealistic, at least in a precinct with judges who worked as hard as ours did and who were as vigilant. At the same time, I found that I had underestimated some of the threats before…. I continue to believe that the Diebold voting machines represent a huge threat to our democracy."

Category 29.4 Online & electronic voting

2004-05-06 **Diebold voting machines security problems lawsuits**

NYT Circuits

David Pogue of the New York Times wrote a blistering editorial criticizing Diebold and other electronic-voting machine manufacturers. He wrote,

>Remember how, a few months back, I expressed my horror that Diebold's touch-screen voting machines, which one in five Americans will use in this fall's elections, were failing every security test? Its technicians make changes to the machines' software AFTER inspection by local election boards. The machines' software is not made available for public inspection — an unacceptable situation in what's supposed to be a democracy. And incredibly, these machines produce no paper record of the votes.

They're also buggy. During California's presidential primary in March, machines in more than half of San Diego County's precincts malfunctioned.

I'm happy to report that the nation is finally waking up. Many states, as well as Federal lawmakers, are considering legislation that requires voting machines to leave a paper trail. Better yet, California Secretary of State Kevin Shelley had the guts to ban or decertify tens of thousands of Diebold machines across California. He's even considering filing criminal or civil charges against the company.

My guess is that if the defiant, unhelpful Diebold doesn't start showing some humility, fixing its work and letting the public see what it's doing under the hood, California will be only the first state of many to get wise.<

Category 29.4 Online & electronic voting

2004-05-06 **Diebold electronic paperless voting machines vulnerabilities hacking perversion distortion election**

http://www.computerworld.com/printthis/2004/0,4814,92950,00.html

Voting-machine vendors sneered at the analysis of security vulnerabilities presented in testimony before the U.S. Election Assistance Commission in early May 2004. Officials received scientific reports of simple introduction of Trojan horse software into the machines to distort election results, the impossibility of verifying accuracy of results without a voter-verified paper ballot for audit purposes, and the use of inadequate encryption for transmission of data (including a single hardwired key for all the voting machines). The representatives of the voting machines dismissed the objections as theoretical and unrealistic but never addressed the fundamental problem: a voter cannot know whether his or her vote has been registered correctly by the machines if there is no independent mechanism of validation.

Category 29.4 Online & electronic voting

2004-05-12 **e-voting Diebold fund-raising politics marketing mistake error**

http://www.nytimes.com/2004/05/12/politics/campaign/12vote.html

Walden W. O'Dell, the chairman and chief executive of Diebold Inc., said on Monday [10 May 2004] that it had been a "huge mistake" for him, as the head of a voting machine company, to express support for President Bush's re-election in a fund-raising letter last year. Mr. O'Dell also said the company was working to address computer security problems and build voter confidence in its wares.

Category 29.4 Online & electronic voting

2004-05-24 **e-voting electronic voting concerns Virginia study**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/articles/A51595−2004May 24.html

May 24, Washington Post — E-voting woes prompt Virginia study.

Virginia General Assembly leaders say they will soon appoint members of a new commission that will study the security and reliability of electronic voting machines, a response to growing concerns that new-generation voting technology may be riddled with problems. Commission members could be announced as soon as this week, though the final list may not be named until the end of June. The commission will be composed of six members of the General Assembly and five private citizens. They will study how voting equipment is certified and tested and how the equipment should be handled before, during and after it is used. The panel ultimately could propose a statewide system for verifying electronic voting machine accuracy, according to lawmakers and other officials involved in the commission's creation. Lawmakers, academic experts and citizen-activists across the country are urging changes in how the machines work, proposing that electronic voting machines produce paper receipts for each vote. Another proposal is to require the software that powers new voting machines to meet certain standards set by public officials. California and Ohio currently require that electronic voting machines have verifiable paper trails by 2006.

Category 29.4 Online & electronic voting

2004-06-08 **electronic voting e-voting research Election Assistance Commission**

NewsScan

E-VOTING OVERSEER WANTS 'MORE RESEARCH' ON PAPER BACKUP BALLOTS

DeForest B. Soaries, the head of the federal Election Assistance Commission, says he wants election officials to be able to analyze software source code in the electronic systems they purchase. Some vendors have resisted providing source code, on the ground that it is proprietary information. As for requiring that the systems produce paper copies of votes cast electronically, Soaries is undecided: "If there was unanimity among scholars and scientists on the paper issue it would be a more compelling case. All of the research, all of the testimony we've received, all the writings that I've read argue for more research." (AP/Los Angeles Times 8 Jun 2004)

Category 29.4 *Online & electronic voting*

2004-06-14 **electronic e-voting paperless League of Women Voters**

NewsScan

LEAGUE OF WOMEN VOTERS SAYS NO TO PAPERLESS VOTING SYSTEMS

The League of Women Voters has withdrawn its support of electronic voting machines that can't produce auditable paper backup copies of individual ballots. Computer scientist Barbara Simmons, a member of the League as well as a past president of the Association for Computing Machinery (ACM), said: "My initial reaction is incredible joy and relief. This issue was threatening to split the League apart… The league now has a position that I feel very comfortable supporting." (AP/San Jose Mercury News 14 Jun 2004)

Category 29.4 *Online & electronic voting*

2004-07-07 **electronic e-voting concern fear threat California Americans with Disabilities**

NewsScan

E-VOTING CONCERNS

California's Secretary of State has won a victory in federal court and new agreements from counties with touch-screen machines to make extra security arrangements. U.S. District Judge Florence-Marie Cooper denied requests by disability rights activists and four California counties to
overturn the Secretary's conditional April 30 ban on touch screens for the November election. In the suit, disability groups argued that banning electronic voting will deny hundreds of thousands of people the right to vote in private, but the judge ruled the Americans With Disabilities Act requires only that disabled voters be given the opportunity to vote. (Bloomberg News/San Jose Mercury News 7 Jul 2004)

Category 29.4 *Online & electronic voting*

2004-07-12 **Diebold electronic e-voting systems manufacturer whistleblower lawsuit fraud California**

NewsScan

"WHISTLEBLOWER" LAWSSUIT FILED AGAINST DIEBOLD

Opponents of electronic voting are suing Diebold Inc. under a California whistleblower law, accusing Diebold of defrauding the state by providing shoddy balloting equipment that exposed California elections to vandals and to software bugs. The individuals who filed the suit are Jim
March, a programmer, and Bev Harris, an activist. Under the whistleblower statute, the two could collect up to 30% of any reimbursement. March says: "This is about money now -- a case of the capitalist system at work. The laws on voting products and processes are unfortunately unclear. But the law on defrauding the government is really, really clear. Going after the money trail is cleaner than going after proper procedures." But some critics of Diebold are equally critical of March and Harris. One of them says, "I would like to see people support a real solution rather than just try to cash in. There are a lot of people who could be a tremendous asset, but they're grandstanding and reveling in the expose." (San Jose Mercury News 12 Jul 2004)

Category 29.4 *Online & electronic voting*

2004-07-19 **Ohio voting machine electronic Diebold security problem**

NewsScan

OHIO QUESTIONS VOTING MACHINE USE

Ohio Secretary of State Kenneth Blackwell has blocked three counties in that state from using Diebold electronic voting machines in November because the systems have shown security problems. Some of the state's 88 counties already were using electronic voting machines, and the decision does not affect them. A Diebold executive says, "We are anxious to learn the areas where the consultant believes additional work is needed." (AP/San Jose Mercury News 19 Jul 2004)

Category 29.4 *Online & electronic voting*

2004-08-05 **Hack the Vote challenge Defcon 12 Rebecca Mercuri abandon e-voting systems 2004 elections**

DHS IAIP Daily; http://www.pcworld.com/news/article/0,aid,117261,00.asp

August 05, PC World — Can you hack the vote?

E-voting technology expert Rebecca Mercuri, a Harvard research fellow, has issued a "Hack the Vote" challenge, trying to illustrate what she calls their unreliability and vulnerability. She unveiled the so-called Mercuri Challenge at the recent Black Hat Briefings and Defcon 12 security conferences. Mercuri suggests electronic voting machines be hacked during their preelection testing, so officials will abandon them before an actual election. As part of her challenge, Mercuri is calling on e-voting system vendors VoteHere and Advanced Voting Solutions to supply any challengers "full specifications" of their voting system for review. The first person to undetectably change vote tallies can claim $10,000 from a separate challenge. Tom Mereckis, head of marketing for VoteHere, says VoteHere makes full specifications of its voting systems available to anyone. Conversely, the president of Advanced Voting Solutions says he has no intention of ever releasing the proprietary workings of its voting systems.

Category 29.4 *Online & electronic voting*

2004-08-05 **electronic e-voting system touchscreen South Carolina election attorney general**

NewsScan

APPROVAL FOR TOUCHSCREEN VOTING SYSTEM

Ruling that the state's new touch-screen voting machines meet federal requirements, the South Carolina attorney general has rejected a request from the South Carolina Progressive Network (SCPN) to stop the State Election Commission from buying the machines. The SCPN's objections to the machines are that they do not provide proof on paper that the vote was cast the way the voter intended, but the attorney general ruled that the state's new machines give voters a chance to review and make changes to the ballots before finalizing their votes. (AP/USA Today 5 Aug 2004)

Category 29.4 *Online & electronic voting*

2004-08-06 **electronic e-voting Defcon 12 security experts skeptical**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/story/0,10801,95094,00.html

August 06, Computerworld — Public, security experts' e-voting views differ sharply.

Security experts are substantially more skeptical about e-voting than the public, but their greatest worry is system and programming errors, not malicious hacker attacks, according to a survey released last week by the Ponemon Institute. The study, conducted in July and early August, aimed to measure public opinion about electronic voting systems and then compare the results with those of security experts--both IT pros and hackers. The Tucson, AZ-based institute collected 2,933 usable responses nationwide from the public, both online and by postal mail, and surveyed 100 attendees at the Black Hat and Defcon hacking/security conferences. Six out of 10 Black Hat/Defcon attendees had an unfavorable view of e-voting, while only 17% of the public did. Twenty percent of the experts cited system and programming errors as their top concern, followed by attempts to influence the outcome of an election. A potential breach of security by hackers and cybercriminals ranked third as a potential e-voting worry among the Black Hat/Defcon attendees. Among the public, the top worry was a decline in voter turnout because of fear or distrust of e-voting systems, followed by human errors and privacy violations.

Category 29.4 *Online & electronic voting*

2004-08-10 **electronic e-voting petition Maryland Diebold security question**

DHS IAIP Daily; http://www.computerworld.com/governmenttopics/government/policy/story/0,10801,95162,00.html

August 10, IDG News Service — Maryland voters file petition against e-voting system.

Eight Maryland voters have asked an appeals court to force the Maryland State Board of Elections (SBE) to address alleged security risks in a Diebold electronic voting machine system and provide a voter-verified paper trail during elections. The plaintiffs, some representing advocacy group TrueVoteMD.org, accuse the SBE of ignoring scientific and government studies that question the security of the Diebold e-voting machines and of ignoring a Maryland legislative requirement to include a voter-verified paper trail with an e-voting system. Such a paper trail would allow voters to check their electronic votes against paper printouts, which can then be used to audit the election results, said Linda Schade, director and cofounder of TrueVoteMD.org.

Category 29.4 *Online & electronic voting*

2004-08-17 **voting data database Australia safe integrity authenticity possession privacy voter information**

NewsScan

VOTER DATA 'SALE' IN AUSTRALIA

The Australian Electoral Commission will investigate whether the Liberal Party has on-sold to its federal and state candidates political databases containing private information about voters, in breach of federal electoral laws. Former ministerial staffers have told The Australian the Liberal Party secretariat has offered discounts to ensure candidates buy the Feedback database, which contains personal information about their constituents based on Australian Electoral Roll electronic data. AEC spokesman Brien Hallett said the law prohibited the use of protected electoral roll data being used for "commercial purposes," but that definition would need to be tested by a court. (The Australian 17 Aug 2004) Rec'd from John Lamp, Deakin U.

Category 29.4 *Online & electronic voting*

2004-08-23 **electronic e-voting machine certification criticism testers hardware software Federal Election Commission**

DHS IAIP Daily;
http://www.cnn.com/2004/TECH/biztech/08/23/evoting.labs.ap/index.html

August 23, Associated Press — E-vote machine certification criticized.

Although up to 50 million Americans are expected to vote on touchscreen voting machines on November 2, federal regulators have virtually no oversight over testing of the technology and critics allege that the three companies that certify the nation's voting technologies operate in secrecy, and refuse to discuss flaws in the ATM-like machines. Federal regulations specify that every voting system used must be validated by a tester. Yet it has taken more than a year to gain approval for some election software and hardware, leading some states to either do their own testing or order uncertified equipment. The election directors' voting systems board chairman, former New York State elections director Thomas Wilkey, said the testers' secrecy stems from the Federal Election Commission's refusal to take the lead in choosing them and the government's unwillingness to pay for it, leaving election officials no choice but to find technology companies willing to pay. A 2002 law, the Help America Vote Act, created a four-member, bipartisan committee, headed by U.S. Election Assistance Commission chairman DeForest Soaries Jr., to oversee a change to easier and more secure voting. Soaries said there should be more testers but the three firms, CIBER and Wyle Laboratories in Huntsville, AL, and SysTest Labs in Denver, CO, are "doing a fine job with what they have to work with."

Category 29.4 *Online & electronic voting*

2004-08-25 **California electronic e-voting approval**

DHS IAIP Daily; http://www.theregister.co.uk/2004/08/25/evoting_california/

August 25, The Register — California approves e-voting.

California will allow voting at electronic voting machines in November in 11 of the state's counties. Kevin Shelley, California's secretary of state, said that the counties had improved the security of their voting machines so that they now comply with all conditions required for state certification. Four counties that remain unapproved are those using the Diebold AcuVote-TSx Voting System voting machines. Shelley decertified the machines in April after problems with the March elections. California has invested more than $139 million on electronic touch screen technology, and during the March presidential primary vote 42 percent of the state's voters could have had access to 42,714 electronic voting machines.

Category 29.4 *Online & electronic voting*

2004-08-30 **Missouri electronic e-mail voting security concern military overseas ballots**

DHS IAIP Daily;
http://story.news.yahoo.com/news?tmpl=story&ncid=1212&e=4&u=
/ap/20040828/ap_on_hi_te/voting_by_e_mail&sid=95573501

August 30, Associated Press — E-mail voting prompts security concerns.

Missouri will allow members of the military stationed overseas to return absentee ballots via e-mail, raising concerns from Internet security experts about fraud and ballot secrecy. State and federal officials insist safeguards, such as signature verification and tracking numbers, are in place to protect the ballots from tampering, duplication or other forms of fraud. However, some critics warn that e-mail is fundamentally insecure. "E-mail is subject to all kinds of tampering," said Bruce Schneier, co-founder of Mountain View, CA-based Counterpane Internet Security Inc. Missouri appears to be the first state using the e-mail option, but other states also could adopt it. About half of states permit electronic transmission of voted ballots, generally by fax, and could follow Missouri's lead, according to the Pentagon's Federal Voting Assistance Program. Ballot secrecy is not available with e-mail and sending such a message is akin to sending a postcard, with its content easily viewable in transit using widely available software. Military personnel are told upfront that their e-mailed ballots won't be secret and that they can mail them in instead. Because of security concerns, the Pentagon earlier this year canceled an Internet voting plan that would have allowed as many as 100,000 military and overseas citizens from seven states to cast votes in November through a Web browser.

Category 29.4 *Online & electronic voting*

2004-09-01 **touch-screen electronic e-voting judge ruling Circuit Court Maryland OK**

NewsScan

MARYLAND JUDGE OKAYS TOUCH-SCREEN VOTING

Rejecting a challenge to the state's touch-screen voting machines, a Circuit Court judge in Maryland suggests that the machines are more accurate than the paper ballots the plaintiffs are seeking to make optional for the November elections, and notes that election officials have "taken all
reasonable steps to protect the integrity of the voting process." The lead plaintiff's response is: "I am very disappointed that Maryland voters will be forced to vote on machines that we believe are illegal under Maryland law and that are clearly very insecure." In his ruling the judge wrote: "No
system is infallible. No machine is infallible. All experts agree systems such as these are much more secure and less vulnerable than the paper ballot" -- or the optical scan machines used in most Maryland jurisdictions in the last presidential election. (Washington Post 1 Sep 2004)

Category 29.4 *Online & electronic voting*

2004-09-07 **electronic e-voting paper trail audit Nevada elections 2004 example US states legislation**

DHS IAIP Daily; http://securityfocus.com/news/9461

September 07, The Associated Press — Nevadans to become first to use touch-screen voting that produces a paper trail.

In what could become a model for other states, Nevada voters on Tuesday, September 7, became the first in the nation to cast ballots in a statewide election on computers that printed paper records of electronic ballots. Nevada's $9.3 million voting system includes more than 2,600 computers and printers deployed in every county. California, Washington and Illinois recently passed laws requiring a paper trail for electronic ballots, and at least 20 others are considering similar legislation. The system aims to address concerns that paperless touchscreen votes cannot be properly audited or recounted. As many as 50 million Americans will cast ballots in the November presidential election on electronic machines that do not produce a paper receipt of the vote.

Category 29.4 *Online & electronic voting*

2004-09-08 **electronic e-voting Nevada security audit concern Sequoia touchscreen**

NewsScan

E-VOTING IN NEVADA

Nevada voters have become the first in the nation to cast ballots in a statewide election using computers that produced printed paper records of electronic ballots. "Knock on wood, so far things have been working flawlessly," said Secretary of State Dean Heller. Nevada's $9.3 million voting system includes more than 2,600 computers and printers deployed in every county. The system, developed by California-based Sequoia Voting Systems, aims to address concerns that paperless touchscreen votes cannot be properly audited or recounted. "From what I've seen, voters seem to enjoy the experience," says DeForest B. Soaries Jr., chairman of the U.S. Election Assistance Commission. "There hasn't been frustration or confusion."(AP/USA Today 8 Sep 2004)

Category 29.4 *Online & electronic voting*

2004-09-13 **electronic e-voting Nevada primary California observe accurate recording**

NewsScan

E-VOTING IN NEVADA

Nevada $9.3 million voting system worked well in last week's primary. California official Marc Carrel, who observed the election, says, "They were incredibly organized. I think California could pull off a similar election if we had adequate training and education programs for poll workers and
voters." Printers attached to the systems offer assurances that elections can be fully audited, and a spokesman for Sen. Dianne Feinstein says, "The Nevada election demonstrates that you can have efficient electronic voting machines yet at the same time have a paper trail so voters can be assured
they've voted accurately and their vote is being recorded accurately." But Georgia elections director Kathy Rogers warns that the printers could have unintended consequences, allowing unethical poll workers to determine how individuals voted: "We seem to have traded a secret ballot for this piece of
paper." (AP/USA Today 13 Sep 2004)

Category 29.4 *Online & electronic voting*

2004-10-18 **survey online ratings reliability trustworthiness accuracy authenticity**

NewsScan; http://www.pewinternet.org/

ONLINE RATING RANKS HIGH WITH ONE IN FOUR INTERNET USERS

Twenty-six percent of adult Internet users in the U.S. have participated in "reputation systems" -- those online rating systems used by Amazon, eBay and others to assist other users in deciding whether a product or service is trustworthy, worthwhile or enjoyable. Men are slightly more likely to offer their opinions than women (29% vs. 22%) and Generation Yers are more likely than Baby Boomers to have posted a rating (30% vs. 23%). In addition, those from wealthier households (income above $75,000) are more likely to participate in rating than those who live in households with an income below $30,000. The findings provide evidence that the trend toward using the Internet for two-way communication among online communities is increasing. "Internet users see these systems as a way to help them figure out what information and people they can trust online," says Paul Hitlin, a research associate at the Pew Internet Project, which conducted the study. "People also see the Internet as a place where they can voice their own opinions. Online they can recommend a CD, warn about a dishonest salesperson, or even defend their high school history teacher."

Category 29.4 *Online & electronic voting*

2004-10-27 **e-voting Diebold Election Systems Software Hart InterCivic Sequoia proprietary source code audit reliability trustworthiness quality assurance open-soure**

NewsScan; http://apnews.excite.com/article/20041027/D85VOSTG1.html

E-VOTING COMPANIES DIVULGE *SOME* SOFTWARE CODE

Electronic voting equipment makers Diebold Election Systems, Election Systems & Software, Hart InterCivic and Sequoia Voting Systems have agreed to submit millions of lines of software code to the National Software Reference Library, but have refused to include their most valuable data -- their proprietary source code. They also say they might not provide the library with copies of software patches and updates. The companies acted at the request of the U.S. Election Assistance Commission, whose chairman noted that although the data submitted was far from complete, he hoped the companies' ongoing submissions would eventually result in making election software more transparent. A number of scientists have called for "open source" voting software that could be independently verified, but many computer security experts remain pessimistic because no technology exists today that would allow an election official who suspects fraud to check software code on a voting machine and compare with the code stored in the library. Avi Rubin, technical director of the Johns Hopkins Information Security Institute, called the code-sharing program "meaningless." (AP 27 Oct 2004)

Category 29.4 *Online & electronic voting*

2004-11-03 **touchscreen e-voting Sequoia Voting Systems glitches problems bugs failures flaws problems denial-of-service DoS availability**

NewsScan;
http://www.cnn.com/2004/TECH/11/03/electronic.voting.ap/index.html

TOUCHSCREEN VOTING SPAWNS GLITCHES

U.S. voters across the country reported some 1,100 problems with e-voting machines, bearing out scientists' concerns that touchscreen machines are prone to tampering and unreliable unless they're equipped to print out paper records for recounts. Some problems were blamed on factors as mundane as power outages and incompetent poll workers, but there were a number of voters in six states -- especially Democrats in Florida -- who said that although they voted for John Kerry, when the computer asked them to verify their choice, it indicated that they had voted for President Bush. One voter in Clearwater reported that it took her about 10 tries and a quick touchscreen clean-up with a wet-wipe towel before she could successfully select Kerry. A spokesperson for Sequoia Voting Systems said the machines' monitors may need to be recalibrated periodically to ensure the touchscreen is sensitive enough to record users' votes. (AP/CNN.com 3 Nov 2004)

Category 29.4 *Online & electronic voting*

2005-07-13 **electronic voting machines optical scanners vote tampering vulnerabilities hack Diebold report analysis flaws**

RISKS; http://www.blackboxvoting.org/BBVreport.pdf 23 94

DIEBOLD OPTICAL SCAN VOTING MACHINE SUSCEPTIBLE TO TAMPERING

Bruce O'Dell provided an extensive summary of a thorough analysis of the Diebold Optical Scan systems used to tally 25M votes in the 2004 elections in the US. Here are excerpts.

>Harri Hursti, an independent security consultant - with the consent of election officials in Leon County, Florida - was able to take full control of the Diebold optical scan device and manipulate vote totals and audit reports at will.

The Diebold Precinct-Based Optical Scan 1.94w device accommodates a removable memory card. It had been believed that this card contained only the electronic "ballot box", the ballot design and the race definitions; astonishingly enough, the memory card also contains executable code essential to the operation of the optical scan system. The presence of executable code on the memory card is not mentioned in the official product documentation. This architecture permits multiple methods for unauthorized code to be downloaded to the memory cards, and is wide open to exploitation by malicious insiders.

The individual cards are programmed by the Diebold GEMS central tabulator device via a RS-232 serial port connection or via modem over the public phone network. There are no checksum mechanisms to detect or prevent tampering with the executable code, and worse yet, there are credible exploits which could compromise both the checksum and executable. The report notes that this appears to be in violation of Chapter 5 of the 1990 Federal Election Commission Standards for election equipment, and therefore should never have been certified for use.

The executable code is written in a proprietary language, Accu-Basic. Accu-Basic programs are first compiled into ASCII pseudocode, which is then executed by an interpreter residing in the optical scan device. Hursti located an inexpensive device capable of reading and updating the memory cards advertised on the Internet, and using a publicly-available version of the Accu-Basic compiler (found on the Internet, along with Diebold source code and other documents, by Bev Harris in 2003) was able to exploit these vulnerabilities - and publicly demonstrated the ability to modify vote totals and audit reports at will.

According to the report:

"Exploits available with this design include, but are not limited to:

"1) Paper trail falsification - Ability to modify the election results reports so that they do not match the actual vote data

"1.1) Production of false optical scan reports to facilitate checks and balances (matching the optical scan report to the central tabulator report), in order to conceal attacks like redistribution of the votes or Trojan horse scripts such as those designed by Dr. Herbert Thompson.(19)

"1.2) An ingenious exploit presents itself, for a single memory card to mimic votes from many precincts at once while transmitting votes to the central tabulator. The paper trail falsification methods in this report will hide evidence of out-of-place information from the optical scan report if that attack is used.

"2) Removal of information about pre-loaded votes

"2.1) Ability to hide pre-loaded votes

"2.2) Ability to hide a pre-arranged integer overflow

"3) Ability to program conditional behavior based on time/date, number of votes counted, and many other hidden triggers.<

After discussion of the demonstration that all of these vulnerabilities can be exploited, Mr O'Dell added, "The affected Diebold optical scan equipment should be immediately withdrawn from use in any election until independent recertification is achieved, or a secure alternative is obtained. All other election equipment - manufactured by Diebold or by other vendors - should be examined, and if subject to the same vulnerability, should also be withdrawn. An investigation to determine how equipment with such serious vulnerabilities to insider manipulation could ever have been certified should also be launched, and certification and oversight procedures enhanced."

He ended his report with these words: "Good people died to gain and defend our right to vote. Election administration must not be exempt from industry best practices for security, audit and control."

Category 29.4 *Online & electronic voting*

2005-08-17 **electronic e-voting study grant NSF higher education colleges ACCURATE produce technical standards secure voting systems**

EDUPAGE; http://washingtontimes.com/upi/20050817-124413-4457r.htm

NSF GRANT FUNDS STUDY OF ELECTRONIC VOTING

A team of researchers will use a five-year, $7.5 million grant from the National Science Foundation (NSF) to study electronic voting. The grant will support a research center called ACCURATE, A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections. Based at Johns Hopkins University, the center includes researchers from the University of California, Berkeley; Stanford University; Rice University; the University of Iowa; and California-based research firm SRI International. According to Dan Wallach, associate professor of computer science at Rice, "The basic question is, 'How can we employ computer systems as trustworthy election systems when we know computers are not totally reliable, totally secure, or bug-free?'" The ACCURATE project is expected to produce technical standards for electronic voting and to develop secure voting systems that are easy to use. Washington Times, 17 August 2005

Category 29.4 *Online & electronic voting*

2005-09-13 **electronic voting vulnerabilities design government research agency report**

RISKS 24 04

NRC REPORT ON ELECTRONIC VOTING

Election officials across the United States are increasingly looking to electronic voting systems as a way to administer elections more efficiently, but skeptics have raised concerns about the security and reliability of these systems. ASKING THE RIGHT QUESTIONS ABOUT ELECTRONIC VOTING, new from the National Academies' National Research Council, offers a set of questions that policy-makers and the public should ask to help ensure that the technologies implemented are secure, reliable, efficient, and easy to use. Advance copies are now available to reporters. The report, which was chaired by DICK THORNBURGH, former governor of Pennsylvania, and RICHARD F. CELESTE, former governor of Ohio, was released on September 13, 2005, and is available free in PDF form at the web site below.

Press release at
http://www4.nationalacademies.org/news.nsf/isbn/0309100240?OpenDocument

Full report at
http://www.nap.edu/catalog/11449.html (sign-in required for the PDF version).

[Contributed by Herb Lin]

Category 29.4 *Online & electronic voting*

2005-10-03 **electronic voting machines flaws weakness errors fraud disenfranchisement hacking data corruption integrity Diebold**

RISKS; http://josephhall.org/nqb2/index.php/2005/10/03/desi_nc 24 06

NORTH CAROLINA DOCUMENTS REVEAL DIEBOLD VOTING MACHINE VULNERABILITIES

1. In one city, Dallas, NC, a bug appears to have prevented the downloading of 11,945 votes which wasn't caught for seven days. At which point, it appears the county compared paper print-outs from the precinct with the totals reported by the tabulation server. A DESI technician reproduced the bug twice and then decided to forgo usual DESI protocol and loaded the flash-based memory packs directly into the central (GEMS) server to retrieve the votes from the memory pack.

2. In another case, another memory pack "failed to download" and the DESI technician got approval to send a back-up file electronically to DESI technicians who then e-mailed the results back. After writing this data to a memory pack, the on-site technician loaded them into the central server via a tabulator unit.

3. Finally, the document describes hand-entering of "three to five" ballots. DESI claims as a "check and balance" this process doesn't allow the technician to enter more votes than the total vote count (that is, the number of valid plus spoiled ballots). This would implicate that one would be prevented from entering more than a certain number of votes, but, of course, does nothing to constrain what votes are entered. A human looking over the technician's shoulder is the only other constraint.

[Summary by Joseph Lorenzo Hall]

Category 29.4 Online & electronic voting

2005-11-15 **electronic voting glitches errors flaws fraud problems data integrity audit trails**

RISKS; http://josephhall.org/nqb2/index.php/2005/11/11/2005_glitches 24 10

VOTING GLITCHES FROM THE 7 NOV 2005 ELECTION

Joseph Lorenzo Hall provided an extensive list of voting glitches on his Web site. He provided excerpts on RISKS:

* San Joaquin County, California - S.J. County has election night déjà vu

San Joaquin County workers misplaced a memory cartridge for an optical-scan machine. They rescanned the ballots and but haven't found the cartridge. In this story, an official says that the new Diebold TSx DREs that they want to use will make things work more smoothly… although the official doesn't recognize that misplacing the memory cartridge in a paperless DRE would not be as easily recoverable (although I believe you'd still have the ballot images resident in memory, no?).

* Cumberland County, Pennsylvania - Software error forces recount in close race for district judge

Two candidates in a race were both mistakenly listed as being from same party. Straight-ticket votes counted both candidates and initially resulted in over-votes. After this was corrected for, the race was down to a 2-vote margin (1703 to 1701 votes).

* Harwinton, Connecticut - Voting machine snafu may lead to challenge in Harwinton

One candidate was endorsed in a race by both Republican and Democratic parties and was listed twice in a choose 2 out of 3 race. This candidate, due to being listed twice, got twice as many votes as the other two candidates in the same contest.

* Pasquotank Co., North Carolina - In Elizabeth City, a 14-vote gap has one candidate calling for a recount

Selecting a certain candidate in the only contest on the ballot resulted in a write-in candidate box being selected instead. The margin in this race was 14 votes. Also, 60 blank ballots were cast (recall that there was only one race for this election).

* Lucas Co., Ohio - State plans to investigate voting chaos; Tuesday's problems are latest for Lucas County

This one is mysterious: "workers accidentally 'set an option [on the five machines] that prevented the results from being transported onto the memory card.'" Also, massive labor shortage resulted in chaos as election was highly understaffed and a system of "rovers" didn't function correctly (where one elections worker would travel to five polling places to get aggregate totals from machines).

* Montgomery County, Ohio - Vote count goes all night

Various problems resulted in having to download votes from 2000 memory cards instead of from one card each from the 548 precincts. However, during this process, 186 memory cards were found to be missing. After looking through bags of precinct materials ("I voted" stickers, signs, etc.) they had found 171 cards. The remaining 15 cards were only found after rousing pollworkers from bed at 3 am so they could return to the polling place to get the cards either left in machines or lying around the polling place.

* Wichita County, Texas - Human errors hamper voting

35 precincts neglect to perform zeroing out process before election. This resulted in the vote data being impossible to download from the DRE (ES&S) with PEB device. ES&S technicians were able to open the machines, remove the removable memory cards and read the data from there.

* Montgomery County, Ohio - 'Human error' creates doubt about failed vote in Carlisle

77 "phantom votes" found to have been cast in an election where a bond measure was defeated by a margin of 146 to 79. ("Phantom votes" are when there are more votes counted than there are registered voters that could have cast votes) In this case, there were only 148 registered voters that could have cast votes in this race.

[Lightly edited by MK. Each item in the original has a reference to a specific URL]

Category 29.4 *Online & electronic voting*

2005-12-09 **electronic e-voting certification lawsuit EFF North Carolina**

RISKS; http://www.siliconvalley.com/mld/siliconvalley/13361799.htm 24 12

EFF E-VOTING CERTIFICATION LAWSUIT

Peter Ludemann reports that the North Carolina is being sued by the Electronic Frontier Foundation (EFF) for improper certification of voting machines:

>North Carolina law requires the Board of Elections to rigorously review all voting system code "prior to certification." But last week the state's Board of Elections certified voting systems from Diebold Election Systems, Sequoia Voting Systems, and Election Systems and Software without bothering to do so…. "This is about the rule of law," said EFF Staff Attorney Matt Zimmerman. "The Board of Elections has simply ignored its mandatory obligations under North Carolina election law. This statute was enacted to require election officials to investigate the quality and security of voting systems before approval, and only approve those that are safe and secure. By certifying without a full review of all relevant code, the Board of Elections has now opened the door for North Carolina counties to purchase untested and potentially insecure voting equipment." Keith Long, a North Carolina voting systems manager, defended the state's decision, telling News.com that reports from "independent testing authorities" were sufficient for certification. But that comes as poor reassurance. Because if the "independent testing authorities" to which Mr. Long refers are as impartial as he is, North Carolina is in big trouble. Long, you see, worked for Diebold Election Systems as recently as Oct. 1, 2004. And between 1983 and 1992 he worked for Sequoia.<

Mr Ludemann adds cogently, "So by 'independent' you mean 'independent of any public oversight,' right?"

Category 29.4 *Online & electronic voting*

2005-12-16 **Florida lawsuit drunk driving breathalyzer source code disclosure electronic e-voting relation**

RISKS; http://online.wsj.com/article_print/SB113470249958424310.html 24 13

FLORIDA BREATHALYZER SOURCE-CODE DISCLOSURE CASE

Contributor Danny Burstein refers to the following clip from _The Wall Street Journal_:

"A court fight in Florida over the software used in the instruments that detect alcohol in breath could threaten the ability of states and localities to prosecute drunk drivers.

"The battle is over the source code of breath analyzers made by CMI Group, a closely held maker of breath-alcohol instruments. Defense lawyers have challenged the use of the device and asked to see the original source code that serves as its computer brain, saying their clients have the right to examine the machine that brings evidence against them.

"Last February, a state appeals court in Daytona Beach ruled that Florida had to produce 'full information' about the test that establishes the blood-alcohol level of people accused of driving under the influence, or DUI. Otherwise, the court said, the evidence is inadmissible…"

Mr. Burstein exclaims, "Imagine if this logic followed through to the equipment being slid into election vote counting!"

Category 29.4 *Online & electronic voting*

2006-01-19 **optical scanner electronic voting machine memory card tampering testing hacking Digital Millennium Copyright Act DMCA**

http://www.computerworld.com/printthis/2006/0,4814,107881,00.html

E-VOTING SYSTEMS TESTER SEES 'PARTICULARLY BAD' SECURITY ISSUES

Herbert Thompson tested Diebold AccuVote optical scanning equipment used for vote-counting in Leon County, FL. Marc Songini interviewed Dr Thompson for an article in Computerworld and discussed the issues. Dr Thompson and his colleagues were able to alter voting results by tampering with the device's memory card. The results could twist the vote-count to favor a preselected candidate. Diebold officials strongly criticized the test methodology, saying that the memory cards were normally sealed precisely to prevent such tampering and that the tests were equivalent to complaining about poor security by deliberately disabling protection and then complaining about security breaches. They also complained that the tests themselves may have violated the terms of Diebold's licensing agreements and intellectual property rights.

Category 29.4 *Online & electronic voting*

2006-03-31 **electronic voting software bug corruption election cancelled voided quality assurance QA**

RISKS; Wisconsin State Journal http://tinyurl.com/napdn 24 23

E-VOTING SOFTWARE GLITCHES RUINS UNIVERSITY ELECTION

Computer problems caused the University of Wisconsin-Madison Student Council to throw out online votes cast this week for campus offices, but retained votes cast for two referendums on the same ballot. The cause of the problem may have been a "little-used, multiple-name tool has worked in prior elections but may have been corrupted by a database upgrade several months ago." The main risk appears to be the lack of testing of the voting system prior to the vote (along with no testing after a major software upgrade).

The parallels with the world of voting machines are obvious: the voting system needs to be tested and certified BEFORE voting occurs.

[Abstract by Dana Freiburger]

29.5 Online legal proceedings

Category 29.5 Online legal proceedings

2002-03-22 **electronic legal notice anonymity e-mail legal judgement online gambling**

NewsScan

COMING TO YOUR IN-BOX: "YOU'VE GOT A SUBPOENA"
A federal appellate court has ruled that a Las Vegas casino suing an unlocatable Internet gambling group can use e-mail to send sufficient notification of the legal action it is taking. Law professor Ann McGinley of UNLV says the decision sets a precedent that will "make it easier for lawyers to find elusive defendants. I think we are moving in the direction of service by e-mail." (AP/San Jose Mercury News 22 Mar 2002)
http://www.siliconvalley.com/mld/siliconvalley/2913542.htm

Category 29.5 Online legal proceedings

2002-09-30 **e-mail legal proceedings traffic tickets court explanations**

NewsScan

E-MAIL IT TO THE JUDGE
County officials in Yakima, Washington, are setting up a program that will enable citizens who've received traffic tickets to e-mail their explanations and excuses to a judge rather than sit in traffic court for hours waiting their turn. Judges will then have a choice of e-mailing their replies or responding via old-fashioned postcard. (AP 29 Sep 2002)
http://apnews.excite.com/article/20020929/D7MBH7NG0.htm

29.6 Flash crowds, social e-links

Category 29.6 *Flash crowds, social e-links*

2003-01-23 **impolitness etiquette wireless e-mail laptop computers audience inattention rudeness**

NewsScan

WIRELESS AND RUDE
The increasing availability of wireless networks is creating new opportunities for rudeness — or, theoretically, politeness. One wireless enthusiast admits, "When I speak to a room of people with laptops, they all have their heads buried in their laptops. Many of them are taking notes of what we're saying, but I think many of them are just trying to catch up with their e-mails." Etiquette expert Sue Fox adds: "If you're doing other work — talking on a phone, working on a computer — I think it's ill manners. It's very rude." (USA Today 23 Jan 2003)

Category 29.6 *Flash crowds, social e-links*

2004-04-20 **critical thinking disintermediation flash crowds psyops information warfare homeland security**

Network World Fusion
http://www.nwfusion.com/newsletters/sec/2004/0419sec1.html &
http://www.nwfusion.com/newsletters/sec/2004/0419sec2.html

Critical Thinking and Disintermediation

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

One of the battlespaces of information warfare is the cognitive domain: knowledge, perception, attitudes and mood. For example, military campaigns have long used propaganda and misinformation to influence both the military decisions of the enemy and to discourage soldiers and civilians. In the Second World War, for example, the Nazis used radio broadcasts into Britain to spread false information about the progress of the war; conversely, the Allies broadcast to the peoples of the Axis powers to blame the governments, but not the population, for the war, thus attempting to drive a wedge between civilians and their regimes. In more recent years, there was a scandal in the USA in October 1986 about a reputed disinformation campaign during the Reagan administration in which government officials were accused of misleading the press to convey false information to Libyan dictator Qaddafi about an imminent attack. And of course currently there's a major division in the USA between those who argue that the administration deliberately misled the American people into a pre-emptive attack on Iraq versus those who suggest that the decision was based on incorrect information (or, for that matter, was correct despite the failure to find corroborative evidence of weapons of mass destruction).

Prof. Daniel Kuehl, PhD, is the distinguished Professor and Director of the Information Strategies Concentration Program at the Information Resources Management College of National Defense University in Fort McNair, Washington DC. A frequent contributor to scholarly analysis of information warfare, Dr Kuehl was the keynote speaker on Thursday the 11th of March 2004 at the 17th Annual Meeting of the Federal Information Systems Security Educators' Association at the University of Maryland University College. After his lecture, we got into a discussion about the information warfare implications of a couple of trends in modern society: disintermediation and the lack of critical thinking in the population at large.

Disintermediation in general is defined by the Webopedia as "Removing the middleman. The term is a popular buzzword used to describe many Internet -based businesses that use the World Wide Web to sell products directly to customers rather than going through traditional retail channels. By eliminating the middlemen, companies can sell their products cheaper and faster. Many people believe that the Internet will revolutionize the way products are bought and sold, and disintermediation is the driving force behind this revolution."

Disintermediation in the distribution of news is the phenomenon of reducing gate-keepers in the flow of information from provider to user. For example, Matt Drudge is free to spread unsubstantiated rumors to a huge audience without having to bother with the fact-checking that is customary in responsible news media such as reputable newspapers or magazines and some television or radio programs.

Critical thinking is the ability to analyze information skeptically rather than gullibly. For example, people who open unexpected attachments in e-mail from friends are failing to distinguish among different targets of trust:

* Trust in the authenticity of the FROM line of an e-mail message (which may not, in fact, correctly identify the source);

* Trust in the technical competence of the sender to evaluate the quality of the attachment (which may not, in fact, correlate with how loveable and friendly Aunt Gladys is);

* Trust in the authenticity of the labeling of the attachment (which may not, in fact, really be a document at all but may be an executable);

* Trust in the description and safety of an attachment (which may not, in fact, be a screen saver with frogs).

Now couple disintermediation with a lack of critical thinking. Consider the likely effects of a concerted campaign to, say, spread a number of rumors about major publicly-traded companies. We know that pump 'n' dump schemes have successfully manipulated stock values to the benefit of criminals; why not expect terrorists to apply the same techniques to manipulating the entire stock market? If people are willing to believe and act upon stock tips e-mailed to them by total strangers using spam (even though tiny print clearly states that the junk mailer has been paid to distribute the information), why wouldn't uncritical thinkers cheerfully act on "advice" spread by enemies of the nation?

Similarly, the phenomenon of flash crowds worries me: training people to assemble on command in large numbers at, say, shoe stores, piano showrooms or restaurants for no good reason other than the fun of being part of a huge crowd is a perfect setup

for creating an army of willing, mindless drones who will congregate on command at the site of a terrorist attack or at places where their presence will interfere with response to criminal or terrorist activities. Want to rob a bank in peace and quiet? Set up a conflict between two instant crowds to draw the police to an instant riot.

I think that all of us in the IT, network and security fields are used to critical thinking. We have to be to keep up with the flood of technical information and distinguish marketing exaggerations from realistic information. We are used to writing and reading product comparisons, strategy evaluations and management recommendations as part of our work. Let's use our skills to foster critical thinking throughout the educational system. Let's work as volunteers on school boards, in the classroom and in social organizations to introduce critical thinking to children and adults who haven't learned how to distinguish reality from propaganda. Push for curriculum changes to accompany lessons on how to use the Internet with lessons on how to weigh the information found through e-mail and on the Web.

Let's make sure that we're not patsies for an information warfare attack rooted in disintermediated propaganda.

* * *

For further reading

Agre, P. (1998). Phil Agre talks more about disintermediation.
< http://www.xent.com/FoRK-archive/august98/0321.html >

Webopedia (2004). Disintermediation.
< http://www.webopedia.com/TERM/D/disintermediation.html >
Bosworth, S. (2002). Information Warfare. Chapter 7 from _Computer Security Handbook, 4th Edition_, Bosworth, S. & M. E. Kabay, eds. Wiley (New York). ISBN 0-471-41258-9. xxiv + 1184. Index.

Campen, A. D., D. H. Dearth, & R. T. Goodden, eds. (1996). _Cyberwar: Security, Strategy, and Conflict in the Information Age_. AFCEA International Press (Fairfax, VA). ISBN 0-916-15926-4. vii + 296.

Gordon, S., R. Ford & J. Wells (1997). Hoaxes & hypes. Presented at the 7th International Virus Bulletin Conference.
http://www.research.ibm.com/antivirus/SciPapers/Gordon/HH.html

Henry, R. & C. E. Peartree (1998), eds. _The Information Revolution and International Security_. Center for Strategic and International Studies (Washington, DC). ISBN 0-892-06299-1. xx + 194. Index.

Kabay, M. E. (1995). Information Warfare.
< http://www2.norwich.edu/mkabay/overviews/infowar_1995.htm > or
< http://www2.norwich.edu/mkabay/overviews/infowar_1995.pdf >

Kabay, M. E. (2003). Cyber-Safety for Everyone: from Kids to Elders, Second Edition. Accura Printing (Barre, VT). ISBN TBD. vi + 124. In press. Also available free from http://www2.norwich.edu/mkabay/cyberwatch/cybersafety.pdf

Kuehl, D. (2000). Statement to the Joint Economic Committee of the Senate of the United States.
< http://www.cdt.org/security/dos/000223senate/kuehl.html >

Kuehl, D. (2004). Information Warfare: What it Is, Isn't and How It Shapes National Security. Slide show from January 23, 2004 presentation at New York Military Affairs Symposium.
< http://libraryautomation.com/nymas/infowarfare2004.htm >

Lesser, I. O., B. Hoffman, U. Arquilla, D. Ronfeldt & M. Zanini (1999). _Countering the New Terrorism_. RAND Corporation Report
< http://www.rand.org/publications/MR/MR989/ >
Also available as a printed document, ISBN 0-833-02667-4 through online purchase.

Schwartau, W. (1996). _Information Warfare, Second Edition_. Thunder's Mouth Press (New York). ISBN 1-560-25132-8. 768. Index.

Category 29.6 *Flash crowds, social e-links*

2004-05-13 **friends social networking cellular mobile phone text message**

http://www.nytimes.com/2004/05/13/technology/circuits/13dodg.html

SOCIAL NETWORKING THROUGH CELL-PHONE TEXT-MESSAGING

Users of cell-phone based text-messaging services for social connections such as Dodgeball.com find it convenient to meet people who are friends of their friends. Some 5,000 people signed up in New York City, Boston, Philadelphia, San Francisco and Los Angeles within about a month from its introduction.

[MK notes: This system, were it to be hacked, could be misused to trick people into becoming victims of Bad People — thieves, stalkers, rapists and so on. I hope we will be hearing more about security measures to prevent damage to the databases on which the affinity relations are based.]

Category 29.6 *Flash crowds, social e-links*

2004-07-06 **Los Angeles cybercafes close computer crime cybersyndrome**

NewsScan

L.A. TO CLEAN UP CYBERDENS OF INIQUITY

The Los Angeles City Council members have voted unanimously to regulate cyber cafés where teens and others hang out to use computers. The proposal was introduced after a string of shootings at cyber cafés, but council members say it is not their intention to drive the cafés out of business.
One 14-year-old patron says: "Most people can't afford computers that work this good. At least we're being social here instead of staying at home." (Los Angeles Times 6 Jul 2004)

Category 29.6 *Flash crowds, social e-links*

2004-07-29 **Wiki wikipedia online encyclopedia information spread source disintermediation**

NewsScan

THE WIKI WAY TO COMMUNICATE

A wiki (the Hawaiian word for 'quick') is a type of Web site that many people can revise, update and append with new information. Whereas blogs are essentially designed for personal expression, wikis are designed for collaboration. The concept was pioneered in the mid-1990s by programmer Ward Cunningham, who called it the WikiWikiWeb and intended it to serve as a platform for freewheeling collaboration in software and engineering projects. Ross Mayfield of the Silicon Valley startup called Socialtext says: "People have tried very hard to take fragmented knowledge within
corporations and put it somewhere that it can be used, but it's been an uphill effort. Our focus is literally to get everyone on the same page." And New York University communications professor Clay Shirky explains that "people are realizing that perhaps the most human value actually occurs in
smaller groups." (Wall Street Journal 29 Jul 2004)

Category 29.6 *Flash crowds, social e-links*

2004-08-17 **California cyber café violence gang gathering activity**

NewsScan

VIOLENCE AT CALIFORNIA'S CYBERCAFES

Episodes of violence at several businesses in southern California have prompted a number of municipal crackdowns -- the latest of which is taking the form of a Los Angeles ordinance requiring that the city's 30 Internet cafes enforce the city's long-standing curfew for minors, pay for in-store
surveillance cameras, enforce limits on how many computers each business can operate, and obey prohibitions against dark window coverings. But Ernest Miller, a spokesman for iGames, which represents about 500 PC gaming parlors in the U.S. and abroad, insists that there's nothing particularly violent about cybercafes: "A haven for gang activity can be any location where people gather -- corner liquor stores, pool halls or cinemas." (AP/San Jose Mercury News 17 Aug 2004)

Category 29.6 *Flash crowds, social e-links*

2004-10-27 **blogs weblogs fasion advertising discussion forms ideas data leakage confidentiality**

NewsScan; http://www.nytimes.com/2004/10/27/business/media/27adco.html

MADISON AVENUE WAKES UP TO WEB LOGS

Advertising agencies and communications professionals are testing the effectiveness of using blogs to create forums for discussion about ideas within their industries, with topics ranging from video game marketing to the art of client service. However, the biggest agencies are still holding out, noting that the potential risks still outweigh the benefits. "Blogs are in fashion, and it is easy to hop on the bandwagon and say that every company should have one," says an executive with Deutsch, a unit of the Interpublic Group of Companies. "The questions any smart marketer should be asking are, 'Does this provide a platform to connect with their most relevant audiences and how will this address business objectives?' That's not to say we would never enter blogland, but there is a fine line between being timely, topical and keeping current while making sure that we are doing what's best for our business long term." The biggest risk, say many experts, is an uncontrolled message slipping out and damaging the company. But it's clear that as blogging evolves into a corporate tool, it's also losing those qualities that made it such a hit in the first place: attitude, irreverence and a penchant for kicking up a ruckus. (New York Times 27 Oct 2004)

Category 29.6 *Flash crowds, social e-links*

2004-11-15 **RFID radio freqency identifier nTAG infrared**

NewsScan;
http://www.boston.com/business/technology/articles/2004/11/15/breaking_the_ice_20/

HELLO, I'M A DOG LOVER, TOO!

Schmoozing at big corporate events can be painful for the socially challenged, but now there's the nTAG -- an electronic name tag that beams messages to fellow conventioneers like, "Hi, Jane, I like strawberry ice cream, too." The device uses infrared sensing and radio frequency identification to communicate with other tags and it lights up in the dark for those who do their networking at the bar. "People want a reason to interact," says nTAG inventor Rick Borovoy. "They need help. This gives them a powerful nudge in that direction." Meeting participants have given the nTAG high marks for being an icebreaker that helps them circulate beyond their usual pool of friends or colleagues, and meeting planners use the data collected to evaluate session popularity and exhibit attendance. (Boston Globe 15 Nov 2004)

29.7 Outsourcing

Category 29.7 *Outsourcing*

2005-06-23 **data theft insider attack employee outsourcing foreign worker call center reporter investigation bank account details identity theft credit card fraud**

RISKS; http://news.bbc.co.uk/1/hi/uk/4121934.stm 23 93

INDIAN CALL-CENTER WORKER SOLD BANK-ACCOUNT DETAILS TO REPORTER

Police are investigating reports an Indian call centre worker sold the bank account details of 1,000 UK customers to an undercover reporter. The information passed on could have been used to clone credit cards.

The Risks?

Obvious really - overseas call centres in poverty stricken third world countries, the staff of whom have unlimited access to personal and private information of the more wealthy, are the worst security risks ever devised by financial organisations.

[The abstract and comments above are reorganized from the original note submitted to RISKS by "SB", who is not otherwise identified.]

Category 29.7 *Outsourcing*

2005-12-05 **Intel Corp investment research development R&D outsourcing India foreign offshore Bangalore**

EDUPAGE; http://news.bbc.co.uk/2/hi/business/4499362.stm

INTEL UPS INVESTMENT IN INDIA

Intel has announced plans to invest $1 billion in India, where it already operates the company's largest nonmanufacturing site outside the United States. That site, in Bangalore, hosts development efforts for software. The new investment, expected over the next five years, will be split between the existing research and development efforts and local firms. Craig Barrett, chairman of Intel, said, "We will grow our local operations, boost venture capital investments, and work closely with the government, industry, and educators." The company said it has not made any decisions about opening manufacturing facilities in India, though such an option remains open. The costs of doing business in countries including India are significantly lower than in the United States. Some estimates put the salary for an Indian software engineer at one-sixth of what a comparably skilled engineer would earn in the United States. BBC, 5 December 2005

Category 29.7 *Outsourcing*

2006-02-23 **report study outsourcing fears exaggerated ACM US computer science academia hurt**

EDUPAGE; http://www.nytimes.com/2006/02/23/technology/23outsource.html 23

REPORT SAYS OUTSOURCING FEARS EXAGGERATED

A new report from the Association for Computing Machinery (ACM) argues that fears of a wholesale migration of high-tech jobs away from the United States are not supported by the data so far. Representing a year's work by a study group, the report predicts continued offshoring of 2 to 3 percent of IT jobs each year for the next decade, but it notes that the number of high-tech jobs continues to grow and already exceeds the number at the height of the dot-com boom. Although the report acknowledges losses to lower-wage markets and notes that the marketplace for technology is tightening, "the notion that information technology jobs are disappearing is just nonsense," according to Moshe Vardi, computer scientist at Rice University and cochair of the study group. David Patterson, president of the ACM and computer science professor at the University of California, Berkeley, said that exaggerated fears of outsourcing have hurt the U.S. market by discouraging college students from pursuing careers in IT, which, in turn, will lead to fewer qualified members of the U.S. IT workforce.

---

31 The state of information security & technology

Category 31 *The state of information security & technology*

1997-02-03 **security business Farmer SATAN survey**

Business Journal web site

Ted Julian of IDC (Framingham, MA), author of a study of firewalls, predicts 300% growth in the number of installed firewalls in 1997 over 1996; he estimates revenues growing from $338M to $600M in the same period. Hewlett-Packard reports significant growth in the amount of security consulting they are called on to do; McAfee's revenues have grown from $9M to $150M in three years.

Category 31 *The state of information security & technology*

1997-02-13 **audit survey fraud**

PA News

The audit Faculty of the Institute of Chartered Accountants of England and Wales, in conjunction with _Accountancy Age_ magazine, reported the results of a survey showing that many professionals expect to see an increase in the rate of corporate fraud. Reasons given by the respondents included reduced staffing and increased performance pressure. People thought that legal protection for whistle-blowers and increased vigilance would help fight fraud. The size of the respondent population was not given in the Press Association report.

Category 31 *The state of information security & technology*

1997-02-20 **credit card fraud**

PA News

Barclays Bank in England warned shoppers to be on guard against credit-card fraud. Although losses have been dropping, theft using cloned (counterfeit) cards are large enough at 23.6M pounds (about U$40M) to warrant investment in smart cards. In the UK alone, said a Barclays' spokesman, over half a million retail points of sale will have to be converted to interact with the microchips on the new credit cards.

Category 31 *The state of information security & technology*

1997-03-09 **statistics crime**

EDUPAGE

The 1997 Computer Security Institute survey of computer crime revealed that 75% of 563 respondents had lost money because of computer crimes in the past year. United Press International reported, "The institute says 26 respondents reported a total of $24.8 million in losses due to telecommunications fraud; 22 reported $21 million in losses from theft of proprietary information; 26, nearly $4.3 million from sabotage of data or networks; 22, nearly $4 million from unauthorized access by insiders; and 22, $2.9 million from system penetration by outsiders. Computer virus infestations caused nearly $12.5 million in losses for 165 respondents. Laptop theft caused $6.1 million in losses for 160 respondents; employee abuse of Internet privileges caused more than $1 million in losses to 55 organizations."

Category 31 *The state of information security & technology*

1997-04-07 **Internet computer network hacker policy**

http://www.cert.org/research/JHThesis/Start.html

John D. Howard published his PhD dissertation at Carnegie Mellon University: An Analysis Of Security Incidents On The Internet 1989 - 1995. He analyzed 4,299 Internet-related security incidents. Highly recommended: read the full document starting at <http://www.cert.org/research/JHThesis/Start.html>.

Category 31 *The state of information security & technology*

1997-06-09 **privacy cookies Web**

AP

The Electronic Privacy Information Center (EPIC) released its survey on Web privacy just before an important US government hearing of the Federal Trade Commission. Their research found widespread use of intrusive technology such as cookies files without requesting permission from their users. David Kalish, writing for AP, stated that "The survey found that of the Internet's 100 most popular Web sites, about half collect personal information from users who click on their sites or through mailing lists and other means. Only 17 sites even mention the privacy issue, and most of those fell far short of what the group considered adequate disclosure — explaining why information is collected, how it will be used, and what steps will be taken to limit improper use."

Category 31 *The state of information security & technology*

1997-06-27 **policy implementation survey**

PR Newswire

A survey of 333 system integrators, value-added resellers, vertical resellers and consultants was conducted during May 1997.by J. River Inc. and revealed that only about half the companies replying had implemented any network security policies despite widespread plans for intranets and Internet communications. In other sections of the research, there were indications that about half the companies involved used only user IDs and passwords for security and that about a third used no security at all.

Category 31 *The state of information security & technology*

1997-06-30 **statistics disasters hard drive failures**

Information Systems Update 97 7

Christopher D. McDonald, editor of the Information Systems Update, wrote: >Stuart Hanley, a data recovery manager with Ontrack Data International, has an article in the June 1997 edition of "Contingency Planning & Management", entitled "Minimize Loss, Maximize Recovery". He presents a pie-chart for 50,000 hard drives and other data storage devices which Ontrack has examined upon failure since 1987. Again here are REAL numbers to consider for contingency planning. Reasons for failure include: 44% hardware or system malfunction; 32% human error; 14% software program malfunction; 7% computer virus; and 3% natural disasters. CP&M is available free to qualified individuals.<

Category 31 *The state of information security & technology*

1997-08-14 **CERT alerts warnings patches vulnerabilities**

COMPUTER WEEKLY

The Computer Emergency Response Team Coordination Center (CERT-CC) issued yet another alert warning administrators that their failure to keep up to date in applying patches for known vulnerabilities increases the risk of hack attack. [Eventually, one hopes, some enraged stockholder will sue the administrators who do not apply patches in time; in justice, the lawsuits should also name upper managers who refuse to allocate sufficient resources to their network and security managers for effective response to CERT alerts.]

Category 31 *The state of information security & technology*

1997-09-05 **hackers defense police policy**

Newsbytes

Japanese police asked computer operators to increase security in an attempt to resist increasing attacks by hackers. Reported hacking increased 25% in the first six months of 1997. Recommendations included better password management, installation of fire walls, and effective encryption.

Category 31 *The state of information security & technology*

1997-11-08 **bank reporting hacking intrusion law**

Privacy Guild

Vin McLellan of the Privacy Guild circulated what appears to be a draft letter from the Federal Reserve Bank to all member banks in the United States warning them that they are obliged under law to report all violations of computer security to the FBI.

Category 31 *The state of information security & technology*

1998-01-04 **hackers statistics Australia**

Australasian Business Intelligence

According to the Australian Computer Emergency Response Team, the number of computer hacker assaults reported in Australia more than doubled in the 12 months to early August, 1997. Most of the increase came from "script weenies", unskilled hackers who use automated hacking programs.

Category 31 *The state of information security & technology*

1998-01-05 **macro virus infection Japan**

Nihon Keizai Shimbun via COMLINE News Service

According to the Japanese Ministry of Posts and Telecommunications, Japan experienced its worst year of virus infections in July 1997, with 353 reported incidents, of which 66% were due to macro viruses.

Category 31 *The state of information security & technology*

1998-02-19 **survey computer crime reporting UK**

EDUPAGE

In the UK, a report from the Audit Commission stated that 45% of its respondents reported "computer misuse" such as fraud or use of pirated software in 1997. The reporting rate rose from 36% in 1994.

Category 31 *The state of information security & technology*

1998-03-23 **criminal hackers motivation profit money studies surveys**

Communications Week

The long-standing belief that internal attacks outweigh external threats in computer security is finally starting to crumble. Tim Wilson reported in Communications Week that "WarRoom Research LLC found that the vast majority of Fortune 1000 companies have experienced a successful break-in by an outsider in the past year. More than half of those companies have experienced more than 30 system penetrations in the past 12 months. Nearly 60 percent said they lost $200,000 or more as a result of each intrusion." In addition, the 1998 Computer Security Institute / FBI survey showed that "520 U.S. companies reported a total loss of $136 million from computer crime and security breaches in 1997-an increase of 36 percent from the year before. The Internet was cited by 54 percent of the respondents as a frequent point of attack — that's about the same percentage of respondents that cited internal systems as a frequent point of attack."

Category 31 *The state of information security & technology*

1998-03-24 **breaches break-ins surveys estimates crime**

EDUPAGE

Studies released by the Computer Security Institute (with support from the FBI) and by War Room Research both indicated that computer intrusions and cybercrime in 1997 were up from 1996 levels — 36% at $135M according to the former report. Losses from individual breakins at Fortune 1000 companies ran around $200,000 per incident in 60% of the cases reported — and more than half of the respondents admitting to 30 or more breaches within a single year.

Category 31 *The state of information security & technology*

1998-06-16 **survey DoE risks vulnerabilities weaknesses management**

RISKS 19 81

The Department of Energy surveyed 64,000 unclassified computer systems and found widespread security vulnerabilities including readable password files, write access through FTP, and the presence of "classified and sensitive nuclear weapons information on 1,400 systems open to anyone on the Internet."

Category 31 *The state of information security & technology*

1998-06-18 **criminal hacker cracker threat overview persecution**

ST. PETERSBURG TIMES (FL)

Robert Trigaux worte an extensive review of cases of harassment by criminal hackers. Quoting security expert Ray Weadcock, he wrote, "With the global boom in the Internet and ever-cheaper personal computers, hacking is spreading like online kudzu. Hacking is getting more sophisticated and, in many cases, a lot nastier. And it's chipping away at the ability of government, the military, and the business community to protect proprietary information and preserve individual privacy."

Category 31 *The state of information security & technology*

1998-06-20 **Japan security vulnerabilities**

RISKS 19 82

Peter Neumann's "Stark Abstracting" is so concise it's usually hard to beat his summaries, as in this succinct report: "A 1996 survey of 2,000 Japanese companies conducted by an institute affiliated with the Ministry of Industrial Trade and Industry revealed that only 17.1 percent had a security manager in charge of preventing unauthorized access to their computer networks; 14.3 percent offered security education; 7 percent used firewalls. More than half of the respondents said they didn't take necessary protective measures because they don't know what to do. "

Category 31 *The state of information security & technology*

1998-07-17 **university academic penetration intrusion crackers costs**

EDUPAGE

Dr Virginia Rezmierski of the University of Michigan published a study of the costs incurred in academia by computer incidents, including deliberate attacks as well as accidental downtime. Costs of recovery averaged around $15,000 for the most part but ranged above $100,000 in some severe disruptions.

Category 31 *The state of information security & technology*

1998-07-23 **survey article overview criminal hacking cracking Internet**

MSNBC

Mike Brunker wrote a good overview of Internet security in July <http://www.msnbc.com/news/177668.asp>.

Category 31 *The state of information security & technology*

1998-09-29 **e-commerce growth exaggerated hyperbole OECD estimates**

EDUPAGE

The OECD criticized projections that paint a picture of a world full of e-cash carrying smart-card users buying products and services online. In fact, the total estimated volume of e-commerce in 1997, $26B, was 0.5% of the total retail sales (not GDP) in the seven largest economies of the planet.

Category 31 *The state of information security & technology*

1998-10-26 **survey e-commerce consumer security policy fraud**

Advertising Age
http://www.adage.com/interactive/articles/19981026/article6.html

Dana Blankenhorn, writing in Advertising Age, reported expert opinions that consumer fears of shopping on the Web were unfounded, but that businesses would have to respond anyway to quell the anxiety. One of the mechanisms available for fraud reduction was pattern matching of electronic transactions to detect misuse. The CyberSource company of San Jose, CA was described as providing such a service for Web-based merchants.

Category 31 *The state of information security & technology*

1998-10-30 **management apathy ignorance bean-counters strategy**

Newsbytes http://cnnfn.com/digitaljam/newsbytes/120619.html

According to The Knowledge Group, a British consultancy, information technology managers largely blame upper management for failing to support efforts at protecting corporate information systems and networks. According to an article by Sylvia Dennis in Newsbytes, "For its survey, TKG asked 250 IT and network managers to list the contributing factors to network attacks via the Internet. While 33 percent included lack of board-level understanding or commitment to network security as a significant factor, 60 percent said that not enough time or money was invested in access control or risk assessment." For details, see <http://www.ktgroup.co.uk>.

Category 31 *The state of information security & technology*

1998-11-10 **survey management security concerns conference**

Business Wire

A self-selected sample of 80 security experts answered a survey at the Bellcore/Global Integrity's SecureComm 98 conference in Washington, DC. The top five infosec concerns for 1999 were as follows:
1. Ability of current security infrastructure to support electronic commerce activities.
2. Implementing remote access without compromising the security of the corporate network.
3. "Insider" attacks against corporate systems.
4. The extension of networks to support business partner connections.
5. Encryption and key management technology for customer interfacing systems.

Category 31 *The state of information security & technology*

1999-01-08 **criminal hacker statistics survey report China international**

Newsbytes

The official Xinhua news agency reported that computer crime has been exploding in the People's Republic of China. The annual growth rate of 30% led to over 100 recorded cases of computer-related crimes in 1998 with estimates of undetected crime running about 6:1, with a projected rates of 600 crimes in 1998 in the PRC. One Chinese estimate guessed that 95% of all PRC Web sites have been penetrated by local and overseas criminal hackers because of the relatively weak level of security in the PRC. A test of Shanghai and Shenzhen networks showed that almost all of them were vulnerable to penetration. Local software companies are beginning to respond to the need for security software, and in late 1998, an anti-virus company announced the release of the first firewall made in the PRC.

Category 31 *The state of information security & technology*

1999-02-18 **computer crime penetration data diddling Japan survey**

OTC

In Japan, the National Police Agency reported in February that computer crime was up 58% in 1998 compared with 1997 — a 1300% growth since the first statistics were kept in 1993. Specific crimes increased even more than the aggregate average; e.g., forgery and data diddling cases grew 67% in 1998. Current Japanese laws do not consider unauthorized penetration of a computer system as a crime; only breaches of data integrity are criminal.

Category 31 *The state of information security & technology*

1999-02-19 **study survey insider crime sabotage industrial espionage computer crime**

National Business Review (NZ)

Allan Watt, director of forensic operations for computer security specialists S P Bates & Associates of New Zealand, said that his studies strongly support the view that 80% of computer crime is perpetrated by insiders. He said that many executives dismiss the consequences of computer crime as malfunctions and warns that it is unwise to allow I.T. staff to investigate suspected crime without supervision by forensic experts outside the department. His research also supports the widespread opinion that 90% of detected computer crime is unreported because of fears of embarrassment.

Category 31 *The state of information security & technology*

1999-02-22 **criminal hacker penetrations attacks China crime intrusion**

Reuters

The Chinese Department of Public Security announced that it had solved 100 cases of criminal hacking in 1998 but estimated that this was only about 15% of the actual level of unauthorized system access. Reported computer crime was growing at an annual rate of 30%, they said. About 95% of all Chinese systems on the Internet had been attacked last year, with many banks and other financial institutions the target of Chinese and international criminals.

Category 31 *The state of information security & technology*

1999-02-23 **survey crime fraud insider criminal hacker infowar espionage**

Australian

The annual Australian Computer Crime and Security Survey, organized by the Victorian Computer Crime Investigation Squad and Deloitte Touche Tohmatsu, reported on computer crimes in 350 of the largest Australian companies. In brief, the salient results were that about one third of the respondents had suffered one or more attacks on their systems in 1998; of those, 80% had experienced insider attacks, 60% experienced outsider attacks; and 15% of the respondents with any attacks claimed they had been the targets of industrial espionage. Almost three-quarters of all the respondents had no formal policy requiring notification of police authorities in case of attack. More than a fifth of all the respondents had experienced a breach of confidentiality and almost a fifth reported a breach of data integrity.

Category 31 *The state of information security & technology*

1999-04-07 **survey study computer crime costs defenses prevention**

Detroit News; http://www.gocsi.com/prelea990301.htm

The Fourth Annual Computer Security Institute / Federal Bureau of Investigation Computer Crime and Security Survey demonstrated yet again that computer crime is a growing problem for US companies, financial institutions and government agencies. Losses amounted to hundreds of millions of dollars, much of it resulting from industrial espionage. Key findings:
* 26 percent reported theft of proprietary information.
* System penetration by outsiders increased for the third year in a row; 30 percent of respondents reported intrusions.
* Those reporting their Internet connection as a frequent point of attack rose from 37 percent of respondents in 1996 to 57 percent in 1999.
* Unauthorized access by insiders rose for the third straight year; 55 percent reported incidents.
* More companies - 32 percent compared with 17 percent in the past three years - are reporting serious cyber crimes to law enforcement.

Category 31 *The state of information security & technology*

1999-04-17 **Internet crime detection enforcement international**

Reuters

Dick Satran summarized the computer crime scene for Reuters in mid-April. Computer crime is growing and international cooperation is insufficient to stop the perpetrators who take advantage of jurisdictional and technical problems on the law enforcement side.

Category 31 *The state of information security & technology*

1999-04-19 **computer crime criminal hacking penetration survey vulnerabilities firewalls**

OTC

M2 Communications reported in April 1999 that, a survey conducted for Infosecurity '99 and _Government Computing_ magazine found serious vulnerabilities among local authorities (municipal governments):
* 33% of local authorities in the UK were at risk of penetration by hackers
* 33% of local authorities lack firewall
* 6% do not have basic anti-virus software installed
* many of the systems with firewalls did not enable them to filter traffic.
A similar survey in 1998 suggested that 3/4 of medium-sized accountancy practices, law firms and PR and advertising agencies had no security measures in place at all.

Category 31 *The state of information security & technology*

1999-04-20 **survey management firewalls network viruses millennium**

InformationWeek UK via CMPWeb

Andrew Darling, writing for InformationWeek in the UK, penned a dismal litany of management failure to integrate security into their business operations. Interviews with many senior I.T. staff showed that the same decades-old pattern of ignoring security in favor of short-term focus on operations and profits makes it impossible for technical staff to do their job adequately.

Category 31 *The state of information security & technology*

1999-04-30 **survey e-mail servers vulnerability patch software**

OTC / PR

NTA Monitor Ltd released a survey of e-mail servers in British government systems showed that almost half had security vulnerabilities that made it possible for breaches of e-mail confidentiality. "The testing analysed the 689 Internet domains within the "gov.uk" name space, which includes central government departments, local government and a number of governmental organisations, and after discounting domains where no Internet email systems had been set-up, or which were not reachable during the tests, the survey reported on 345 live email servers." The analysis took place between November 1998 and April 1999.

Category 31 *The state of information security & technology*

1999-05-03 **criminal hacker damages loss theft controversy restitution**

LA Times
http://www.latimes.com/HOME/BUSINESS/CUTTING/t000039748.1.html

The criminal-hacking magazine, _2600_, published letters from victims of Kevin Mitnick that estimated damages from his depredations. Total estimated costs (dismissed as preposterous by the _2600_ crew) were $292M, of which NEC claimed $1.8M and Nokia reported $135M.

Category 31 *The state of information security & technology*

1999-05-13 **privacy Web policies attestations assertions claims survey**

LA Times

A study by Georgetown University researchers revealed that about 66% of the 7,500 popular Web sites in the review included a privacy policy. Critics claimed that most of these were paying lip-service to privacy; Edupage editors wrote, "The FTC names five ingredients in its definition of a successful all-encompassing privacy policy, but [the] survey showed that just 10 percent of surveyed sites follow all five steps."

Category 31 *The state of information security & technology*

1999-05-21 **criminal hacking penetration vulnerability government report**

Reuters, AP

The General Accounting Office (GAO) of the US reported that some key computer systems at NASA are poorly protected against criminal hackers. "We successfully penetrated several mission-critical systems, including one responsible for calculating detailed positioning data for Earth-orbiting spacecraft and another that processes and distributes the scientific data received from these spacecraft. . . . [W]e could have disrupted NASA's ongoing command and control operations and stolen, modified or destroyed system software and data." Among other findings, the government auditors said that NASA failed to assess risks and evaluate security requirements; 135 of the 155 mission-critical systems reviewed failed the agency's own requirements for risk assessment. NASA provided inadequate computer security training, did not clearly classify information as public or confidential, and was unable to say how mission-critical systems should be protected from known threats from the Internet.

Category 31 *The state of information security & technology*

1999-05-25 **software piracy intellectual property theft copying**

Computer Reseller News Online

The Business Software Alliance and the Software and Information Industry Association announced a slight fall in piracy in 1998, although worldwide rates of unauthorized use remained at 38% (231M of a total of 615M new installations). Vietnam with 97% and China with 95% stolen software led the pack. Total theoretical losses were around $11B worldwide. However, the report also cited evidence that governments were working harder to reduce piracy.

Category 31 *The state of information security & technology*

1999-05-27 **survey study Internet usage children adolescents Web parental supervision involvement**

USA Today Online

A poll of 500 households showed that young people between 8 and 18 received minimal parental supervision in their use of the Internet. Some of the key points:
* 20% of parents did not monitor their children's Internet usage;
* 52% monitored usage only moderately;
* 18% of the children surveyed intended to physically meet someone they met on the Internet;
* 48% of parents allowed unlimited frequency of access to the Net;
* 24% of parents placed no restrictions on the length of time their children stay on the Internet;
* 71% of parents with children aged 14 years or older did not supervise their children's Internet use at all.

Category 31 *The state of information security & technology*

1999-05-27 **virus infection rates study survey**

Reuters

CERT-CC found that malicious software infections increased in the second quarter of 1999, with the Melissa and Chernobyl viruses causing widespread trouble.

Category 31 *The state of information security & technology*

1999-06-16 **criminal hacker attacks statistics study survey police business reporting intrusions**

Courier Mail (Brisbane, Australia), Sydney Morning Herald, Australian Financial Review

Studies by the Australian government contradicted accepted wisdom about the preponderance of inside attacks on business systems; the results suggested that most attacks were from outsiders rather than from disgruntled or dishonest employees. Apparently 42% of businesses said they did not report intrusions — implying that an astonishing (not to say unbelievable) proportion of 58% did report intrusions. Common agreement among security specialists has been that no more than 10% of all detected computer crimes are reported to authorities. Federal Justice Minister Amanda Vanstone everyone to stop seeing hackers "nerdy, pre-pubescent teens with youthful ideals." On the contrary, she said, "Increasingly, organisations around the world are experiencing attacks on their computer systems designed to financially benefit the perpetrator. This is a crime in the old-fashioned sense in that the motivation is greed."

Category 31 *The state of information security & technology*

1999-06-18 **economic impact costs expenses virus worm e-mail attachments damage harm consequences**

Computer Economics http://mindfulness.com/new4/pr/pr990618.html

A study by the Computer Economics firm estimated losses to victims of virus and worm infections at around $7.6B in the first half of 1999.

Category 31 *The state of information security & technology*

1999-06-21 **survey study consumer confidence suspicion worry e-commerce Web**

E-Commerce Times Online

In a study of 1,001 respondents selected at random among the general public, most people expressed suspicion about the security of online transactions. Highlights:
58% of consumers do not consider any financial transaction online to be safe;
67% are not confident conducting business with a company that can only be reached online;
77% think it is unsafe to provide a credit card number over the computer; and
87% want e-commerce transactions confirmed in writing.
The National Technology Readiness Survey was carried out by Rockbridge Associates over a two-year period.

Category 31 *The state of information security & technology*

1999-07-12 **virus hacker breaches survey attacks vulnerabilities**

InformationWeek
http://www.informationweek.com/shared/printArticle?article=infoweek/743/prsecur.htm&pub=iwk

A study of 2700 information technology professionals in 49 countries was summarized in July in InformationWeek. The Global Security Survey had many interesting findings; highlights:
* 64% of companies fell victim to a virus attack in the past 12 months, up from 53% the previous year
* In the U.S. alone, viruses hit 69% of companies, about four times as many as that of the next-highest category of security breach, unauthorized network entry
* 22% of companies reported no security breaches at all
* Hackers and terrorists were blamed for 48% of the security breaches, compared with 14% blaming hackers in 1998
* 31% of respondents blamed contract service providers for breaches (up from 9% last year)
* 41% blamed authorized users and employees (compared with 58% last year).

Category 31 *The state of information security & technology*

1999-08-11 **Internet hosts vulnerabilities scan report**

http://www.securityfocus.com/templates/forum_message.html?forum=2&head=32&id=32%20%20

A small group of experts scanned 36 million Internet hosts in three weeks in December 1998. They published the results in August 1999. They tested for 18 vulnerabilities. They found 730,213 vulnerabilities on 450,000 hosts. They wrote, "These open points of penetration immediately threaten the security of their affiliated networks, putting many millions of systems in commercial, academic, government and military organizations at a high compromise risk."

Category 31 *The state of information security & technology*

1999-09-01 **online auctions fraud theft software copyright violations licenses**

IDG News Service

According to a study by the Software & Information Industry Association (SIIA), almost half the software sold online in auctions managed by eBay, ExciteAtHome and ZDNet violates the terms of the software licenses or is frankly pirated. Highlights of the findings covering 221 auction sales:
* 49% were illegal software
* 33% were legal
* 18% were of undetermined legality.
The 95% confidence limits for a percentages in a sample size of 221 are about ±8% for the 50% mark and decline steadily to about ±2% for lower values.

Category 31 *The state of information security & technology*

1999-09-16 **cyberwar information warfare infowar Trojan virus logic bomb back door criminal hacker penetration vulnerabilities**

SANS, Computerworld Online

The SANS (System Administration, Networking, and Security) Institute warned in September that the Y2K gefuffle provides a perfect cover for disgruntled employees to install logic bombs and back doors. In addition, SANS experts warned that most computers have well-known vulnerabilities — Allan Paller estimates from 5 to 30 — that even novice criminal hackers can exploit.

Category 31 *The state of information security & technology*

1999-09-22 **software piracy theft Web fraud service support disappointment customer resentment**

USA Today

The BSA (Business Software Alliance) released a report showing that the number of Web sites peddling illegal copies of proprietary software grew from 100,000 in 1997 to 900,000 in 1999. Losses are estimated not only at around $11B but also in good will by customers innocently buying stolen software who are shocked (shocked!) at not receiving support from the publishers of the original software. [Hey wait a minute, what about all the people who buy legitimate copies of the software and are shocked (shocked!) at not receiving support from the publishers?]

Category 31 *The state of information security & technology*

1999-10-03 **study report vulnerability assessment infrastructure information warfare infowar**

Reuters

The General Accounting Office of the US government warned that the nation is increasingly vulnerable to information warfare and that the government is not doing enough to prevent damage. Areas of concern included air-traffic control, law enforcement, national defense and tax collection among others. As evidence of the rising threat, the GAO report cited statistics from the CERT-CC (Computer Emergency Response Team Coordination Center) at Carnegie-Mellon University, which handled 1,334 incidents in 1993; in the first half of 1999 the number was 4,398.

Category 31 *The state of information security & technology*

1999-10-04 **information warfare infowar Y2K threats attacks**

Reuters

By October, Worldwide preparations for Y2K-related disruptions were proceeding, with contingency plans for nuclear meltdowns, nuclear shutdowns, false alarms of missile attacks, and electronic attacks on critical infrastructure. In addition, many governments were concerned about disruption and violence from millennial cults and guerrillas looking for softened targets. Many jurisdictions have canceled police leave for the Y2K transition; some countries have canceled leave for the entire military.

Category 31 *The state of information security & technology*

1999-10-05 **survey information warfare Y2K vulnerabilities infrastructure trap doors logic bombs**

Newsbytes

The GAO issued a report, "Critical Infrastructure Protection: Comprehensive Strategy can Draw On Year 2000 Experiences," that emphasized the growing threat of information warfare. Sen. Robert Bennett (R-UT), chair of the Senate Special Committee on the Year 2000 Technology Problem, admitted that there might be a point to converting the Committee to a permanent group focusing on computer crime.

Category 31 *The state of information security & technology*

1999-11-17 **survey vulnerability networks outsourcing standards**

OTC

The Cutter Consortium reported that about 20% of 152 companies they studied had no information security standards at all. About 60% claimed they would implement such policies by the end of the year 2000. Only about 25% of the respondents said they had used security consulting companies for advice.

Category 31 *The state of information security & technology*

1999-11-18 **computer crime attacks vandalism penetration denial of service estimates survey conference**

TechWeb

Thomas Longstaff of the CERT-CC reported on the increasing number of cyberattacks, saying that the situation will only get worse as society increases its reliance on telecommunications for mobile computing and telecommuting. Speaking at the Annual CSI Conference in Washington, Dr Longstaff said that intrusion detection is a necessary component of today's security posture and added that computer emergency response teams are needed too.

Category 31 *The state of information security & technology*

1999-11-29 **fraud shopping e-commerce credit card debit**

Guardian

Gary Parkinson wrote an extensive review of e-commerce risks for The Guardian Weekly (1999-11-29, p. 13). Among his key findings:
* Some fraud artists trade legitimately online to establish credibility before exploiting online shoppers by withholding products or shipping shoddy substitutes or fake goods.
* Although most credit-card companies indemnify victims against losses, online users of debit cards are mostly out of luck if their money is stolen — debit card transactions are equivalent to cash purchases.
* "Visa says that half of all credit card disputes are about internet transactions, even though the net accounts for only 2 per cent of overall business. "

Category 31 *The state of information security & technology*

1999-11-30 **internal fraud statistics surveys studies report UK**

Corporate Insurance & Risk

Martin Allen-Smith wrote a summary of current studies on internal fraud in British corporations. According to his sources (quoting directly from his article),
* 75% of all companies have been hit by fraud at least once in the last five years. 41% have been hit five times or more.
* One in four UK companies have lost more than #600,000 in fraud in the last five years.
*Total UK company losses are estimated at 2% to 5% of annual turnover.
*Only 11% of corporate fraud losses are ever recovered.
*Fraud overtook bad debts as the major cause of business failure in the UK in 1996 according to The Society of Practitioners in Insolvency.
*More than 85% of UK companies believe that they are more at risk from fraud now than they were five years ago.
*The number of fraud charges made against companies by investors and investigated by the Serious Fraud Office has risen by 164% from 1993-96. In 10 of the 11 trials conducted in 1995, one or more of the company defendants were convicted.

Category 31 *The state of information security & technology*

1999-12-06 **survey e-commerce merchants ignorance liability fraud**

Newsbytes

The e-commerce firm CyberSource commissioned a survey of online merchants; the work was carried out by Mindwave and interviewed over 100 online businesses. The findings showed that 75% of the respondents rated credit-card fraud as "a concern" but only 59% knew that they would be liable for restitution in cases of fraud. About 72 percent of online merchants surveyed believed that sales would increase if online shoppers were not worried about fraud. The 95% confidence limits for percentages in a sample of 100 are approximately ±10% at worst.

Category 31 *The state of information security & technology*

1999-12-29 **survey UK Britain British Web ignorance**

ACM TechNews, Newsbytes

British Telecom released survey results [I could not find the sample size] about Web security in December 1999. Highlights:
* 85% of "small to medium" businesses that responded had company Web sites;
* 88% said they had no idea how to secure those sites;
* 25% said they thought better security would hamper online business;
* 12% said they offered their Web visitors SSL;
* 12% used PKI.

31.1 Surveys, studies, audits of security

Category 31.1 *Surveys, studies, audits of security*

1997-01-02 **passwords security management**

PA News

A recent survey by Compaq in the financial district of London showed that poor choices are the norm for computer passwords there. A staggering 82% of the respondents said they used, in order of preference, "a sexual position or abusive name for the boss" (30%), their partner's name or nickname (16%), the name of their favorite holiday destination (15%), sports team or player (13%), and whatever they saw first on their desk (8%).

Category 31.1 *Surveys, studies, audits of security*

1997-06-24 **denial of service interrupts**

EDUPAGE

Pitney Bowes sponsored a study by the Gallup organization and San Jose State University that revealed high levels of interrupts from messages among 972 top-level staff of Fortune 1000 companies. Half of the respondents said they were interrupted at least every 10 minutes and felt overwhelmed by the volume of messages.

Category 31.1 *Surveys, studies, audits of security*

1997-08-05 **statistics data reporting crime break-ins attacks networks**

American Banker

The American Bankers Association announced a new, voluntary system for banks to report attacks on their computer systems. According to the ABA, this voluntary system would provide reassurance to a nervous public and reduce pressures from law enforcement and government officials who have been moving towards legislated reporting mandates. Data would be shared among participating banks and with some government officials. One commentator wrote, "This action displays everything wrong with the current state of the information systems intrusion tracking. Their focus is to prove that break-ins are rare and not identify problems and threats, nor do they plan on sharing the data with law enforcement or intelligence community. When individuals forget they are part of a society with shared problems and goals then we no longer have a society. It will take cooperative effort to track this threat, and this effort will only make them more vulnerable."

Category 31.1 *Surveys, studies, audits of security*

1999-04-06 **theft surveillance eavesdropping data diddling hacking bank**

TIMES OF INDIA

The Times of India reported on the abysmal state of security in Indian businesses, where, as in the rest of the world, managers pay little attention to security until after there's a problem. The article claimed that "a large public sector bank in India was electronically molested recently by hackers who allegedly transferred cash . . . by invading the banks' network."

Category 31.1 *Surveys, studies, audits of security*

2000-01-19 **survey study statistics computer crime cybercrime**

Guardian

Internet-related credit-card fraud rose 29% in 1999, according to the British Home Office's statistics published on the Web (see <http://www.homeoffice.gov.uk/rds/crime statistics> and <http://www.digitalcentury.com/encyclo/update/crime.html>. Cybercrime growth accounted for a major part of the rise in total crime, according to Paul Wiles of the Home Office.

Category 31.1 *Surveys, studies, audits of security*

2000-01-27 **electronic survey Web privacy policy implementation lacunae holes enforcement Web commerce intrusion monitoring government future**

EPIC Alert 7 01

The Electronic Privacy Information Center (EPIC) released an interesting survey of the state of privacy on the Web using a sample of 100 prominent sites. The summary was depressing: "_Surfer Beware III_ found that few of high-traffic websites offered adequate privacy protection. In fact, not a single one of them fulfilled important elements of Fair Information Practices investigated in the survey. Fair Information Practices serve as basic guidelines for safeguarding personal information. Also alarming was the significant proportion (35 out of 100) of shopping sites that allowed profile-based advertising networks to operate. These advertising networks present a stealthy and invasive way in that third parties — companies that display banner advertisements — are tracking online behavior without the knowledge of the Internet user."

Category 31.1 *Surveys, studies, audits of security*

2000-02-18 **vulnerability weakness audit report management Web Internet government**

AP

A Congressional audit report by the General Administration Office included devastating criticisms of the US Environmental Protection Agency on 2000-02-17. The EPA had already shut down its public Web site for fear of penetration in the face of observations such as, "riddled with security weaknesses" and "a likely target for hackers." The investigators "found serious and pervasive problems that essentially render EPA's agencywide information security program ineffective. . . Moreover EPA cannot ensure the protection of sensitive business and financial data maintained by its larger computer systems or supported by its agency-wide network."

Category 31.1 *Surveys, studies, audits of security*

2000-02-22 **e-commerce survey**

NewsScan, CNet http://news.cnet.com/news/0-1007-200-1554830.html

A Forrester Research survey last summer [1999] of 17,000 households in Germany, France, Sweden, the Netherlands and the U.K. indicates that less than 10% of respondents were interested in shopping online. In Sweden, where e-commerce was most popular, 14% of households were connected to the Web and 7% had ordered goods. At the other end of the scale, only 7% of French households were linked to the Net, and only 2% had bought anything. However, a third of French homes subscribe to Minitel, which has offered shopping and information services for 17 years, and presents a strong challenge to Internet-based e-commerce in that country. Most respondents cited privacy concerns and the inability to actually see what they were buying as the major impediments to e-shopping. (Reuters/CNet News.com 22 Feb 2000)

Category 31.1 *Surveys, studies, audits of security*

2000-03-02 **poll survey study consumer confidence criminal hacking Web vandalism**

NewsScan, Washington Post http://www.washingtonpost.com/wp-dyn/business/A56622-2000Mar1.html

The Gallup polling organization [said] that the recent attacks by network vandals on prominent Web sites have left one-third of online consumers less likely to make a purchase via the Internet. The chief executive of At Plan, the online marketing consultancy that sponsored the Gallup poll, says that the attacks were "a cold dose or reality to many people... almost like the loss of innocence in first love." (Washington Post 2 Mar 2000)

Category 31.1 *Surveys, studies, audits of security*

2000-03-22 **CSI FBI annual survey computer crime costs losses trends study**

Reuters, CSI http://www.gocsi.com/prelea_000321.htm, NewsScan, Los Angeles Times http://www.latimes.com/business/20000322/t000027053.html

The annual CSI / FBI computer crime survey was released in March 2000. The self-selected response group included 273 organizations and 643 security practitioners in US corporations, government, finance, health-care, and academia. Total reported losses were $265M. About 90% of the respondents experienced breaches of information security in the preceding 12 months; the top three problems were computer viruses, laptop theft and employee net abuse. However, 70% of the respondents also reported other types of breach: theft of secrets, financial fraud, outsider penetration of security perimeters, denial of service, and sabotage of data or networks. In addition, 74% acknowledged financial losses — higher than in the 1998-1999 survey. Some 59% of the respondents rated Internet connections as a more frequent point of attack than internal systems (38%). As usual, there were many other interesting questions and responses in the survey.

Category 31.1 *Surveys, studies, audits of security*

2000-05-25 **e-mail productivity appropriate use restrictions improvements education spam**

NewsScan

Ferris Research . . . released the results of a study designed to quantify the costs and benefits of e-mail, and estimates that the overall benefit in terms of increased productivity equals about $9,000 per employee. Rather than treading into the murky area of nonquantifiable benefits, such as improved decision-making, Ferris attempted to focus on items that delivered a tangible benefit, like time not spent on addressing snail mail envelopes, operating postage and fax machines, etc. It derived a 15% to 20% productivity improvement, with an overall increase of 326 hours per employee on the average. Ferris then attempted to quantify those hours, giving them a value of $13,000. Then came the downside: Ferris found that employees waste on an average 115 hours dealing with nonproductive e-mail, translating to a loss of about $4,000 per worker a year. Subtract the loss from the gain, and the result is an overall benefit of $9,000 per employee, or a 15% productivity gain. Ferris says that rate can be raised to 20% by more actively managing company e-mail systems: discouraging personal e-mail, shortening e-mail distribution lists, and helping workers identify and trash spam. (Investor's Business Daily 25 May 2000)

Category 31.1 *Surveys, studies, audits of security*

2000-05-25 **intellectual property copyright infringements violations theft music sales**

NewsScan, Los Angeles Times
http://www.latimes.com/business/20000525/t000049387.html

A [highly controversial] study of music sales commissioned by Reciprocal Inc., a digital rights management company, shows that sales of recorded music have declined in the vicinity of college campuses in the last two years, while rising elsewhere. Music sales were up 12% during the first three months of 2000 over the same time period in 1998, but at stores within five miles of a college campus — which account for about half of all music purchased — sales were down 4%. Music industry officials attribute the dip to use of Napster, which has been especially popular among college students. Some colleges have banned the music downloading software from campus computer systems because heavy use was clogging their networks. (AP/Los Angeles Times 25 May 2000)

Category 31.1 *Surveys, studies, audits of security*

2000-06-12 **confidence government regulation industry pornography protection business research report survey focus groups**

NewsScan, New York Times
http://partners.nytimes.com/library/tech/00/06/biztech/articles/12mark.html

Focus groups held . . . [in June] by Greenberg Quinlan, a Washington public policy research firm, . . . [seemed] to indicate a shift in public attitudes about Internet regulation. Whereas two years ago people were more inclined to look to government to regulate pornography and other kinds of activities found on the Internet, they now seem to trust business rather than government. Stanley Greenberg, who directed the research project on behalf of the nonprofit Markle Foundation, says: "People didn't understand the Internet as well. They understand more now about the difficulty of regulation." (New York Times 12 Jun 2000)

Category 31.1 *Surveys, studies, audits of security*

2000-06-15 **intellectual property copyright theft survey purchase ethical downloading**

NewsScan, Wall Street Journal
http://interactive.wsj.com/articles/SB961025291366759846.htm

A new survey, . . . [released in June] by the Digital Media Association, indicates that Internet users who download music to sample are likely to follow up by purchasing CDs in stores or online. The new poll contradicts the findings of previous studies that found digital music downloading via Napster made a significant dent in bricks-and-mortar music store sales, especially in areas around college campuses. This latest survey, conducted by market research firm Yankelovich Partners, says 66% of all consumers said that listening to a song online has at least once prompted them to later buy a CD or cassette featuring that song. Most people who downloaded music (92%) listened to it on their desktop computers, while 10% used a portable device and 14% used their home stereo. More than 60% of them used the Internet to get to music they couldn't find on radio. According to Media Metrix, 22.8 million people visited the top 30 Internet music sites in April, up 19% from November 1999, the most recent number available. Paid digital music downloading is expected to hit $1.1 billion in sales by 2003, according to estimates by Forrester Research. (Wall Street Journal 15 Jun 2000)

Category 31.1 *Surveys, studies, audits of security*

2000-07-31 **survey study vulnerabilities weakness Web servers SSL public-key digital certificates**

RISKS, http://www.meer.net/~ericm/papers/ssl_servers.html 21 02

Eric Murray published the results of a survey of Web security: "A random sample of 8081 different secure Web servers running the SSL protocol in active use on the Internet shows that 32% are dangerously weak. These weak servers either support only the flawed SSL v2 protocol, use too-small key sizes (40 bit encryption), or have expired or self-signed certificates. Data exchanges with all types of weak servers are vulnerable to attack."

Category 31.1 *Surveys, studies, audits of security*

2000-08-12 **audit study weakness security program government agency evaluation failure miserable pathetic fiasco**

RISKS, http://com-notes.house.gov/ai00215.pdf 21

The General Accounting Office of the US government gave the Environmental Protection Agency a failing grade on computer security in August. The GAO described the agency's program as "Ineffective, inadequate, and riddled with weaknesses."

Category 31.1 *Surveys, studies, audits of security*

2000-08-21 **privacy cookies dishonesty Web personal information anonymity blocking encryption e-mail**

NewsScan

A . . . study by the Pew Research Foundation finds that "There is broad-based concern about privacy being compromised [on the Net]," . . . [said] Lee Rainie, director of the study. Eighty-four percent of respondents reported they were concerned about businesses invading their privacy online, and many were frustrated by their unfamiliarity with the basic mechanics of Internet data collection. For instance, 56% of Internet users surveyed did not know what an Internet "cookie" is. The study attributes this lack of knowledge to the fact that about 35% of the 144 million people who use the Internet in the U.S. came online within the past year. Among more sophisticated Web surfers, only 5% use "anonymizing" software to hide their identities; 10% report using encryption software to protect their e-mail; 20% use a secondary e-mail address when forced to provide information on a Web site; and 25% say they have given a fake name or provided false responses on a Web site information form. (Los Angeles Times 21 Aug 2000)

Category 31.1 *Surveys, studies, audits of security*

2001-01-04 **survey CIO confidence security law enforcement**

NewsScan

CIOs: "WHAT, ME WORRY?"

A national poll of 1,400 CIOs reveals that 90% have confidence in their network security, despite estimates that billions of dollars are lost every year to cybercrime. The survey, conducted by RHI Consulting, has raised eyebrows among security experts who point out that it's generally in a CIO's best interest to keep quiet when security breaches occur. A recent survey conducted by the Computer Security Institute indicated that more than half of the respondents said they did not report the intrusions to law enforcement out of fear of negative publicity or that rival companies would use the information to competitive advantage. In addition, many CIOs may feel that they must live with a "buffer of acceptable risk." "Just as credit card companies accept some level of loss as a cost of doing business, so some CIOs are saying, 'if I do a really solid job of protecting my systems, then I can live with the low-level pain that some break-ins cause,'" says one expert. Meanwhile, a 1999 survey found that Fortune 1000 companies lost more than $45 billion in thefts of proprietary information that year. (InfoWorld 3 Jan 2001) http://www.infoworld.com/articles/hn/xml/01/01/03/010103hncios.xml?p=br&s=2

Category 31.1 *Surveys, studies, audits of security*

2001-01-12 **computer crime statistics exaggeration inflation**

RISKS 21 21

S. Harris contributed an interesting analysis to RISKS of how very large figures get reported for losses due to industrial espionage. In response to another correspondent's question about how companies estimate the costs of breaches of confidentiality, he wrote the following:

>I can give a first hand account of a $2 billion theft of proprietary information to illustrate how these exaggerated figures get manufactured. Back in 1989 I worked at a Toronto software development company that did lots of work with the Unix operating system, and licensed the Unix source code from AT&T for about $60,000 a year.

Night after night someone was logging in to the computers from a dialup line to download chunks of the Unix source code. Somebody at the company noticed this, called in the police, who traced the connection to an ex-employee, raided his house and seized his home computer. Apparently the ex-employee, a software development manager, who had recently left the company, missed having access to the Unix source code and wanted to grab a copy of it for personal study. Satisfied that the source code had been recovered, and that this wasn't a case of espionage or sabotage, the company would have been happy to let the matter drop.

But the cops insisted on laying charges and it appears that they leaked the story to the media. All three Toronto newspapers (Toronto Sun, Toronto Star, and the Globe & Mail) reported that the police had foiled a $2 billion theft!

Why wasn't this as a $60,000 theft of a commercial source code license? Or at the very most a $500 theft of an educational license, since the ex-employee's intended use was only to study it?

Well it seems that the police had called up AT&T and asked them "How much is Unix worth?" The answer was $2 billion. AT&T gave Unix an asset value of $2 billion on their books. The police equated a little mischief to the cost of acquiring total ownership of AT&T's Unix System Laboratories and all its intellectual property!

In this case, the large corporation gave an accurate estimate to a bogus question. It was law enforcement (and sloppy fact checking by the media) that twisted the story.

But you know, even the $2 billion asset value seems suspect to me now because AT&T sold Unix to Novell in 1993 for just $270 million (see http://www.att.com/press/0693/930614.ulb.html). Novell in turn sold it to SCO in 1995 for a paltry $54 million (6M SCO shares at about $9 each is $54M, see http://www.novell.com/company/ir/96annual/mandis.html). But if AT&T overestimated by tenfold, the police still exaggerated by 4 million fold.<

Category 31.1 *Surveys, studies, audits of security*

2001-01-24 **privacy marketing children study survey**

NewsScan

ONLINE KIDS READY TO TELL YOUR SECRETS
Three out of four children are perfectly willing to divulge private family information online in exchange for incentives such as prizes, products or cash, according to a new report by eMarketer. Fifty-four percent of the children surveyed were willing to disclose the name of their parents' favorite store, while 26% were willing to tell e-tailers about their parents' weekend activities. According to the study, the information typically given by children online tends to be marketing oriented, rather than financial. "The information is not the really serious information like credit card or Social Security numbers," says eMarketer analyst Rob Janes. "It's more stuff that's of value to a marketer, such as product information, family activities, etc... Children and teens were very casual about revealing family information. It can't be extrapolated accurately to the entire population, but it's a good strong indicator of how kids will respond to information online. It's an issue that parents should address." (E-Commerce Times 24 Jan 2001)
http://www.ecommercetimes.com/perl/story/6942.html

Category 31.1 *Surveys, studies, audits of security*

2001-02-12 **privacy corporate governance administration position CPO**

NewsScan

CHIEF PRIVACY OFFICER AN ACCEPTED POSITION IN TODAY'S ORGANIZATIONS
The position of CPO ("chief privacy officer") is being created at an increasingly large number of U.S., including some companies as IBM, AT&T, Eastman Kodak, DoubleClick, RealNetworks, Microsoft, U.S. Bancorp, and many others. Privacy expert Alan F. Westin says there are now at least 100 privacy chiefs in the United States, making $125,000 to $175,000 a year, and he expects that number will grow by 5 to 10 times just one year from now." Who becomes a CPO? Stephanie Perrin, the chief privacy officer of Montreal-based Zero-Knowledge Systems, explains: "Obviously, we're not going to just pick somebody from the legal department," because privacy is more than a matter of just following the law. "You have to have a fundamental commitment to - dare I say it? - morality. Privacy is not just good business. We are framing the information age, and it is important to take that job seriously. We really do look at privacy as a human right, and not just a luxury item for spoiled North Americans. We're talking about the global information infrastructure." (New York Times 12 Feb 2001)
http://partners.nytimes.com/2001/02/12/technology/12PRIV.html

---

Category 31.1 *Surveys, studies, audits of security*

2001-02-12 **online gambling survey predictions**

NewsScan

ONLINE GAMING TAKES OFF IN U.S.
Forty million households will be engaged in online gaming by 2004, up from 25 million in 2000, according to new research from IDC. Fueling the growth will be faster Internet connections, the arrival of next-generation game consoles, and new, nontraditional gaming platforms. Most online gaming business models are based on advertising revenue, but sites are seeking ways to create different types of advertising opportunities or to migrate free subscribers to a paid model. Meanwhile, NetValue reports that in Europe, the U.K. leads Germany, France, Spain and Denmark in online gaming, with one in five British Internet users visiting a game site in December. Spanish gamers spent an average of 27 minutes on each site, Danish and U.K. users 23 minutes, French and German users just 14 minutes, while U.S. users stayed online an average of 38 minutes. The most visited game site in the U.S. was uproar.com, while in the U.K., gamers flocked to gamesdomain.com. (NUA Internet Surveys 12 Feb 2001)
http://www.nua.ie/surveys/?f=VS&art_id=905356444&rel=true

Category 31.1 *Surveys, studies, audits of security*

2001-03-10 **CERT/CC Summaries general trends vulnerabilities attacks malicious software malware**

CERT/CC Summaries

The CERT/CC Summaries Web page < http://www.cert.org/summaries/ > lists (and links to) the following regularly-scheduled overviews for January 2001 through March 10, 2002:

CS-2002-01
February 28, 2002
Topics in this regularly scheduled CERT Summary include multiple vulnerabilities in SNMP, a buffer overflow vulnerability in Microsoft Windows UPnP, vulnerabilities in SSH implementations, and the W32/BadTrans Worm.

CS-2001-04
November 20, 2001
Topics in this regularly scheduled CERT Summary include the W32/Nimda Worm and active exploitation of vulnerabilities in SSH1 CRC-32 Compensation Attack Detector and in Microsoft DNS servers.

CS-2001-03
August 28, 2001
Topics in this regularly scheduled CERT Summary include self-propagating worms, active exploitation of vulnerabilities in Solaris in.lpd, BSD telnet daemon, and Microsoft IIS by intruders. We have also seen an increase in intruder activity directed at home users.

CS-2001-02
May 29, 2001
Topics in this regularly scheduled CERT Summary include a significant increase in reconnaissance activity, a number of self-propagating worms, and active exploitation of vulnerabilities in snmpxdmid, BIND and IIS by intruders

CS-2001-01
February 28, 2001
Topics in this regularly scheduled CERT Summary include multiple vulnerabilities in BIND, compromises via "ramen" toolkit, input validation problems in LPRng, and VBS/OnTheFly (Anna Kournikova) malicious code. There is also mention of the new Vulnerability Notes Database.

Category 31.1 *Surveys, studies, audits of security*

2001-04-03 **survey privacy attitudes USA surveillance Internet**

NewsScan

PEOPLE WANT PRIVACY FOR THEMSELVES, SURVEILLANCE FOR OTHERS
A Pew Internet & American Life Project survey of Internet users has found that Americans have distinctly mixed feelings about privacy on the Internet: they want it for themselves but they also want the government to use surveillance techniques to catch pornographers, con artists, and other criminals online. More than 90% of those surveyed expressed revulsion at child pornography online, and 62% want legislators to pass new laws protecting online privacy. According to project director Susannah Fox: "Americans are searching for an Information Age answer to the age-old question of how to balance their yearning to be protected from criminals and their yearning to prevent government authorities from abusing their investigative powers.." (Washington Post 2 Apr 2001)
http://washingtonpost.com/wp-dyn/articles/A28560-2001Apr2.html

---

Category 31.1 *Surveys, studies, audits of security*

2001-04-10 **survey study music intellectual property copyright sharing alternative**

NewsScan

STUDENTS WILLING TO PAY FOR MUSIC
More than a third of students who download music from the Internet would be willing to pay $8.50 a month for the privilege, according to a survey of 1,800 students on campuses ranging from Harvard to the University of Southern California. The typical student is interested in singles, live tracks, international music and new artists, and spends more time listening to tunes on his or her computer than on the radio. Boosting these figures is the fact that the typical student also has access to fast Internet connections and high bandwidth. "As broadband grows, more people will use computers for music and other entertainment," says an analyst with Mercer Management Consulting, which conducted the poll in conjunction with the National Association of Recording Merchandisers. "We don't feel this is going to erase CD purchasing completely. This is a new opportunity. There's a whole other batch of music record labels could sell to people... One of the biggest surprises to some of the retailers is that people sample music on Napster and then go out and buy it." (InformationWeek 9 Apr 2001)
http://www.techweb.com/wire/story/TWB20010409S0020

Category 31.1 *Surveys, studies, audits of security*

2001-04-17 **privacy policy compliance federal government Web report**

NewsScan

FEDS LAX IN FOLLOWING PRIVACY GUIDELINES
Senator Fred Thompson (R., TN) says that a forthcoming study will show that dozens of federal Web sites are ignoring guidelines intended to protect the privacy of persons visiting them, and are not closely managing how the sites are operated. One agency, the National Aeronautics and Space Administration, was not even able to determine how many Web sites it operates. The report, which will be released within a few months, was assembled from 16 separate agency audits.
http://www.cnn.com/2001/TECH/internet/04/17/internet.privacy.ap/index.html?s=10

Category 31.1 *Surveys, studies, audits of security*

2001-04-19 **study COPPA Children's Online Privacy Protection Act enforcement evasion Web**

NewsScan

CHILD PRIVACY LAW BEING EVADED [28 Sep 2001]
A study of the effectiveness of the rules the Federal Trade Commission issued to implement Children's Online Privacy Protection Act (COPPA) has found that most Web sites have failed to do what the law requires. One of its requirements is for sites must obtain "verifiable parental consent" involving any use of data from children under 13; another is that the privacy policy of the sites be clearly explained. The new study, which was authored by Joseph Turow of the University of Pennsylvania's Annenberg Public Policy Center, says that a large number of sites are skirting the intent of those requirements, and that most of the site policy statements were so long and complex that it took an average of 9.4 minutes to reach policy in search of its COPPA statements. (San Jose Mercury News 28 Sep 2001)
http://www.siliconvalley.com/docs/news/svfront/034390.htm

FTC FINES THREE KIDS SITES FOR PRIVACY VIOLATIONS [19 Apr 2001]
Three Web sites for young people -- GirlsLife.com, BigMail.com, and InsideTheWeb.com -- have agreed to pay $100,000 to settle charges brought against them by the Federal Trade Commission for collecting personal data about children without proper permission from their parents. A survey of kids sites by the nonprofit Center for Media Education found that only 38% of those required to obtain parental permission did so adequately. (AP/USA Today 19 Apr 2001)
http://www.usatoday.com/life/cyber/tech/2001-04-19-kids-sites-privacy-fine.htm

---

Category 31.1 *Surveys, studies, audits of security*

2001-05-01 **audit review study survey Web weaknesses vulnerabilitiesl servers**

NIPC Daily Report

At least 100 New Zealand Web sites have security flaws, claims an Auckland-based Internet security firm. Software Creations says this includes one in five of those using version 5 of Microsoft's Internet Information Server (IIS) and a third of those with version 4. The claim follows a "friendly hack" of the sites earlier this month by owner-operator Brett Moore using a year-old "web bug." The program enters a Web site and, depending on the code returned, tells a hacker if a system is at risk.assess the sites using a simple program he developed in 20 minutes. He says it is similar toand took two hours to test the sites. (IDG News Service, 1 May)

Category 31.1 *Surveys, studies, audits of security*

2001-05-07 **Web sites vulnerabilities audit weaknesses study survey**

NIPC Daily Report

Out of three million Web sites tested worldwide, 80 percent have been given the thumbs down when it comes to security vulnerability, exposing a large number of organizations and governments to hackers, criminals and vandals. The study, by Unisys Australia Architecture Director, IT Security Consulting Services Ajoy Ghosh, randomly tested three million .com, .net, and .au domains for security holes, finding 80 percent of Web sites transacting on the Internet open to damage and theft as the correct technology is not in place. The study further revealed that Australian banks were among the Web sites most open to online attacks.

Category 31.1 *Surveys, studies, audits of security*

2001-05-29 **music piracy copyright intellectual property youth culture survey study**

NewsScan

YOUNGER USERS CRANK UP THE VOLUME ON ONLINE MUSIC
More than half of all young adult Web users (age 18 to 24) have downloaded tunes from the Internet, according to a survey of 7,688 Internet users from 30 countries. Research firm Ipsos-Reid found that 61% of users in that age group had downloaded music, up from 53% a year earlier. The study also found that 70% of males age 18 to 24 had downloaded music, compared with 48% of females. Meanwhile, another study conducted by Informa Media Group predicts that with the advent of big-label music subscription services, subscriptions likely will account for nearly 24% of online music sales worldwide by 2006. The study estimates total global music sales, online and off, will increase 26% to $46.5 billion in 2006, led by the U.S. with 54% of the market. Europe and Asia-Pacific will follow, with 25% and 18% respectively. "We really are witnessing the dawn of the global music bazaar," says a senior researcher at Ipsos-Reid. "In a few years we're going to be seeing people from anywhere in the world acquiring music online from anywhere in the world -- a sort of musical ubiquity." (CNET News.com 29 May 2001)
http://news.cnet.com/news/0-1005-200-6087379.html?tag=owv

Category 31.1 *Surveys, studies, audits of security*

2001-06-05 **physical damage sabotage computers equipment rage**

NewsScan

SURVEY REVEALS EPIDEMIC OF BATTERED PCs
A survey by British PC maker Novatech, intended to take a lighthearted look at techno-glitches, instead revealed the darker side of computing. One in every four computers has been physically assaulted by its owner, according to the 4,200 respondents. "The incidents of willful neglect have always been high," says the owner of a New York computer repair shop. "We've always had to deal with computers damaged by people who dumped their refreshing beverage on the computer's keyboard, or got tangled up in the cords, bringing the computer crashing down off their desk." But recently, more instances of intentional abuse are cropping up -- broken keys "from people smacking down on the keyboard with an open hand or sometimes a fist," and more commonly, "a sharp slap delivered to the monitor or the hard drive case. If you smack a machine when the hard drive is spinning, you can kill the hard drive." Most likely to provoke abuse by British users were "oops" moments, like when sensitive e-mail is sent to the wrong recipient, or a cache of previously visited porn sites is revealed at the wrong time. But an Italian repair specialist said it was all part of the culture: "People here tend to express themselves very emotionally. It is not uncommon for them to hit their televisions, their scooters and their computers... And sometimes a fast smack does fix the problem, you know." A retired psychology professor from Budapest sums it up: "We treat our machines as if they are persons. We talk to them, we name them, we even somachine. And when the little god turns out to be evil we beat the machine to purge the demon." (Wired.com 5 Jun 2001)
http://www.wired.com/news/culture/0,1284,44284,00.html

Category 31.1 *Surveys, studies, audits of security*

2001-06-09 **expectation of privacy workplace monitoring survey study**

NewsScan

WORKPLACE PRIVACY "A CONTRADICTION IN TERMS"
A study by the American Management Association (AMA) has found that three out of four of the 1600 U.S. businesses it surveyed electronically monitor their employees in one way or another. Internet connections were monitored by 63%, telephone use by 43%, computer use (time logged on or keystroke counts) by 19%, video security surveillance by 38%. Although federal law generally prevents employers from monitoring of live conversations, it does not apply when the communication is stored and retrieved, such as through voice mail, e-mail, or Web monitoring. The director of the AMA study said: "Workplace privacy is a contradiction in terms. It's an oxymoron. I know the illusion of privacy is there, but you are not using your own stuff. The phone, the keyboard, the connections, the job itself -- they don't belong to you; they belong to the company, legally." (San Jose Mercury News 9 June 2001)
http://www.siliconvalley.com/docs/news/svfront/066891.htm

Category 31.1 *Surveys, studies, audits of security*

2001-07-15 **Internet Web fraud statistics survey study report**

NewsScan

INTERNET FRAUD KEEPS GOING AND GOING
The National Consumer League says that the average loss from Internet fraud rose from $310 a person in 1999 to $427 last year, when total losses from Internet fraud reached $3.3 million. New York City's consumer affairs commissioner Jane Hoffman warns: "Internet fraud runs the gamut from work-at-home scams to bogus travel and vacation schemes, to securities fraud and investment scams... For many consumers the Internet can be a virtual nightmare when it comes to fraud." Hoffman says the five most common Internet scams are: Web auctions (mainly in the form of goods not delivered as promised, inflated prices, or fake bids to puff up prices); travel and vacation schemes with hidden costs; theft of ID numbers, bank data, or passwords; and investment schemes promising -- but of course failing to deliver -- huge profits. (AP/Washington Post 15 Jul 2001)
http://washingtonpost.com/wp-dyn/business/latestap/A492-2001Jul15.html

---

Category 31.1 *Surveys, studies, audits of security*

2001-08-03 **security audit government passwords access confidentiality operations availability**

NewsScan

NETWORK SECURITY PROBLEMS AT COMMERCE DEPARTMENT
The General Accounting Office has prepared a report critical of the U.S. Commerce Department's computer security measure: "Individuals, both within and outside Commerce, could gain unauthorized access to these systems and read, copy, modify and delete sensitive economic, financial, personnel and confidential business data. Moreover, intruders could disrupt the operations of systems that are critical to the mission of the department." Many users of Commerce systems were found to have easily-guessed passwords and to have greater network access than justified by their 'need-to-know' level. (AP/San Jose Mercury News 3 Aug 2001)
http://www.siliconvalley.com/docs/news/svfront/064118.htm

Category 31.1 *Surveys, studies, audits of security*

2001-08-28 **survey study music intellectual property copyright sharing alternative**

NewsScan

CONSUMERS NOT READY TO PAY FOR ONLINE MUSIC
Consumers are resistant to the idea of purchasing and downloading music from the Web and are likely to remain so, according to a poll of 4,000 Internet users by GartnerG2. Less than 50% of respondents listened to CDs on their computers, and only 25% had listened to music downloads on their PCs. Only 6% reported purchasing digital music downloads in the last three months. "The percentage of Internet music buyers is not likely to increase with new Internet services being developed by the big five music companies unless they make their copyright protection systems more flexible to entice consumers," says a Gartner analyst. "Digital distribution needs to be brain-dead simple for consumers, and any DRM solution deployed should work with all music software and hardware. In order for this to happen, the Big 5 need to work together, and that doesn't look hopeful before 2002." (Reuters 28 Aug 2001)
http://news.cnet.com/news/0-1005-200-6997967.html?tag=nbs

Category 31.1 *Surveys, studies, audits of security*

2001-08-30 **privacy online banking industry survey study report inadequate problems**

NewsScan

PRIVACY INADEQUATE FOR ONLINE BANKING, SAYS REPORT
A report by the nonprofit advocacy group Center for Democracy and Technology says that the Center has filed a complaint with the Federal Trade Commission charging five regional bankers of failing to post any notice of their privacy rules. George Washington law professor Peter Swire said at the press conference held to announce the report's release: "The price of opening a checking account should not be that your personal information is traded, sold or swapped." The CDT found some banks much better than others with regard to privacy protection, and praised First Union Bank for providing multiple ways in which customers can protect their personal information from being shared with merchants and others. (Washington Post 30 Aug 2001)
http://washingtonpost.com/wp-dyn/articles/A16683-2001Aug29.html

---

Category 31.1 *Surveys, studies, audits of security*

2001-10-02 **Web security audits studies vulnerabilities**

NewsScan

NEW INTEREST IN NETWORK SECURITY
Security companies are being deluged with business opportunities, and CEO Peggy Weigle of the Internet security firm Sanctum explains, "Network security used to be a necessary evil, but now it's a core value of companies." Doing security audits commissioned by 300 organizations, Weigle found the results "scary" and said, "We could have stolen flight manifests, personnel files, sensitive data... We could have easily gotten onto a flight illegally." Research firms Gartner and IDC predict that the network security market in the U.S. will grow 20% to 24% a year between now and 2005. (USA Today 2 Oct 2001)
http://www.usatoday.com/life/cyber/tech/2001/10/2/network-security.htm

---

Category 31.1 *Surveys, studies, audits of security*

2001-11-16 **security audit government departments agencies Congressional committee failing grade GAO passwords encryption confidentiality**

RISKS 21 76

Peter G. Neumann summarized another security evaluation of government departments and agencies:

"The latest quarterly computer-security report card put together by Congressman Steve Horn's House Reform Committee government efficiency subcommittee and the GAO and OMB gives the government an F grade (down from a D- a year ago), based on lax protection of federal computer networks against hackers, terrorists, and others. Two-thirds of the federal agencies flunked this time, including the departments of Defense, Commerce, Energy, Justice, Treasury, Agriculture, AID, Education, Health and Human Services, Interior, Labor, Transportation, Small Business, and Veterans Affairs. The B+ given to the National Science Foundation was tops, with Social Security getting a C+ and NASA C-. As expected, the GAO found systems with no passwords, with ``password'' as password, and with unencrypted accessible password files. [Source: AP Online via COMTEX, 9 Nov 2001, PGN-ed] "

Category 31.1 *Surveys, studies, audits of security*

2001-12-29 **medical information security informatics implementation failures ignorance**

RISKS 21 84

Laura S. Tinnel analyzed a medical-office's new online medical records system and wrote a good essay in RISKS about the perils of having amateurs deal with such systems. Some highlights (or maybe "lowlights" would be a better word) summarized from her interesting report:

* Physically unprotected workstation allowed reboot and installation of Trojan software.

* Live network connection allowed network access to anyone.

* Responsible doctor had no idea how system was configured to avoid default wide-open state.

* No thought about unauthorized write-access to patient data or consequences of such data diddling.

Category 31.1 *Surveys, studies, audits of security*

2002-01-10 **copyright intellectual property music sales statistics survey study royalties fees**

NewsScan

LET THERE BE MUSIC, LET THERE BE LOVE, LET THERE BE VULGAR ROYALTIES
Soundscan, a company that tabulates retail sales of recorded music, has reported that the number of albums sold last year dropped 2.8% from previous-year's sales, the first decline since the company began a decade ago. One record company executive warns, "We have to rethink our business, and it may not be the record business anymore." Concurring with that assessment, Michigan congressman John Conyers Jr., the senior Democrat on the House Judiciary Committee, says: "Technology is forcing the record labels and the artists and the writers and the composers to come together. The Internet says to the industry that you folks are yesterday's news, you're following outdated models, your business strategies don't work anymore, and your profit motive is showing rather vulgarly." And Eben Moglen, a Columbia University law professor and general counsel of the Free Software Foundation, pleads for a return to the spirit of "music before Edison" -- a time when (he believes) music was not a commodity but a form of love. Alluding to the music-swapping experiments that take place on the Internet, Moglen argues that "everything that can be shared will be shared. But people make music because they love it, and they'll pay for it because they love it." (New York Times 10 Jan 2002)
http://partners.nytimes.com/2002/01/10/arts/music/10CONF.html

---

Category 31.1 *Surveys, studies, audits of security*

2002-01-30 **non-profit organizations security practices survey audit results sensitive data confidentiality intrusion vulnerability disaster recovery**

RISKS 21 91

Audrie Kraus, Executive Director of NetAction, summarized the disturbing results of that organization's "survey of security practices in nonprofit organizations" which found among many other things that non-profits studied had ". . . substantial room for improvement, especially in maintaining the security of confidential and/or sensitive files, user work habits, and disaster planning."

http://netaction.org/security/.

Category 31.1 *Surveys, studies, audits of security*

2002-02-04 **security industry survey study statistics revenue growth**

NewsScan

SECURITY FIRMS PROSPERING UNDER NEW CONDITIONS
Computer security companies are surviving the technological recession quite nicely, and one of them, Symantec, expects to break the billion-dollar sales mark this year. Gartner says that Symantec is the No. 1 provider of security and antivirus software but that it has been trailing Internet Security Systems and Check Point Software Technologies in detection and firewall software. (San Jose Mercury News 4 Feb 2002)
http://www.siliconvalley.com/docs/news/svfront/symant020402.htm

---

Category 31.1 *Surveys, studies, audits of security*

2002-02-25 **online pornography addiction survey study statistics estimates**

NewsScan

ADDICTED TO "ADULT" SITES
An online survey by the San Jose Marital and Sexuality Centre reports that 10% of the 7,037 individuals responding to the survey say they are addicted to cybersex. Other data: Neilsen/NetRatings figures indicate that there were 27.5 million U.S. visitors to adult-oriented sites last month; of that number, 72% were men and 28% women. (USA Today 25 Feb 2002)
http://www.usatoday.com/life/cyber/tech/2002/02/26/cybersex.htm

---

Category 31.1 *Surveys, studies, audits of security*

2002-02-25 **music piracy copyright intellectual property theft survey study statistics losses damage ethics**

NewsScan

RIAA: PUT ANOTHER NICKEL IN THAT NICKELODEON FOR MUSIC, MUSIC, MUSIC
The music industry is desperate to find a way of downloading a solution to the problem of illegal downloading of copyrighted songs. The Recording Industry Association of America (RIAA) says that shipments by record companies to consumers have dropped by more than 10% in the past year, and RIAA president Hilary Rosen complains: "When 23% of surveyed music consumers say they are not buying more music because they are downloading or copying their music for free, we cannot ignore the impact on the marketplace. " (Reuters/New York Times 25 Feb 2002)
http://partners.nytimes.com/reuters/technology/tech-leisure-music.html

---

Category 31.1 Surveys, studies, audits of security

2002-03-20 **e-commerce wireless cellular mobile phone survey study e-payments**

NewsScan; http://online.wsj.com/article/0,,SB1016559287588926040.djm,00.html
(sub req'd)

CONSUMERS WANT M-COMMERCE 'SIMPLE AND SMALL'
Consumer enthusiasm for mobile commerce -- buying goods and services via cell phones -- has dwindled since 2000, with only 1% of mobile users surveyed worldwide in January saying they intend to use Internet-enabled phones for any type of transaction. That's down from 12% a year earlier and 32% in June 2000. "The more they have used it, the less they have liked it," says a consultant at A.T. Kearney in London. However, 44% of the 5,600 wireless customers polled said they would be interested in finding out more about "m-cash" -- systems that allow users to make small purchases by dialing a number on the mobile phone and then having the charge included on the monthly phone bill. Companies already experimenting with m-cash include Pepsi, which has launched an m-cash program for distributors in the U.S. Cingular Wireless and Vodafone have also initiated limited m-cash services. Despite consumer interest, enthusiasm risks being derailed by the technical difficulty of installing the necessary hardware infrastructure to accommodate m-cash transactions. "It's convenient from a consumer perspective because it removes the need for small cash," says a marketing manager for Visa International. "But if you're going to retrofit every vending machine just to have people zap it with their mobile phones, I don't think there's a business case for that." Additional questions arise over the willingness of wireless carriers to act as the collector of other companies' debts. "There's a substantial credit risk related to this," says a Scandinavian banking expert. (Wall Street Journal 20 Mar 2002)

Category 31.1 Surveys, studies, audits of security

2002-04-04 **security threats vulnerabilities survey attitudes beliefs viruses hackers terrorists**

Security Wire Digest, 4 26
http://www.instat.com/press.asp?ID=162&sku=IN020154NA

Security Wire Digest reported, "… [A] recent survey says infosec spending continues to be driven by the threat of hackers and viruses. According to InStat, a technology market research firm, … 80 percent of the businesses it survey have the same attitude toward network security as they did prior to the Sept. 11 attacks and that they are more concerned about viruses and hackers than terrorists."

Category 31.1 Surveys, studies, audits of security

2002-04-08 **computer crime survey statistics study**

NewsScan;
http://news.bbc.co.uk/hi/english/sci/tech/newsid_1916000/1916655.stm

COMPUTER CRIME WAY UP, SAYS FBI
Eighty-five percent of respondents report having been victims of computer crime, costing them millions of dollars, according to a survey by the Computer Security Institute and the FBI. The study, which polled 583 computer security experts in business, government agencies, medical institutions and universities, concluded that the most serious losses stemmed from theft of proprietary information. In addition, almost all of the organizations had suffered from computer virus attacks last year, and 90% said they had been victims of Web site defacement in 2001, up from 64% a year earlier. "Organizations that want to survive in the coming years need to develop a comprehensive approach to information security, embracing both the human and technical dimensions," says Patrice Rapalus, director of the Computer Security Institute. In response to the growing threat of cybercrime, the FBI has set up the National Infrastructure Protection Center and has formed regional Computer Intrusion Squads in several offices throughout the U.S. (BBC Online 8 Apr 2002)

Category 31.1 Surveys, studies, audits of security

2002-05-15 **data overload productivity study research report signal-to-noise ratio social interaction worklow tools utility saturation**

NewsScan

DATA DYSPEPSIA
The quantity of information flowing into your office on a daily basis has reached an officially indigestible level, says Gartner, which reports that 90% of companies are suffering from data overload to the point where it's affecting their productivity. Gartner estimates that businesses will spend as much as $30 billion this year alone on information management systems in the hope of digging out, but it still may not be enough to improve the signal to noise ratio in most offices. Surprisingly, Gartner found that the most useful information employees receive comes from personal contacts, contact with friends and colleagues and e-mails, rather than the corporate Intranet. The company has therefore recommended that businesses encourage more social interaction -- in cafeterias, lounges and around the water cooler -- while at the same time implementing workflow tools that can help stem the tide of useless information. (The Register 15 May 2002)
http://www.theregister.co.uk/content/23/25283.html

Category 31.1 *Surveys, studies, audits of security*

2002-05-30 **software piracy stealing attitudes beliefs survey study ethics morality**

NewsScan

IS STEALING WRONG ALWAYS, OFTEN, SOMETIMES, OR NEVER?
A new survey commissioned by the Business Software Alliance indicates that more than 50% of Americans who use the Internet regularly download commercial software without paying for it -- and that only 12% think that what they're doing should be considered piracy. Other depressing findings for software developers were that 43% of the survey respondents strongly agreed with the statement: "It makes no sense to charge me hundreds of dollars per user license vs. pennies to reproduce," and 22% somewhat agreed with: "The technology industry is so prosperous that a few people using unlicensed software won't make any difference." On the other hand, the modestly good news for developers is that 54% of respondents strongly agreed with the statement: "People that develop software deserve to be rewarded for their efforts." (San Jose Mercury-News 29 May 2002)
http://www.siliconvalley.com/mld/siliconvalley/3363169.htm

Category 31.1 *Surveys, studies, audits of security*

2002-06-04 **e-commerce Web design usability study survey**

NewsScan; http://news.com.com/2100-1017-931274.html

E-COMMERCE SITE DESIGN IS *SLOWLY* IMPROVING
A new study by the Nielsen Norman Group that examined 15 e-commerce Web sites, including those of Martha Stewart, L.L. Bean and Office Depot, indicates that their usability quotient is increasing, but only slightly. A similar study conducted two years ago concluded that the sites met an average of 45% of the group's usability guidelines; that percentage is now 49%. "If we continue at this rate for the next 15 years, we will reach a level that we really want to be at," says Jakob Nielsen. "Fifteen years is a long time to wait to get good services on the Internet, but in the big picture, this is a new technology, and whenever anything else was invented, it took awhile to get it right." Among the sites studied this year, L.L. Bean came in on top, meeting 66% of the 207 usability guidelines. The guidelines cover everything from whether a site's product search engine can handle misspellings to whether a site requires a customer to select a state as part of their information profile -- something foreign visitors can't do. (CNet News.com 3 Jun 2002)

Category 31.1 *Surveys, studies, audits of security*

2002-06-06 **survey financial costs QA quality assurance software testing research report**

RISKS; http://www.nist.gov/director/prog-ofc/report02-3.pdf 22 11

NIST engaged the Research Triangle Institute (RTI) to assess the cost to the U.S. economy of inadequate software testing infrastructure. Inadequate testing is defined as failure to identify and remove software bugs in real time. Over half of software bugs are currently not found until downstream in the development process leading to significant economic costs. RTI identified a set of quality attributes and used them to construct metrics for estimating the cost of an inadequate testing infrastructure. Two in depth case studies were conducted. In the manufacturing sector, transportation equipment industries were analyzed. Data were collected from software developers (CAD/CAM/CAE and product data management vendors) and from users (primarily automotive and aerospace companies). In the service sector, financial services were analyzed with data collected again from software developers (routers and switches, financial electronic data interchange, and clearinghouse) and from users (banks and credit unions). …. [T]he annual cost to these two major industry groups from inadequate software infrastructure is estimated to be $5.85 billion. Similarities across industries with respect to software development and use and, in particular, software testing labor costs allowed a projection of the cost to the entire U.S. economy. Using the per-employee impacts for the two case studies, an extrapolation to other manufacturing and service industries yields an approximate estimate of $59.5 billion as the annual cost to the nation of inadequate software testing infrastructure.

Category 31.1 *Surveys, studies, audits of security*

2002-06-12 **survey study online business e-commerce growth**

NewsScan; http://online.wsj.com/article/0,,SB1023828339638741520.djm,00.html (sub req'd)

MAIL-ORDER/E-TAIL HYBRIDS LEAD E-COMMERCE INTO THE BLACK
Online retail sales rose 21% last year to $51.3 billion and are expected to grow by 41% to $72.1 billion this year, with mail-order catalogue companies racking up the most revenues. "What was remarkable to me is that the online portion of retail continued to grow, not at the same pace as in the past, but still solid improvement in a pretty dismal year," says Elaine Rubin, chairman of Shop.org, which commissioned the study by Boston Consulting Group and Forrester Research. The report predicts that the Internet retailing category as a whole will break even on an operating basis for the first time this year. Catalogue companies, like L.L. Bean and Lands' End, are leading the pack, showing a 6% operating margin last year, excluding interest and taxes. Meanwhile, bricks-and-mortar retailers showed a -5% operating margin last year, while Web-only companies had a -13% operating margin. Online retailing as a whole continues to represent only a sliver of total retail sales -- 2.4% last year and an anticipated 3.2% this year. However, in specific markets, such as computer hardware and software sales, e-tailing has made significant inroads, accounting for 17.9% of those sales last year, rising to a projected 23.4% this year. (Wall Street Journal 12 Jun 2002)

Category 31.1 *Surveys, studies, audits of security*

2002-06-14 **music piracy intellectual property economic effects sales increase**

NewsScan

MUSIC DOWNLOADERS MAY BE RECORD LABELS' BEST CUSTOMERS
Four out of five people who download music from the Internet report that their CD purchasing frequency either remained the same or increased, according to a new study by Ipsos Reid that concludes downloading music and burning CDs may actually stimulate legitimate sales. The research backs up an earlier study by Jupiter Media Metrix that concluded people using file-sharing networks were more likely to spend money on music. "While the goal of this was not to draw a link between file sharing, CD burners and the slump in music sales, we can see that American music enthusiasts are becoming increasingly acquainted with the flexibility that digital music allows," says a senior research manager at Ipsos Reid. "As a result, (American consumers) may be more apt to venture beyond the traditional channels of music distribution as part of their audio behaviors." (Wired.com 14 Jun 2002)
http://www.wired.com/news/mp3/0,1285,53157,00.html

Category 31.1 *Surveys, studies, audits of security*

2002-06-17 **telecommuting confidentiality tunneling VPN encryption productivity**

NewsScan

TELECOMMUTING STILL GAINING IN POPULARITY
The number of U.S. workers toiling at home three or more days a week rose nearly 23%, from 3.4 million in 1990 to 4.2 million in 2000, according to U.S. Census figures. Meanwhile, the estimated number of workers who telecommute at least some portion of the week jumped more than 42% in two years, from 19.6 million in 1999 to 28 million in 2001, according to the International Telework Association and Council (ITAC). Most telecommuters live in New England and on the East and West coasts in areas with dense population and notorious traffic congestion, and more than two-thirds of telecommuters polled for an ITAC survey expressed satisfaction over their at-home worker status. "They're saying, 'This is three hours I don't need to be in the car, and I could be with my kids, pick (up) the dry cleaning, or whatever,'" says ITAC president Tim Kane. A formal E-Worker program instituted two years ago at Cigna Corp. has seen productivity increases of up to 15% among teleworkers while job turnover rates in some divisions of the company were cut in half. (AP 16 Jun 2002)
http://apnews.excite.com/article/20020616/D7K6EEM00.html

Category 31.1 *Surveys, studies, audits of security*

2002-07-01 **PC workstation personal computer sales broadband digital divide**

NewsScan

PC SALES HIT THE 1 BILLION MARK
Approximately 1 billion PCs have been shipped worldwide since the mid-1970s, according to a new Gartner report, which predicts the next billion sales won't take nearly as long. Thanks to declining prices, the growth of the Internet, and the rapid adoption of computers in the developing world, the number of PCs shipped likely will double by 2007 or 2008. In addition, broadband proliferation is expected to boost shipments, with studies showing that broadband subscribers in the U.S. use their PCs more often and for more functions than do consumers with dialup accounts. "This demand exists because of the power of the PC to leverage intellectual capital, unlocking the capabilities of individuals to succeed and companies to profit," says the report. "However, expanding the market will require that PCs become smaller and even less expensive than they are today, while delivering greater functionality and performance," says the study. About 80% of the computers shipped to date have been desktop models, while notebooks have accounted for 16% of sales. (CNet News.com 30 Jun 2002)
http://news.com.com/2100-1040-940713.html?tag=fd_top

Category 31.1 *Surveys, studies, audits of security*

2002-07-05 **search engine e-mail user utilization popularity**

NewsScan

SEARCHING, NOT SURFING, IS NO. 1 NET ACTIVITY
Internet users increasingly are focusing their computer time on finding specific information via search engine, rather than aimlessly clicking from one site to the next, according to new statistics collected by the Pew Internet Project. More than 80% of all U.S. users have employed a search engine, and 29% of respondents turn to search engines every day to locate information online. Among Internet users who've been online for three years or more, the percentage of daily search engine users rises to 40%. The only activity more popular than searching is e-mail, which 52% said they did on a daily basis. The survey results indicate that people are learning to trust the results produced by search engines, and tend to rely on them rather than scouring the Web on their own. Google ranked No. 1 in popularity, based on the average number of minutes people spend using it per month. (BBC News 5 Jul 2002)
http://news.bbc.co.uk/hi/english/sci/tech/newsid_209700

Category 31.1 *Surveys, studies, audits of security*

2002-07-08 **criminal hackers crackers attacks report infowar information warfare Internet targets**

NewsScan

DOROTHY DENNING SAYS SURFCRACKERS FOLLOW THE MONEY
Renowned cybersecurity expert Dorothy Denning, a Georgetown University professor whose expertise includes information warfare, is not very surprised by a new report showing a 28% increase in the last six months in Internet attacks targeting technology, financial services and power companies: "In the hacker community, you are going to score more points for hitting bigger companies. There is also an economic gain to going after the large financial services targets -- they have the money." The report, prepared by Alexandria, Va.-based security firm Riptech Inc., found more than 180,000 successful Internet attacks between January and June 2002. (Washington Post 7 Jul 2002)
http://www.washingtonpost.com/wp-dyn/articles/A36498-20

Category 31.1 *Surveys, studies, audits of security*

2002-08-01 **information value cost consumer contracts Web economics e-commerce**

NewsScan

INFORMATION WANTS TO BE PAID FOR
A new survey by the Online Publishers Association has found that in 2001 consumers spent nearly double in online purchases what they had spent the year earlier. Not surprisingly, people are most willing to pay money for business and financial information, because that kind of information influences their livelihood -- but beyond that there is a more general trend toward increased consumer willingness to pay for online content. One example: there are now more than a million subscribers to the online greeting card company American Greetings.com, which charges $11.95 a year for virtual cards. Its chief executive says: "In the past five years, we trained customers that content was free -- that was our fault." And now? "Slowly but surely, people are paying for content." (New York Times 1 Aug 2002)
http://www.nytimes.com/2002/08/01/technology/01ONLI.h

FOUR FLORIDA NEWSPAPERS TO CHARGE FOR WEB ACCESS
Four newspapers in the Florida Panhandle, all four owned by Freedom Communications, have decided to start charging for access to their Web sites. Freedom's chief executive says: "We felt there's value to the content and we should get something for the value of the content." The editor of one of the papers adds: "People who work expect to get paid, whether they deliver information or they deliver pizzas." The newspapers have received a barrage of complaints from their readers for the move they've taken. (AP/New York Times 4 Aug 2002)

Category 31.1 *Surveys, studies, audits of security*

2002-08-14 **intellectual property music sales piracy study**

NewsScan

BLAME THE ECONOMY, NOT PIRACY, FOR WEAK CD SALES
A Forrester Research report released Tuesday [Aug 13] says that the true threat to record labels' profits is the sagging economy, and that downloadable music could actually prove to be the industry's salvation rather than its scourge. According to the report's findings, people who download music from the Internet more than nine times a month -- a relatively small percentage of the overall market -- say they'll decrease their album purchases by 2%. At the same time, 39% of downloading enthusiasts said they bought more CDs, because they found new music that they wanted to purchase through their file-swapping activities. Meanwhile, it turns out that consumers who rarely or never download music account for more than two-thirds of CD sales in the U.S. With music sales slumping nearly 10% this year so far, report author Josh Bernoff says the true culprits are limited radio playlists, high-priced CDs and a general economic recession. The Forrester report suggests that record labels should offer more flexible pricing and online access to their entire music back-catalogues in order to make online music-buying more consumer-friendly. The predicted payoff (which some view as excessively optimistic) could amount to a boost of $937 million in album downloads, $805 million in singles downloads and $313 million in subscription fees by 2007. (Los Angeles Times 14 Aug 2002)

Category 31.1 *Surveys, studies, audits of security*

2002-08-20 **information warfare infowar homeland defense backup antivirus survey**

NewsScan

SMALL BUSINESSES SHORE UP THEIR CYBERSECURITY DEFENSES
A Computer Economics survey of 233 U.S. corporations by has found that since September 11 about 77% of businesses have improved their defenses against network vandals, viruses and other cyberattacks. Although smaller firms typically have the most reluctance to hire full-time security professionals, Computer Economics says that companies with less than $1 million in annual revenue represent the biggest proportion of companies that have improved their security with anti-virus programs and backup equipment during the past year. (USA Today 19 Aug 2002)

Category 31.1 *Surveys, studies, audits of security*

2002-08-27 **intellectual property music sales piracy study**

NewsScan

LABELS CLAIM DOWNLOADING CUTS INTO CD SALES
In contrast with the findings of a recent Forrester Research study [see entry for 2002-08-14], the Recording Industry Association of America has unveiled its own study that claims Internet users who say they are downloading more music are also buying fewer CDs. "Among people who said their downloading from file-sharing services had increased over the past six months, 41% reported purchasing less music now than six months ago, compared to only 19% who said they were purchasing more music," the RIAA said in a statement. Jonathan Potter, executive director of the Digital Media Association, downplayed the utility of studies such as the RIAA's. "The way to defeat illegal music distribution services is to offer comprehensive, innovative, fairly priced legal services. Until the record companies offer their content ubiquitously in a consumer-friendly way, studies like this are useless." In response to record labels' complaints that it's unfair to expect them to compete successfully in selling a music subscription service when fans can get the same songs for free, Potter says, "I'd like to introduce the recording industry to something called bottled water? The point is if there were a high-quality product that was affordable and available across multiple services, they would be able to defeat the free services." (Reuters/CNet 26 Aug 2002)
http://news.com.com/2100-1023-955397.html?tag=fd_top

Category 31.1 *Surveys, studies, audits of security*

2002-08-28 **online sales survey study growth e-commerce**

NewsScan

ONLINE RETAIL SOARS 24%
Online retail sales jumped 24% in the second quarter in year-over-year results from the same period in 2001, according to a report from the U.S. Census Bureau that defies the conventional view of e-commerce as a struggling sector. In fact, while online retail grew 24%, total retail grew by only 2.5%, year-over-year. Leading the numbers, which did not include sales from online travel, finance and ticketing sites, were books and apparel. Aggressive moves by Amazon and Barnes & Nobles to offer free shipping have boosted online book sales and J.Crew recently reported that it continued to take in more revenue through its Web site than it did over the phone -- a milestone reached last February. "It wasn't a blip," says a Jupiter Media Metrix analyst Ken Cassar. And what's ahead? With the threat of recession looming, third quarter sales are expected to taper off a bit, but the fourth quarter -- traditionally the strongest -- is expected to be huge. According to Jupiter, the percentage of consumers' holiday purchases bought online is growing every year. (Business 2.0 26 Aug 2002)

Category 31.1 *Surveys, studies, audits of security*

2002-09-06 **Internet Web monitoring surveillance content filntering e-mail**

NewsScan

ATTITUDES ABOUT RESTRICTIONS OF INFORMATION ON THE WEB
An opinion survey conducted by the Pew Internet and American Life Project found that two-thirds of Americans think it's appropriate for government agencies to exclude some information from their Internet postings, and about half think it's all right for government to monitor Web and e-mail activities. David Greene of the First Amendment Project in Oakland, California, worries: "It certainly is significant that our society which has always prided itself on open access of information is now so scared of what open access to information means. People think, 'I'm not going to poison the water system, so what do I need to know about the water supply system?' But if all of a sudden they are part of an effort to restrict development of a watershed and need that data ... all of a sudden it's important." (AP/San Jose Mercury News 5 Sep 2002)

Category 31.1 *Surveys, studies, audits of security*

2002-10-01 **Internet sociology culture effects influence democracy culture digital divide research clearinghouse center projects**

NewsScan

NEW INSTITUTE EXAMINES INTERNET'S IMPACT
The Oxford Internet Institute opened its doors last week — one of the world's first research centers dedicated to studying the Internet and its social consequences. The Institute is structured as a multidisciplinary organization that will house its own teaching staff, carry out its own research, and act as a collection point and clearinghouse for Internet research projects. Institute director Bill Dutton notes that the Internet is already profoundly changing many social relationships: "The fundamental implication of changes in information technology is that it reconfigures access. Not just in terms of the digital divide but also who you know, what you know and what you get access to and use." Meanwhile, Eli Noam, professor of economics and finance at Columbia University, warns against simply assuming that the Net is a force for good all by itself and needs no outside guidance. He notes that rather than flattening social structures and breaking down barriers, today's Internet is concentrating information in the hands of smaller groups. "We need academics to be leaders, not cheerleaders. We must save the Internet from its founding myth that it is good for democracy and is open and cannot be regulated." (BBC News 1 Oct 2002)
http://news.bbc.co.uk/1/hi/technology/2288598.stm

Category 31.1 *Surveys, studies, audits of security*

2002-10-23 **copyright intellectual property software piracy Asia**

NewsScan

SOFTWARE PIRACY IN ASIA
Microsoft senior corporate attorney Katherine Bostick says that software piracy is increasing throughout the world and especially in Asian countries such as China, Taiwan, Hong Kong, Malaysia and Indonesia. "It involves organized crime," says Bostick. "When you are dealing with high-end counterfeits, you are talking about organizations that have a full supply chain, a full distribution chain, full manufacturing tools all in place, and it is all based on profits." How bad is the situation? "Two out of five business software applications were pirated in 2001, which is the second consecutive year that the piracy rate has increased." And why is it happening? "Right now, the cost of violating intellectual property rights is not that high. There is really no penalty for that major person and they will be right back in business the next day or the next month." (Reuters/San Jose Mercury News 23 Oct 2002)

Category 31.1 *Surveys, studies, audits of security*

2002-11-03 **online music sales copyright intellectual property piracy survey study**

NewsScan

ONLINE MUSIC SALES PLUMMET
Statistics from ComScore Media Metrix show that online sales of new music fell 20% in the first half of the year, and 39% for the third quarter. This happened during a period in which online sales for most other categories (such as computer hardware, office equipment and supplies, apparel, consumer electronics, and books) increased over last year's figures. ComScore president Peter Daboll says, "People are buying less and burning more. I'd be worried if I was selling music." (USA Today 3 Nov 2002)

Category 31.1 *Surveys, studies, audits of security*

2002-11-22 **Internet usage digital divide study survey growth e-commerce international**

NewsScan

GLOBAL NET USE CONTINUES TO BOOM
Despite the current economic gloom and the sharp contraction of the technology industry over the past couple of years, global use of the Internet continues to soar and e-commerce is expanding at a robust pace, according to this year's "E-Commerce and Development Report" issued Monday by the U.N. Conference on Trade and Development. The annual study predicts that the value of goods and services sold over the Net could reach as high as $2.3 billion this year, a 50% rise from last year, and could go as high as $3.9 billion by the end of 2003. Meanwhile, m-commerce is forecast to generate revenues of almost $50 billion in 2002, with Western Europe and North America leading that market for the next three years. The report cites SMS, or text messaging, as the dominant driver of m-commerce revenues, followed by micro-payments, financial services, logistics, information services and wireless customer relationship management. However, concerns over security and difficulties in making electronic payments are "limiting the conduct of m-commerce," warns the report. (PCWorld.com 21 Nov 2002)
http://www.pcworld.com/news/article/0,aid,107219,00.asp

Category 31.1 *Surveys, studies, audits of security*

2002-12-09 **e-mail deluge overload survey study myth**

NewsScan

SURVEY DEBUNKS MYTH OF THE E-MAIL DELUGE
The latest study from the Pew Internet and American Life Project indicates that reports of massive e-mail volume swamping workers and sapping their productivity are greatly exaggerated: in fact, 60% of Americans who use e-mail at work receive 10 or fewer messages on the average day, and three-quarters reported spending an hour or less daily dealing with e-mail. Only 6% reported receiving more than 50 e-mails a day, and among those, only 11% said the volume posed a problem. Most workers who receive a lot of e-mail have devised ways to manage the load, such as using filters to automatically sort the mail into folders. "All of the anecdotal evidence you hear from people out there is, 'I'm so overwhelmed by the volume of e-mail. The perception comes from the people who are talking most loudly about it, those few who are most overwhelmed," says Pew senior research fellow Deborah Fallows. The pattern is different for power users, typically those in high-level managerial positions at large corporations. Many of them spend at least two hours daily on e-mail, with the task often stretching out to four or more hours. Meanwhile, the study found that younger users (those under 30) are more likely to use e-mail for personal use while at work, often sending gossip, jokes and chain letters while on the job. (AP 8 Dec 2002)
http://apnews.excite.com/article/20021208/D7NPSN680.htm

Category 31.1 *Surveys, studies, audits of security*

2002-12-11 **broadband Internet access cable International trends study**

NewsScan

DSL GROWTH SURGES TO RECORD HIGH
The number of consumers signing up for DSL (digital subscriber line) service increased nearly 20% between July 1 and September 30 over the previous three-month period — an unprecedented growth rate, according to a DSL Forum survey. Findings indicate there are now about 30 million DSL users globally, although in the U.S. cable modem users still outnumber DSL subscribers about 2 to 1. "In the U.S., (cable modem providers) are beating the hell out of us," says DSL Forum chairman William V. Rodey. "But globally, we're beating the hell out of them." Outside the U.S. there are only about 5 million cable modem customers, while foreign DSL subscribers number about 22.5 million. Tops in DSL subscriber numbers is the Asia-Pacific region (with South Korea ranking highest), followed by Europe (thanks to strong growth in Germany, Norway and Croatia), with the U.S. coming in third. (CNet News.com 10 Dec 2002)
http://news.com.com/2100-1033-976791.html

Category 31.1 *Surveys, studies, audits of security*

2003-01-23 **identity theft statistics growth reports**

NewsScan

IDENTITY THEFTS DOUBLED LAST YEAR
The number of identity thefts doubled in 2002, with 162,000 reports of identity theft compared to 86,000 the previous year. However, the Federal Trade Commission says that the rise in identity theft complaints does not necessarily mean an increase in actual crimes — it may simply reflect an increasing public awareness of the problem and a greater likelihood that such incidents are now being reported. But an official of the Michigan State Police points out that many former violent criminals are now using the Internet for identity theft: "They are switching over to white-collar crime because it's more lucrative and they know they will get less time. Identity theft is not necessarily a sophisticated crime." (New York Times 23 Jan 2003)

Category 31.1 *Surveys, studies, audits of security*

2003-01-28 **cellular mobile telephone driving danger attention study**

NewsScan

CELL PHONE USE CAN IMPAIR VISION WHILE DRIVING
Researchers at the University of Utah have found that drivers using cell phones, even hands-free devices, experience a decrease in the ability to process peripheral vision, creating a potentially lethal "tunnel vision." This "inattention blindness" slows reaction time by 20% and resulted in some of the 20 test subjects missing half the red lights they encountered in simulated driving. "We found that when people are on the phone, the amount of information they are taking in is significantly reduced," says associate professor David Strayer. "People were missing things, like cars swerving in front or sudden lane changes. We had at least three rear-end collisions." The Utah study is only the latest investigation into the effects of driving and cell phone use, and most of the others have also demonstrated some degree of impairment. And while most studies have focused on the distractions of dialing or holding a phone, the Utah research tried to focus on the distractions caused by having a conversation. New York is the only state to have instituted laws against the practice, but 30 more states have similar legislation pending. (CNet News.com 27 Jan 2003)
http://news.com.com/2100-1033-982325.html

Category 31.1 *Surveys, studies, audits of security*

2003-02-03 **criminal hacker attacker vulnerabilities survey study**

NewsScan

CYBER ATTACKS DOWN, VULNERABILITIES WAY UP
The level of cyber attacks dropped for the first time in the second half of 2002, falling by 6%, according to Symantec's Internet Threat Report. But at the same time the number of vulnerabilities shot up significantly, with 2,524 new vulnerabilities reported in 2002, 81.5% over 2001. Power and energy companies saw the highest level of hacking and cracking attempts over the last six months of last year, with financial companies second. South Korea was cited as the source of many of the attacks, both because of the increased use of broadband Internet access in the country, as well as its usefulness as a hopping-off point for hackers. Hacking incidents from South Korea grew 62% between July and December last year. (The Register 3 Feb 2003)
http://www.theregister.co.uk/content/55/29149.html

Category 31.1 *Surveys, studies, audits of security*

2003-02-04 **cyber attacks hacking Internet vulnerability report**

NIPC/DHS

February 03, eWeek — Cyber attacks decline; vulnerabilities surge.

The number of attacks on Internet-connected machines decreased over the past six months while the number of software vulnerabilities continued to skyrocket, according to a new report. This supports the conventional wisdom that most attackers search for a few vulnerabilities to exploit and will abandon their efforts if these vulnerabilities are unavailable," the report concludes. The report, published by Symantec Corp., of Cupertino, Calif., is based on data from more than 400 companies. The company said it recorded more than 2,500 newly identified vulnerabilities in various software products during all of 2002, an 81.5 percent increase over the previous year. Several factors may have contributed to this increase, including the huge jump in recent years in the number of researchers looking for vulnerabilities. Once again, attackers in the United States were by far the most eager to exploit those vulnerabilities and accounted for more than 35 percent of all of the attacks during the reporting period. South Korea, China, Germany and France rounded out the top five. However, the South Koreans appear to have the most attackers per capita among countries with the largest online populations, launching 23.7 attacks per 10,000 Internet users. The U.S. is not in the top 10 on this list.

Category 31.1 *Surveys, studies, audits of security*

2003-02-04 **network attacks vulnerabilities corporate increase rise fall vulnerabilities**

NewsScan

RISING NUMBER OF NETWORK ATTACKS AND VULNERABILITIES
The Internet security firm Symantec says that the number of cyber attacks on corporate networks rose 20% in the second half of last year compared to the same period the previous year. The good news, though, is that the number actually declined by 6% compared to the first six months of 2002. The number of vulnerabilities to such attacks jumped 81%, comparing the last half of 2002 to the last half of the previous year; however, Symantec chief technology officer Robert Clyde noted that the increased number of vulnerabilities may be largely the result of a greater tendency of companies to admit their problems: "It could be that more vendors are reporting vulnerabilities as they are patched." (Reuters/San Jose Mercury News 4 Feb 2003)

Category 31.1 *Surveys, studies, audits of security*

2003-02-11 **cyber terrorism cyberspace threats infrastructure protection international**

NIPC/DHS

February 07, Medill News Service — Don't underestimate cyberterrorists, experts warn.

The Internet is becoming a new battleground for warfare, according to experts concerned about the potential of a cyberattack to cripple the public infrastructure. The recent Slammer worm, which blocked Internet traffic and crippled some corporate networks for most of a weekend, is just a watered-down version of a cybercrisis that could disrupt everything from banks to water supplies, critics say. In the Mideast conflict, pro-Palestinian hackers have successfully taken down Web sites of the Israeli Parliament, the Israeli Defense Force, the Foreign Ministry, the Bank of Israel, the Tel Aviv Stock Exchange, and others, according to a report by Dartmouth College's Institute for Security Technology Studies. Dartmouth's study charts how political cyberattacks often precede physical attacks. Cyberattacks after U.S.-led military action are "extremely likely" and could possibly be catastrophic, according to the report. Information systems—like electrical infrastructures, water resources, and oil and gas—should be considered likely targets, it warns. While cyberattacks can take a variety of forms and may originate from terrorist groups or targeted nation states, they are more likely to be launched by sympathizers or thrill-seekers, according to the institute's report.

Category 31.1 *Surveys, studies, audits of security*

2003-03-07 **survey forecast US firms disaster recovery business continuity unprepared calamity**

NIPC/DHS

March 04, eSecurity Planet.com — Survey says U.S. Firms unprepared for disasters.

A large percentage of U.S. companies are unprepared to face business and IT outages caused by a severe calamity, according to the results of a survey released by research firm Gartner Dataquest Tuesday. The survey found that one third of U.S. businesses face the loss of critical data or operational capability in the wake of a disaster, unless investments toward disaster preparedness planning are made. Tony Adams, principal analyst for Gartner Dataquest's IT Services group, said "Preparation is the key, and without adequate investment for protection of critical systems, the repercussions of disasters will be lengthier and more costly." But cost is one of the primary reasons many of the companies surveyed cited for not having a disaster preparedness plan. "IT managers are not investing appropriately in disaster plans because they do not have a budget to accomplish their needed readiness," Adams said. Most disaster preparedness experts say that sophisticated real-time remote backup capabilities are the foundation of disaster recovery plans. In other words, it's all about redundancy. In the wake of September 11, 2001, Lee Clarke, associate professor of Sociology at Rutgers University — and an expert in organizations, technology and disasters — told Internetnews.com that the redundancy must be "meaningful." For instance, Clarke noted that many of the organizations in the World Trade Center had their disaster facilities in one of the other towers or buildings that were part of the complex.

Category 31.1 *Surveys, studies, audits of security*

2003-03-17 **NIST NSA security configuration IT profile document**

NIPC/DHS

March 10, Government Computer News — NIST and NSA draft safe-IT profiles.

The National Institute of Standards and Technology (NIST) has partnered with the National Security Agency (NSA) to draw up Protection Profiles-basic security recommendations for 10 hardware and software areas. NSA also is developing implementation guides for configuring operating systems securely. A 2,000-page guide for Microsoft Windows 2000 is finished, and a guide for Windows XP is in beta evaluation, said William Billings, chief of operational network evaluation for NSA's Systems and Network Attack Center. In addition, the Defense Information Systems Agency's (DISA) soon-to-be-released Gold Disk tool will apply security configurations to operating systems. The Gold Disk is part of DISA's Security Technical Implementation Guidelines (STIGs), which parallel the NSA guides. Profile development, which began about two years ago, already is complete for OSes, firewalls, intrusion detection systems, tokens and public-key infrastructures. Profiles should be ready by mid-2003 for wireless systems, browsers, databases, virtual private networks and biometric products.

Category 31.1 *Surveys, studies, audits of security*

2003-03-25 **cyber security lack United States US infrastructure protection**

NIPC/DHS

March 24, Federal Computer Week — States need cybersecurity focus.

A Zeichner Risk Analytics LLC study released today found 36 state governments have failed to prepare, adopt and implement acceptable cybersecurity policies, which could have damaging consequences to citizen services, communication systems and critical utilities if the nation were to undergo cyberattacks. Following a yearlong review, the study found that only 14 states and the District of Columbia are in full compliance with the Gramm-Leach-Bliley Act of 1999, which requires federal agencies and states to prepare cybersecurity guidance for financial institutions. Fourteen other states have pending legislation and/or regulations for compliance, while 22 states have little or no cybersecurity activity. The study recommended that: 1) States adopt the National Association of Insurance Commissioners nationwide proposal, which provides an approach similar to that of states in compliance with the Gramm-Leach-Bailey Act; 2) States create a single, nationwide process for developing cybersecurity laws and policies; 3) A single public-private "focal point is badly needed" to coordinate strategy.

Category 31.1 *Surveys, studies, audits of security*

2003-04-02 **software piracy declines Software Business Alliance**

NewsScan

SOFTWARE PIRACY RATES FALLING WORLDWIDE
A report by the Software Business Alliance and market research firm IDC says that software piracy rates (measured by the amount of business installed without a license) have declined in many countries since 1996: down by 30% in Egypt; 28% in Ireland; 14% in Colombia; 20% in South Korea. Pointing out that reductions in piracy rates lead to increased sales and improved government economies, the authors of the report say that the countries with most to gain from curbing software piracy are ones where the rates are highest: China (92%) and Russia (87%). The U.S. has the lowest piracy rate (25%). (San Jose Mercury News 2 Apr 2003)

Category 31.1 *Surveys, studies, audits of security*

2003-04-03 **critical infrastructure protection challenges Homeland Security**

NIPC/DHS

February 28, General Accounting Office — Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors.

The General Accounting Office has released report GAO-03-233 titled "Critical Infrastructure Protection: Challenges for Selected Agencies and Industry Sectors." With computer interconnectivity comes a threat: both physical and cyber assets are potentially vulnerable to computer-based attack. In response, Presidential Decision Directive 63 (PDD 63, May 1998) called for a range of actions to improve the nation's ability to detect and respond to serious infrastructure attacks. GAO examined four specific agencies—the Departments of Health and Human Services, Energy, and Commerce, and the Environmental Protection Agency—and found that the agencies have made progress in implementing several PDD 63 requirements. However, none of the agencies has fully implemented all requirements. GAO also examined private-sector groups known as Information Sharing and Analysis Centers (ISACs) for five specific industry sectors—information technology, telecommunications, energy, electricity, and water supply. ISACs serve as clearinghouses for their sectors to share information. For other suggested activities, such as establishing baseline statistics on computer security incidents, progress is mixed. Both the agencies and the ISACs identified challenges and obstacles to undertaking CIP activities. Agency-identified challenges included coordinating security efforts for critical assets with the General Services Administration, which may often be responsible for protecting agency facilities that house critical assets. The ISACs identified obstacles to information sharing, both between the sectors and the government and within the sectors. In particular, they noted concerns that information reported to the government could be subject to public release under the Freedom of Information Act.

Category 31.1 *Surveys, studies, audits of security*

2003-04-07 **warning survey study Web server Microsoft Internet Information Server vulnerability HTTP Netcraft**

NIPC/DHS

April 02, Security News Portal — 75% of all web servers running MS IIS 5.0 are vulnerable to exploitation.

Three-quarters of web sites running Microsoft's Internet Information Server 5.0 software to serve web pages have the WebDAV protocol enabled and thus remain open to a serious vulnerability which was announced by Microsoft last month, the latest web server survey from Netcraft says. Microsoft issued a security alert on March 17 regarding a buffer overflow vulnerability which allows attackers to execute arbitrary code on Windows 2000 machines. The survey found 767,721 IPs running IIS 5.0 and offering WebDAV and 273,496 IPs running IIS 5.0 with the protocol turned off. The monthly survey looks at web server software usage on internet-connected computers, collecting and collating as many hostnames as can be found providing an HTTP service. Each is systematically polled with an HTTP request for the server name. The March survey received responses from 39,174,349 sites. Additional information may be found on the Netcraft Website: http://news.netcraft.com/archives/2003/03/

Category 31.1 *Surveys, studies, audits of security*

2003-04-09 **Internet fraud crime triples**

NewsScan

INTERNET FRAUD COMPLAINTS TRIPLE
Complaints about fraudulent schemes perpetrated over the Internet tripled in 2002 from the previous year, with the most common grievance being auction fraud, followed by non-delivery of promised merchandise, credit card fraud and fake investments. According to a report from the Internet Fraud Complaint Center, which is run by the FBI and the National White Collar Crime Center, the 48,252 complaints referred for prosecution in 2002 represent only a fraction of the crimes authorities believe are occurring. The center also received almost 37,000 other complaints that did not constitute fraud, but involved such things as spam, illegal child pornography and computer intrusions. The report says 80% of known fraud perpetrators and about 71% of complainants are male. Fraud complaints originated in all parts of the country, with a third coming from California, Florida, Texas and New York. One of the most persistent scams described in the report is the infamous "Nigerian letter," which urges victims to pay an upfront fee (characterized as a bribe to the government) in order to receive non-existent funds from the "Government of Nigeria." There were 16,000 complaints related to that scam in 2002, up from 2,600 in 2001. (AP 9 Apr 2003)

Category 31.1 *Surveys, studies, audits of security*

2003-04-10 **critical infrastructure protection information security progress report**

NIPC/DHS

April 08, The General Accounting Office — Information Security: Progress Made, But Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures.

On April 8, the General Accounting Office (GAO) published report GAO-03-564T titled "Information Security: Progress Made, But Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures." Significant information security weaknesses at 24 major agencies continue to place a broad array of federal operations and assets at risk of fraud, misuse, and disruption. Although recent reporting by these agencies showed some improvements, GAO found that agencies still have not established information security programs consistent with the legal requirements. For example, periodic testing of security controls is essential to security program management, but for fiscal year 2002, 14 agencies reported they had testing the controls of less than 60 percent of their systems. Further information security improvement efforts are also needed at the governmentwide level, and these efforts need to be guided by a comprehensive strategy in which roles and responsibilities are clearly delineated, appropriate guidance is given, adequate technical expertise is obtained, and sufficient agency information security resources are allocated.

Category 31.1 *Surveys, studies, audits of security*

2003-04-14 **Federal Bureau Investigation FBI technology investment return Interner crime fraud thwart security privacy**

NIPC/DHS

April 10, National Journal — FBI director says tech investments are paying off.

FBI Director Robert Mueller on Thursday highlighted the bureau's success in thwarting terrorist attacks, counterintelligence operations and confronting cyber crime in his budget presentation to the Senate Commerce, Justice and State Appropriations Subcommittee. After counterterrorism and counterintelligence, Mueller said that tackling cyber crime was the bureau's third priority area. "Unfortunately, we are seeing explosive growth in cyber crime-both traditional crimes such as fraud and copyright infringement that have migrated online, and new crimes like computer intrusions and denial of service attacks," he said. Over the past six years, the number of such cases grew from 113 to 2,300. The FBI's Cyber Program would "focus on identifying and neutralizing: 1) individuals or groups conducting computer intrusions and spreading malicious code; 2) intellectual property thieves; 3) Internet fraudsters; and 4) online predators that sexually exploit or endanger children," he said. The agency has been consolidating those operations into a new Cyber Division at its headquarters, and its total budget request for fiscal 2004 is $234 million to protect against cyber-based attacks and high-tech crimes, including 77 new agents.

Category 31.1 *Surveys, studies, audits of security*

2003-04-17 **Internet Insecurity Index RSA study survey statistics mathematics**

NIPC/DHS

April 15, AtNewYork.com — "Internet Insecurity Index" unveiled at conference.

Online encryption firm RSA Monday launched its "Internet Insecurity Index" — a simple one-to-ten scale that measures how secure electronic data is each year. Given the amount of attacks, Jim Bidzos of RSA currently ranks 2003 at about a 6 and a half. Bidzos pointed to more than 62,000 hacking incidents last year as a rally cry for better safeguards. In addition to commonplace server strikes, Bidzos said ATM and wireless networks are the new target of hackers. "Part of the price is not having security designed in the first place," Bidzos said. "We found 30 percent of ISPs have no info security plans in place with 33 percent deciding that online security is not a priority." The threat index also identifies last year's $59 billion in data theft as a major impact on how safe the Internet is. The one bright area, according to RSA's index report was the U.S. government. Bidzos said the creation of the Department of Homeland Security and a national strategy to secure cyberspace marked a turning point in how the government is dealing with online threats. California's move to require companies to publicly disclose security breaches may also have a major impact on how well companies secure their networks and data.

Category 31.1 *Surveys, studies, audits of security*

2003-05-07 **Spam Email virus British ISP BT Openworld monitor 25 million**

NIPC/DHS

May 07, Net4Nowt — BT Email: 41% Spam and 1 in 220 has Virus.

British ISP BT Openworld monitored mails sent by its customers between March 17, 2003 and March 23, 2003. Of more than 25 million emails scanned, nearly 11 million were detected and trapped as spam. This equates to a weekly average of 41 per cent. Thursday was the most popular day for spamming, with more than four million examples detected. Sunday polled the highest percentage of spam with the proportion rising to 51 percent of all messages sent. To make matters worse, the filters also detected over 113,000 viruses - one for every 220 mails sent.

Category 31.1 *Surveys, studies, audits of security*

2003-05-20 **women dominate text-messaging UK competent**

NewsScan

WOMEN DOMINATE TEXT MESSAGING IN UK
A survey by the Mobile Data Association found that a full 74% of female respondents said they'd used text messaging in the last two minutes, compared with 26% of males, and about half the women said they'd prefer receiving a sentimental text message to a card on special occasions. Two-thirds of the women described themselves as test-messaging competent, compared with only a third of the men. Text messaging the UK reached an all-time high in March, when 1.7 billion messages were sent. (BBC News 20 May 2003)

Category 31.1 *Surveys, studies, audits of security*

2003-05-27 **OMB federal IT security Office Management Budget systems progress agencies GISRA**

NIPC/DHS

May 27, Government Computer News — OMB: federal IT security's better but still not good enough.

Agencies have made progress in evaluating and securing systems, but serious and pervasive problems persist, according to the Office of Management and Budget (OMB). OMB released its second report to Congress last month under the Government Information Security Reform Act. The report compares the performance of 14 departments and 10 independent agencies in fiscal 2002 with baseline data collected in 2001. Despite across-the-board improvements in eight areas, more than a third of federal systems overall still have not been assessed for risk and lack up-to-date security plans, and less than half have been certified and accredited for use. The 2001 GISRA report identified government-wide areas of weakness: lack of performance measures and senior management attention, poor security education and awareness, failure to include security in IT capital planning, failure to ensure security of contractor services, and poor information sharing.

Category 31.1 *Surveys, studies, audits of security*

2003-05-29 **cyber-attack survey companies organizations authorities FBI computer crime negative publicity**

NIPC/DHS

May 29, eWEEK — Cyber-attack costs down, says survey.

The percentage of organizations that detected unauthorized use of their systems fell to 56 percent from 60 percent a year earlier, according to the latest "Computer Crime and Security Survey" from the Computer Security Institute and the FBI. The 2003 survey also shows that companies are still failing to report most of their intrusions and attacks to law enforcement. Only 30 percent of the survey's respondents said they had contacted the authorities after an attack, a drop from 34 percent a year ago. Negative publicity and fear that competitors would use the information to their advantage were the top two reasons organizations cited for failing to talk to law enforcement after an attack. Among the most frequently seen attacks, viruses, laptop misuse and unauthorized access by insiders continued to lead the way, according to the survey. The 530 organizations surveyed reported $201.8 million in losses this year; in 2002, 503 respondents lost $455.8 million.

Category 31.1 *Surveys, studies, audits of security*

2003-05-30 **technical errors government sites web bug Business Internet Group San Francisco applications server blank pages content Keynote Systems internal**

NIPC/DHS

May 30, Government Computer News — Study finds technical errors in government sites.

A survey of 41 federal Web sites found that 68 percent will present some sort of bug within the first 15 minutes of a visit, according to the Business Internet Group of San Francisco. Most glitches were application server and Web server errors such as blank pages, embedded content errors and the 500 internal server error, the survey found. Diane Smith, the group's research director, said she selected the sites because they are used in the Keynote Government Internet Performance Index from Keynote Systems Inc. of San Mateo, Calif. The index includes sites of 10 Cabinet departments, the White House, both houses of Congress and several large agencies. Smith said she visited each Web site for up to 15 minutes and explored as if she were unfamiliar with the agency. She stopped exploring at the first error, even if the 15 minutes were not yet up. Twenty-five of the buggy sites had blank pages and internal server errors. Smith said she found three other sites with data errors, such as a wrong page link or bad data returned from a database query.

Category 31.1 *Surveys, studies, audits of security*

2003-06-02 **Software piracy 2002 vietnam russia ukraine indonesia china BSA pirate piracy illegal copy**

NewsScan

SOFTWARE PIRACY DOWN IN 2002
Global business software piracy declined slightly last year, thanks to increased education efforts and more aggressive tactics by the software industry, according to a report released Tuesday by the Business Software Alliance. The study estimates that 39% of business software installed on computers worldwide in 2002 was not legally obtained, with the most common violation being purchasing a single legal copy and installing it on several computers, said Robert Holleyman, president and CEO of the BSA. To combat that scenario, the alliance is continuing to circulate brochures on piracy and is conducting amnesty campaigns urging businesses to pay for additional copies without threat of prosecution. In addition, companies like Microsoft have instituted new restrictions, requiring special activation codes for its software that are tied to a single computer. It's too early to tell how well these strategies have worked in reducing piracy, said Holleyman. The country with the largest percentage of illegal software was Vietnam (95%), followed by China (92%), and Indonesia, Russia and the Ukraine, all at 89%. (AP/Wall Street Journal 2 Jun 2003)

Category 31.1 *Surveys, studies, audits of security*

2003-06-04 **boradband risk vulnerability hackers firewall homeland security**

NewsScan

BROADBAND BROADENS RISK AS WELL AS PERFORMANCE
A study of 120 broadband users conducted by the National Cyber Security Alliance (a group of business and government entities) has found that although 77% think their systems are protected from outside hackers, fewer than 60% had installed firewalls to keep their systems safe. "The disconnect means we have to do more to educate people," says Alliance spokesman Keith Nahigan, who is also a consultant to the national Office of Homeland Security. Despite the vulnerability of their systems, 86% of broadband users keep sensitive information on their computers. Broadband systems are "always-on" and Nahigan notes: "When you have your connection open all day and all night, it's easier for hackers to get in." (New York Times 4 Jun 2003)

Category 31.1 *Surveys, studies, audits of security*

2003-06-09 **kids spam symantec research statistics age study**

NewsScan

KIDS GET SPAMMED, TOO
A new study by Applied Research probably won't surprise anyone, but it does highlight the consequences of the current spam-run-amok Internet culture. According to the research, which was commissioned by Internet security firm Symantec, more than 80% of kids (aged 7 to 18) get "inappropriate" unsolicited commercial e-mail on a daily basis, and their spam looks just like yours: sweepstakes offers (80%), "relationship-related" e-mail (62%), financial come-ons (61%), weight-loss ads (55%), pharmaceutical ads (51%), and, of course, p*rn (47%). Symantec has characterized spam as a new summer hazard, right up there with sunburns and insect bites. Almost half of the 1,000 respondents said they were online more than two hours a day in the summer, compared with only 23% during the school year. (CNet News.com 9 Jun 2003)

Category 31.1 *Surveys, studies, audits of security*

2003-06-12 **spam hackers symantec virus threats**

NewsScan

COMPANIES WORRY MORE ABOUT SPAM THAN HACKERS
Businesses are far more concerned about the rising flood of spam that's engulfing their networks than they are about run-of-the-mill hackers, according to a survey of 2,800 silcon.com readers. But the biggest worry is over virus attacks, with 71% of respondents citing viruses as the biggest threat to their businesses. Symantec's Kevin Chapman says he's not surprised by the results. "Spam has now gone way beyond the quick and easy 'hit the delete button and it's gone' solution. It's now a really big problem. From the employees' point of view it is about productivity and the sheer annoyance of dealing with all these e-mails. For the employer it is about bandwidth and other network resources issues." But aside from productivity and bandwidth concerns, there's another consequence that could be lurking out there, says Martino Corbelli, marketing director for SurfControl. "Some of these spam e-mails have completely inappropriate content which can create serious problems for the employer on a legal basis. There may be somebody who feels they should be protected from p*rnographic content, for example, and in some cases they may be prepared to sue their employer if they feel they are being exposed to offensive material on the company's network." (Silicon.com 12 Jun 2003)

Category 31.1 *Surveys, studies, audits of security*

2003-07-07 **security major universities 80% policy importance hijack school computers launch attacks EDUCAUSE**

NIPC/DHS

July 07, Network World — University net execs face variety of security challenges.

A recent Emory University survey of 13 major U.S. universities found that 80% agreed that network security policies are very important, but only half of them are taking steps to combat the growing flood of security breaches. Staffing and budgeting were cited as the main obstacles. A new worry is the legal liabilities created for a university when someone hijacks a school computer and uses it to launch attacks against networks and computers elsewhere on the Internet. "Desktops and laptops are not professionally administered," says Rodney Petersen, of EDUCAUSE, a nonprofit group focused on advancing higher education through IT. "The freedom to allow faculty, staff, and students to alter system configurations and install software make PCs particularly vulnerable," he says.

Category 31.1 *Surveys, studies, audits of security*

2003-07-09 **NIST security products standardization intrusion detection systems effectiveness analyze systems**

NIPC/DHS

July 09, Washington Technology — NIST: Security products need standardization.

Despite wide use across government, intrusion detection systems have no standard metrics to measure their performance, according to a new report by the National Institute of Standards and Technology. The report "An Overview of Issues in Testing Intrusion Detection Systems" concluded that there are no comprehensive and scientifically rigorous methodologies to test the effectiveness of intrusion detection systems, which monitor and analyze systems and network traffic for possible hacker attackers or misuse. The report may be viewed here:
http://csrc.nist.gov/publications/nistir/.

Category 31.1 *Surveys, studies, audits of security*

2003-07-21 **identity theft crime impersonation fraud credit cards social security**

NewsScan

IDENTITY THEFT: A CRIME THAT PAYS?
The number of victims that have fallen prey to identity thieves is severely underreported, according to a study by Gartner Research, which estimates that 3.4% of U.S. consumers — about 7 million adults — have suffered ID theft in the past year. Moreover, identity thieves generally get away with it — arrests are made in only one out of every 700 cases. "The odds are really stacked against consumers," says Gartner VP Avivah Litan. "Unfortunately, they are the only ones with a vested interest in fixing the problem." Typically, victims of ID theft learn of the crime a year or more later after it happens — long after the trail has gone cold. "It is different from payment fraud, where the thief takes a credit card number and consumers are innocent until proven guilty. With identity theft, it is the opposite: Consumers are thought to be guilty until proven innocent," says Litan. "There is a serious disconnect between the magnitude of identity theft that innocent consumers experience and the [financial] industry's proper recognition of the crime. Without external pressure from legislators and industry associations, financial services providers may not have sufficient incentive to stem the flow of identity crimes." (CNet News.com 21 Jul 2003)

Category 31.1 *Surveys, studies, audits of security*

2003-07-29 **Farm Internet access broadband**

NewsScan

WHAT ARE THEY DOING DOWN ON THE FARM?
Answer: surfing and sending e-mail. An Agriculture Department survey has found that 48% of the 2 million farms in the U.S. are connected to the Internet. The next big push will be to upgrade from dialup to broadband connections. Because the scarcity of rural subscribers doesn't justify the cost of laying cable or building rural areas, Congress last year passed a farm bill pushed by President Bush, that provided $100 million in loans and loan guarantees over the next six years to encourage companies, cities and counties to invest in broadband in rural areas. (AP/San Jose Mercury News 29 Jul 2003)

Category 31.1 *Surveys, studies, audits of security*

2003-09-04 **colleges vigilant viruses blaster U.S. infected computers log on campus students**

NewsScan

COLLEGES MORE VIGILANT AGAINST VIRUSES
Reeling from the recent rash of computer viruses, U.S. colleges and universities are taking unusually aggressive steps against further infection by returning students. University of North Texas technicians report they're eradicating viruses from about 10 PCs every hour, charging students a mandatory $30 cleaning fee for the service. Students cited for infectious computers must show proof they've been fixed before they can log back onto the campus network. Vanderbilt University reports about 25% of returning students have infected computers and Oberlin College IT director John Bucher says his department found viruses on nine out of every 10 Windows-based PCs owned by students. Meanwhile, some schools managed to avert catastrophe by filtering e-mails and using antivirus software. Duke University computer security officer Christopher Cramer says his school filtered out 2.5 million infected e-mail messages, limiting the damage to only a few dozen PCs, and Temple University's mandatory use of Symantec's antivirus software kept the infection rate down to about 400 PCs out of 35,000 students. "If it had been 10-fold, it would have crashed the network," says Temple chief information security officer Ariel Silverstone. (AP 4 Sep 2003)

Category 31.1 *Surveys, studies, audits of security*

2003-09-04 **indetity theft account credit card stolen personal information bank internet transaction**

NewsScan

VICTIMS OF IDENTITY THEFT AND ACCOUNT THEFT
The Federal Trade Commission says that the personal credit information of about 3.3 million U.S. consumers has been used last year to open fraudulent new bank, credit card or utility accounts or to commit other crimes, and that an addition 6.6 million people fell victim to account theft to steal from the victim's existing accounts. Half of all victims knew the method by which the thieves had obtained the personal information. About 25% of the victims said the information had been stolen through either the mail or the loss of a wallet, and 13% percent said it had been stolen in the course of a purchase or another transaction. (New York Times 4 Sep 2003)

Category 31.1 *Surveys, studies, audits of security*

2003-09-11 **Net Attack ports ISP block internet worms malicious program SANS Institute Inc. customers**

NIPC/DHS

September 11, IDG News Service — Study: ISPs should block 'Net attack ports.

Internet service providers (ISPs) should block access to communications ports on their customers' computers which are commonly exploited by Internet worms and other malicious programs, according to a report by Johannes Ullrich of the SANS Institute Inc. Leaving the ports open offers little to customers, while needlessly exposing them to infection and making it more likely that ISPs will be overwhelmed by future virus outbreaks, the report said. Many ISPs already block some or all of the ports named, while others offer customers free personal firewall software to install on their home computers. However, home Internet users often lack the technical knowledge necessary to install and configure a firewall, Ullrich said. The report is available on the SANS Institute Website:
http://www.sans.org/rr/special/isp_blocking.php

Category 31.1 *Surveys, studies, audits of security*

2003-09-15 **big brother syndrome IM U.K. UK work job personal use colleagues**

NewsScan

IM-ING HABITS DIFFER IN U.S., U.K.
Using Instant Messenger at work to flirt with colleagues, complain about the boss and gossip about co-workers are among the most common IM themes — at least in the U.K., where 65% of survey respondents say they use IM for personal purposes during work hours. "If you're leaning forward and typing away at your machine, who's to know what you're typing about," says Nigel Hawthorn, whose cybersecurity firm, Blue Coat Systems, conducted a poll of some 300 firms in the U.K. and the U.S. Half the British respondents admitted to spicing up their IMs with abusive language; 40% used IM-ing to conspire with colleagues during conference calls; and nearly a third confessed to "making sexual advances" via IM. U.S. respondents, meanwhile, were much more circumspect in their IM habits, with fewer than one in five using IM to comment on senior management or to flirt. The difference, says Hawthorn, is probably attributable to the Big Brother syndrome. While nearly 60% of Brits were pretty sure their bosses couldn't monitor their IM activities, 71% of U.S. respondents believed — correctly — that their IM messages could be traced back to them. (Reuters 15 Sep 2003)

Category 31.1 *Surveys, studies, audits of security*

2003-09-17 **europe download movie music free file sharing spending money in CDs**

NewsScan

EUROPE'S DOWNLOADERS ARE DIFFERENT
Unlike most Internet downloaders in the U.S., who tend to be teenagers trolling for free tunes, European downloaders are avid music and video fans, as well as regular shoppers who don't mind spending money on CDs in stores. "They are more likely to listen to digital radio and visit artist Web sites," says Jupiter Research analyst Mark Mulligan. "There is compelling evidence that this group is the bedrock community for those willing to pay for legitimate (online) music services in the future." And unlike the U.S. situation, where record labels are waging an all-out war on music swappers, in Europe, labels are pursuing a gentler approach, promoting industry-backed services and educating consumers that downloading copyrighted material is illegal. Europeans also tend to download more videos than their U.S. counterparts — 15% said they downloaded a movie every month from a free file-sharing service with Spain topping the list at 38%. In contrast, about 12% of U.S. Internet users download a video file each month. Mulligan says Hollywood should take note and avoid the hardline tactics of the music industry. "I think there's definitely an opportunity for television companies and movie studios alike to harness an emerging pattern of consumption here." (Reuters 17 Sep 2003)

Category 31.1 *Surveys, studies, audits of security*

2003-10-01 **music download piracy RIAA lawsuit copyright infringement**

NewsScan

MUSIC DOWNLOADING NUMBERS FALL
The lawsuits filed in September by the Recording Industry Association of America (RIAA) against 261 people accused of illegally downloading copyrighted material seem to have been largely responsible for a 40% decrease in usage of the file-swapping service Kazaa. A typical user reaction is this one given by a 27-year-old marketing consultant in New York: "I've been holding off. I don't want to get sued. I was never a big user per se, but I do have a ton of music files." However, Chicago intellectual property lawyer Leonard Rubin suggests that the RIAA's victory may be short-lived: "The record companies are winning a skirmish, but it's still an open question as to whether they're winning the war. What they're not doing is figuring out how to either restore some favor among music lovers, or work with the system to figure out some way to please these people who they are now offending."(San Jose Mercury News 1 Oct 2003)

Category 31.1 *Surveys, studies, audits of security*

2003-10-07 **cyber crime organized Internet Britain scam fraud pornography**

NewsScan

CRIMINALS GO WHERE THE ACTION IS: THE INTERNET
Len Hynds, the head of Britain's National Hi-tech Crime Unit (NHTCU), says that organized crime syndicates have stepped up their presence on the Internet, operating extortion rackets, child pornography rings and elaborate financial scams: "Organized crime is turning to the weakest element in the chain, which is the people. It's the hands on the keyboard on either end of the transaction that is the actual weak point. Organized crime in all its guises is extremely flexible. It does spot the new and lucrative opportunity." One urgent problem is the increase in child pornography online, and Hynds says his group is taking the problem very seriously: "We are focusing on the organized groups that are making money out of peddling child pornography on the Internet. We are doing that in partnership with business and industry. We've deployed officers from this office overseas to physically remove children to places of safety." (USA Today 7 Oct 2003)

Category 31.1 *Surveys, studies, audits of security*

2003-10-21 **employee net usage Internet work monitor survey**

NewsScan

WORKERS PLAYING ON THE NET
About half of the employees polled in an annual survey conducted for Websense admit they spend time accessing non-work-related Web sites during the work day, with the time spent joy-surfing averaging about 3.4 hours a week. The top recreational lure was news, cited by 77% of the survey respondents, followed by personal e-mail (52%), shopping (51%), online banking (47%), and investing (35%). Predictably, male employees accessed sports sites a lot more often than female (47% vs. 17%). And what do the bosses think about all this? Seventy-two percent of managers at large companies expressed concern over their workers' surfing habits, while only 54% at smaller companies saw it as a problem. (Wall Street Journal 21 Oct 2003)

Category 31.1 *Surveys, studies, audits of security*

2003-10-22 **Spam hurt e-mail use messages block millions businesses web list link attachment Pew American Life Project**

NIPC/DHS

October 22, Reuters — Spam beginning to hurt e-mail use, report says.

Half of all Internet users say "spam" e-mail messages has made them less trusting of all e-mail in general, according to a report released Wednesday, October 22 by the Pew Internet and American Life Project. One in four say they now use e-mail less because of spam. The group's June survey of 1,400 Internet users found that most feel they can do little to block the billions of unwanted pitches that arrive in their inboxes on a daily basis. Spam now comprises roughly half of all e-mail messages, according to several estimates, costing businesses billions of dollars in wasted bandwidth and lost productivity. Most respondents said they did not post their e-mail addresses to Web sites in an effort to keep off spammers' lists, and many said they used filters to block spam at work or home. But others admitted to behavior likely to perpetuate the problem. Some 7% said they had bought a product or service that was offered in an unsolicited e-mail, while one-third said they had clicked a link to get more information. Two-thirds said they had clicked a link to be removed from a spammer's e-mail list, an activity consumer advocates say is likely only to generate more spam.

Category 31.1 *Surveys, studies, audits of security*

2003-10-23 **Kansas Health Department Environment High Risk Information Systems Protection fraud disruption bioterrorism password-cracking tools 11 hours 90 percent cracked anti-virus software**

NIPC/DHS

October 23, The Lawrence Journal (Kansas) — Kansas Department of Health and Environment computers at 'high risk'.

The Kansas state agency in charge of protecting the public's health and safety is having trouble protecting its own computers and information system, according to an audit released Wednesday, October 22 by the Legislative Division of Post Audit. Operations of the Kansas Department of Health and Environment (KDHE) "were at an extremely high risk of fraud, misuse or disruption," the auditors concluded. KDHE is a large regulatory agency that collects records and information about Kansans. The agency is the leader for dealing with hazardous wastes, epidemics, immunizations and, most recently, the state's bioterrorism program. Using a standard password-cracking software, auditors were able to determine more than 1,000 employee passwords, which is about 60 percent of the total, in three minutes. Ninety percent of the passwords were cracked within 11 hours. During a lunch hour, auditors easily walked into empty offices where computers were logged on to the network and unlocked. The audit also revealed that many agency computers were infected with computer viruses that could send files and passwords to computer addresses outside the agency, and some 200 computers had no anti-virus software installed. After meeting with auditors, KDHE officials "acted strongly and swiftly to address these problems," according to the audit report.

Category 31.1 *Surveys, studies, audits of security*

2003-10-24 **Internet fraud identity theft report FTC**

NewsScan

INTERNET FRAUD UPDATE
The Federal Trade Commission says that complaints of Internet-related identity theft more than tripled last year, to 2,352 last year from the year before. Jay Foley of the Identity Theft Resource Center says, "Online fraud is becoming as big an issue for eBay and AOL as security is for Microsoft." Typically, eBay covers buyers or sellers for up to $200 (or $500 for some listings) if an item is not delivered or is in bad condition, though there is a $25 processing fee. Posting safety tips for eBay transactions are listed at at www.ebay.com/securitycenter. (USA Today 24 Oct 2003)

Category 31.1 *Surveys, studies, audits of security*

2003-10-27 **cyber crime Brazil laboratory hacker syndicate legislation**

NewsScan

CYBERCRIME: THE BRAZILIAN CONNECTION
Brazil has become a laboratory for cybercrimes such as identity theft, credit card fraud, and online vandalism. Hacker Assunção Marcos Flávio says: "If things go on like this, there'll be no more bank holdups with guns. All robberies will be done over the Net." Already, police in cities such as São Paulo, Rio de Janeiro and Brasília are finding it difficult to keep pace with hacker syndicates. Ronaldo Tossunian of the electronic crime division of the São Paulo police department points a finger at Brazilian law-makers: "We don't have the specific legislation for these crimes like they do in America and Europe. Just breaking in isn't enough to make an arrest, which means there's no deterrent." Brazil's hackers are as strong and resourceful as they are because they have little to fear legally. (New York Times 27 Oct 2003)

Category 31.1 *Surveys, studies, audits of security*

2003-10-29 **enormous data pile up UC Berkeley report**

NewsScan

WHOLE LOTTA DATA PILING UP
A study conducted at UC Berkeley reports that in 2002 people around the globe created enough new information to fill 500,000 U.S. Libraries of Congress (which is the equivalent of a stack of books 30 feet high per person). Berkeley Professor Peter Lyman says that how and to what extent all that information is used will be the subject of another study. (USA Today 29 Oct 2003)

Category 31.1 *Surveys, studies, audits of security*

2003-12-04 **movie piracy indeustry MPAA Motion Picture Association of America web sites copying difficult**

NewsScan

MOVIE PIRACY CONTINUES DESPITE INDUSTRY EFFORTS
Although film industry efforts to make illegal copying more difficult, piracy appears to have increased from previous years. The Motion Picture Association of America (MPAA) estimates that there are now 200,000 Web sites offering movies pirated by "ripping crews" (who recruit members around the world to obtain, edit, transfer and store films); these ripping crews are frequently assisted by people connected to the movie industry itself, such as cinema employees, workers at post-production houses and friends of Academy members. The MPAA and California law enforcement officials are planning how to enforce a new state law barring the illegal recording of motion pictures in movie theaters. (Los Angeles Times 4 Dec 2003)

Category 31.1 *Surveys, studies, audits of security*

2003-12-17 **virus worm cleanup expense Britain UK study**

NIPC/DHS

December 16, SearchSecurity.com — Cost of virus cleanups goes up in Britain. Malicious code attacks are costing enterprises in the UK four times as much as they did in 2002, according to a recent study by Britain's Corporate IT Forum. The forum, an organization of IT professionals from some of the UK's largest blue-chip companies, estimates that each incident costs an average of $213,000 in man-hours and related costs. In contrast, a 2002 survey conducted by Britain's Department of Trade and Industry (DTI) and PricewaterhouseCoopers put the per-incident price tag at $52,000. Three quarters of the administrators recently surveyed reported an average of 365 man-hours lost. Of those, one-third reported an average of 3,080 man-hours lost. The report determined that enterprises with sturdy incident-response teams and procedures suffered fewer malicious code outbreaks and were able to trim costs. Most infections, it was determined, came from systems integrated with business partners and contractors.

Category 31.1 *Surveys, studies, audits of security*

2003-12-29 **cybercrime doubled scammers nigerians cash-sharing partnerships Internet Fraud**

NewsScan

CYBERCRIME MORE THAN DOUBLED IN 2003
This past year the Internet proved a lucrative haven for phishers, online auction scammers and Nigerians proffering cash-sharing partnerships, according to statistics from the Internet Fraud Complaint Center, which reports it received more than 120,000 online fraud complaints in 2003. That translates to an increase of 60% since 2002, when 75,000 complaints were processed. The Center provides cybercrime victims with a convenient process for filing complaints, which it then analyzes and routes to the appropriate FBI field office or local law enforcement agency for further action. (The Register 29 Dec 2003)

Category 31.1 *Surveys, studies, audits of security*

2004-01-12 **computer crime risk Ukraine illegal access hackers library archive resource**

NewsBits; http://www.crime-research.org/library/Golubev1203.html

A Ukrainian criminologist published a review of computer-crime classifications from the point of view of law enforcement specialists in the former Eastern Bloc. Of special interest is the Web site that collected his article: The Computer Crime Research Center at < http://www.crime-research.org/>, which files hundreds of articles per year starting in July 2002.

Category 31.1 *Surveys, studies, audits of security*

2004-01-20 **IP network attack easy report survey estimate infrastructure protection**

DHS/IAIP Update

January 15, CNET News — Report: IP networks easy prey for cyberattackers.

The increasing use of Internet Protocol (IP) technology in power stations, railroads, banks and other critical infrastructure could spell big trouble, and soon, according to analysts. Although an actual act of cyberterrorism or cyberwarfare has never been recorded, the potential exists and is being facilitated by an increasingly connected world, according to a report released on Wednesday, January 14, by market-research firm Gartner. Cyberwarfare could be a reality by 2005, the company said. Technologies such as VoIP and the trend towards voice and data convergence give benefits cost and flexibility to businesses, but they also expose vital telecommunications networks to traditional forms of Internet attack, such as worms and viruses, according to the report. Gartner claims that, unlike traditional circuit-switched networks, VoIP networks have an inherent weakness when it comes to latency--any delay to the packets carrying the voice traffic disrupts communication. A massive denial-of-service attack could "degrade call performance by slowing voice packet arrival at a given destination" and effectively cut off voice communication, the report says. Other weaknesses flagged include the Supervisory Control and Data Acquisition interfaces used to connect a significant portion of critical infrastructure elements such as dams, railroads, electrical grids and power stations.

Category 31.1 *Surveys, studies, audits of security*

2004-01-22 **electronig e-voting Internet-voting Department of Defense DoD SERVE Secure Electronic Registration and Voting Experiment flaw**

RISKS 23 14

PANEL REPORTS DOD SERVE SYSTEM FATALLY FLAWED - BUREAUCRATS IN DENIAL

Scott Miller cites a _Computerworld_ article on the flaws of SERVE, a Pentagon secure e-voting project. Speaking about SERVE, Dr. Aviel D. Rubin, the technical director of John Hopkins' Information Security Institute said: "I think that a dedicated and experienced hacker could subvert the election rather easily…" SERVE spokesperson Glen Flood maintained: "The only 100% way we can avoid some of the security issues [raised by the four panel members] is to not do this. And that is not something we will do…" In a follow-up article, contributor Lillian Coney reported that political party organizations for emigrant Americans opposed SERVE by sending a joint letter to many congressional committees. She writes that about 100,000 from 50 counties were set to be case using SERVE.

Category 31.1 Surveys, studies, audits of security

2004-02-12 **terrorism detection system problems bugs fasle positives reliability audit analysis**

RISKS; http://www.latimes.com/technology/la-na-profiling12feb12,1,3293045.story?coll=la-headlines-technology 23 19

GAO REPORT WARNS OF AIRLINE SECURITY SHORTCOMINGS

In its report (released on 13 Feb 2004), a General Accounting Office study notes that CAPPS II (intended to pick out potential terrorists from among millions of air passengers) has run into "significant challenges" posing "major risks" to its deployment and public acceptance. Problems include overall system reliability and false positives, and resolving the rights of those falsely identified. Passenger-provided information would be outsourced to government contractors for analysis, the government would check supposedly validated identities against a watch list, and the result would be a green, yellow, or red risk rating for each would-be passenger. Allegedly only about 4% would be rated yellow, and "an average of only one or two people a day" would be rated red. [Remember that even a 1% false positive rate would mistakenly identify tens of thousands of travelers.]

"But the GAO report found that the agency has not adequately addressed seven of eight concerns raised by Congress. These include preventing abuses, protecting privacy, creating an appeals process, assuring the accuracy of passenger data, testing the system, preventing unauthorized access by hackers and setting out clear policies for the system." GAO investigators concluded that, though the agency was making advances in all these areas, progress was incomplete.

[This abstract was prepared by Peter G. Neumann.]

Category 31.1 Surveys, studies, audits of security

2004-02-25 **Hotels broadband Internet access vulnerability STSN Windows file sharing**

DHS IAIP Daily; http://edition.cnn.com/2004/TRAVEL/02/25/biz.trav.security/

February 25, CNN — Hotel networks face hacker threat.

Many hotels have added high-speed wireless connections for executives to surf the Internet or access corporate data on the road. However, with security software available on the Internet from sites like www.insecure.org, hackers can explore unsecured hotel networks and tap into a guest's laptop computer. "Most hotels claim to offer secure broadband services, but most do not know enough about security issues to ask their providers the right questions," David Garrison of STSN, a broadband security firm told CNN. The biggest problem is that many laptops using Microsoft Windows have a default setting that enables you to share files or communicate with other computers. Unfortunately, unless this is turned off hackers can easily get in when you log on to a wireless network. The key thing is to ask your hotel about security before booking a room and to only use those that use reputable security systems. Personal firewalls can be used as a deterrent. These are software-based and simple versions can be downloaded for free online. There are a few other steps executives can take to boost their security while using VPNs on the road, according to Garrison. "Install an anti-virus program, turn off file-sharing capabilities and make sure you have the latest security updates for your operating system," he explained.

Category 31.1 Surveys, studies, audits of security

2004-02-25 **software movie digital piracy Australia costs**

NewsScan

PIRACY COSTS INDUSTRY $AU160 MILLION

Video and computer game piracy in Australia costs the industry there at least $AU160 million a year. A new study, "Australian Crime: Facts and Figures 2003" found that the illegal market accounted for one in 12 movies sold in Australia. Software piracy accounts for around one-third of the market, costing the industry $AU138.5 million in 2002. (The Australian 25 February 2004)

Category 31.1 Surveys, studies, audits of security

2004-03-03 **4-1-9 Nigerian advance fee fraud Britain statistics**

http://www.theregister.co.uk/2003/03/03/150_brits_x_419_fraud/

In 2002, more than 150 Britons admitted being fleeced by the Nigerian 4-1-9 advance-fee fraud. Total report lost: £8.4M. Average loss reported: £56K.

Category 31.1 *Surveys, studies, audits of security*

2004-03-17 **anti-spam law failure CAN-SPAM act**

NewsScan

ANTI-SPAM LAW GOES SPLAT

A new survey from the Pew Internet & American Life organization reports the following findings: 63% of e-mail users who responded to the survey think that spam has made them less trusting of e-mail as a communications tool, and 77% think that spam makes being online "unpleasant and annoying." [The respondents obviously don't get NewsScan Daily.] A spokesperson for Senator Ron Wyden (D, OR), who co-sponsored the federal "Can-Spam Act," says: "It's premature to judge the effectiveness of the Can-Spam Act 77 days after it becomes effective. It's not time to write Can-Spam's obituary." Doug Peckover of Privacy Inc. suspects that the people spam is driving away are probably the "fringe" Internet users, who "don't depend on it for business, and for them, their pain threshold is a lot lower than for you and me. These are the folks who are saying, 'You know, it's not worth it anymore.'" (Washington Post 17 Mar 2004)

Category 31.1 *Surveys, studies, audits of security*

2004-03-29 **music piracy study survey RIAA industry claims wrong**

NewsScan

STUDY CONTRADICTS MUSIC INDUSTRY'S PIRACY CLAIMS

Two university researchers have released a study that indicates online music piracy has no negative effect on legitimate music sales, and in fact boosts sales in some cases. "Consumption of music increases dramatically with the introduction of file sharing, but not everybody who likes to listen to music was a music customer before, so it's very important to separate the two," says Felix Oberholzer-Gee, an associate professor at Harvard Business School, who co-authored the study. Oberholzer-Gee and his colleague, University of North Carolina professor Koleman Strumpf, say their "most pessimistic" statistical model indicates that only 2 million CD sales were lost due to illegal file-sharing in 2002, whereas CD sales declined by 139 million units between 2000 and 2002. "From a statistical point of view, what this means is that there is no effect between downloading and sales," says Oberholzer-Gee. The study's results contradict the recording industry's assertions that their financial decline is attributable in large part to music piracy, citing several studies that have supported that claim. However, some other research groups said the Harvard-UNC study conclusions appeared to mirror their own research findings. "While some people seemed to buy less after file sharing, more people seemed to buy more," says Jupiter Research analyst Aram Sinnreich, who conducted similar studies in 1999 and 2002. (Washington Post 29 Mar 2004)

Category 31.1 *Surveys, studies, audits of security*

2004-04-13 **IT professionals grade vendor software standards poorly**

DHS IAIP Daily; http://fcw.com/fcw/articles/2004/0412/web−survey−04−13−04.as p

April 13, Federal Computer Week — IT pros see vendor mediocrity.

Six hundred federal information technology professionals surveyed in January graded the performance of manufacturers, integrators and resellers they do business with at about a C+ average, according to the survey from Market Connections Inc. The report, released this week, states that on 15 performance factors, no one factor got an average score higher than a B-. Forty-six percent of the respondents reported using a credit card to purchase IT products online, with an average purchase under $2,500 for more than half of those surveyed. The survey found that the respondents believe IT security and information sharing among agencies will be the most important initiatives in the immediate future to help agencies fulfill homeland security missions.

Category 31.1 Surveys, studies, audits of security

2004-04-13 **browser attacks increase CompTIA survey**

DHS IAIP Daily; http://www.esecurityplanet.com/trends/article.php/3339731

April 13, eSecurity Planet — Browser-based attacks surging.

The Computing Technology Industry Association (CompTIA), a global trade association based in Oakbrook Terrace, IL, reports that a new survey of 900 organizations shows that browser-based attacks are surging, and may pose the 'next significant security threat' to enterprise networks. The study reports that 36.8 percent of the companies surveyed suffered a browser-based attack in the last six months. That number is up 25 percent from when the same study was conducted last year. These attacks, which are related to the recent spate of phishing scams, use a browser and user system permissions to allow an attacker to gain access to the computer to steal or destroy critical information. The attacks generally occur when a user visits a Website that, on the surface, appears harmless, but contains malicious code that convinces the browser to execute commands designed to sabotage the machine or lift proprietary data or personal financial information. The Computing Technology Industry Association also reports that while incidents of browser-based attacks are on the rise, computer viruses and worm attacks still far outweigh them. The survey shows that 68.6 percent say viruses and worms are the most security threat they have to deal with.

Category 31.1 Surveys, studies, audits of security

2004-04-16 **Cisco security warning IPSec VPN PKI threat**

DHS IAIP Daily; http://news.com.com/2100−7355_3−5193521.html?tag=nefd.top

April 16, CNET News.com — Cisco issues another security warning.

Cisco Systems warned customers on Thursday, April 15, of what security experts are calling a "minor security issue" in its IPSec-based VPN 3000 Concentrator. The problem, which is present in both Linux and Microsoft versions of the IPSec client, occurs when customers configure the VPN (virtual private network) concentrator to accept group passwords rather than digital certificates for authentication. Typically, a group password is encrypted when used for authentication. But on VPN 3000 Concentrator clients, the password can be extracted from memory, making it available to anyone using a device with the Cisco software client. People who have gained knowledge of a group password may use it to hijack connections or gain knowledge of sensitive information when these are used as pre-shared keys during authentication. Cisco recommends that customers deploy PKI (Public Key Infrastructure) instead of a Group Password based authentication scheme. Additional information is available on the Cisco Website:
http://www.cisco.com/warp/public/707/cisco-sn-20040415-grppa ss.shtml

---

Category 31.1 Surveys, studies, audits of security

2004-04-26 **music piracy copyright infringement lawsuits P2P peer-to-peer**

NewsScan

PEW REPORTS DECLINE IN MUSIC DOWNLOADINGS

A new report from the PEW Internet and American Life Project indicates that the lawsuits brought by Recording Industry Association of America (RIAA) against are having a definite impact on Internet music downloaders. A phone survey in February shows that 14% of online Americans (17 million people) say that at some time in their online lives they downloaded music files but no longer do any downloading. The Pew reports also says that new data from comScore Media Metrix show continuing declines or stagnation in the number of people with popular peer-to-peer file sharing applications actively running on their computers. (Pew Internet Project 26 Apr 2004)

Category 31.1 *Surveys, studies, audits of security*

2004-04-28 **survey study UK business vulnerable security IT skills lacking**

DHS IAIP Daily; http://www.vnunet.com/News/1154752

April 28, vnunet.com (UK) — UK businesses still vulnerable to security breaches.

A lack of IT security skills is leaving UK businesses vulnerable to security breaches, according to research. The Department of Trade and Industry Information Security Breaches Survey 2004 suggests that 89 per cent of companies say staff have no formal IT security qualifications. The study, by PricewaterhouseCoopers (PwC), says there is an average of one security incident per month in UK firms, but one a week in large companies. Three-quarters of UK companies, and 94 per cent of large organisations, suffered a security incident in the last year. Human error is the cause of most problems, but only a third of businesses have a security policy in place. Security spending has increased since the last survey in 2002, but only slightly from two per cent to three per cent of the annual IT budget. The report says this is well below the five to 10 per cent benchmark level. The study is available online:
http://www.security-survey.gov.uk/

Category 31.1 *Surveys, studies, audits of security*

2004-05-18 **financial sector external threats**

DHS IAIP Daily; http://continuitycentral.com/news01223.htm

May 18, Continuity Central — Financial institutions struggling to fend-off escalating security threats.

The majority of global financial institutions have had an external attack on their information technology systems within the last year and many of these breaches resulted in financial loss, according to Deloitte's 2004 Global Security Survey. However, even with security attacks on the rise, the largest number of respondents (some 25 percent) reported flat security budget growth. According to the survey, the vast majority (83 percent) of respondents acknowledged that their systems had been compromised in the past year, compared to only 39 percent in 2002. Of this group, 40 percent stated that the breaches had resulted in financial loss to their organization. The survey also finds that companies are sliding backwards when it comes to the use of security technologies. While more than 70 percent of respondents perceived viruses and worms as the greatest threat to their systems in the next 12 months, only 87 percent of respondents had fully deployed anti-virus measures. This result is down from 96 percent in 2003. Report: http://www.deloitte.com/dtt/research/0,2310,sid%253D1013%252 6cid%253D48978,00.html

---

Category 31.1 *Surveys, studies, audits of security*

2004-05-18 **kids downloading music internet access copyiright computer viruses songs**

NewsScan

SURPRISE — KIDS ARE STILL DOWNLOADING MUSIC

Fifty-six percent of American children ages eight to 18 with Internet access are continuing to download music, even though 88% of the respondents polled indicated they were familiar with music copyright restrictions, according to a new survey by Harris Interactive. The survey noted that more kids worry about downloading computer viruses with their songs than about getting in trouble with the law. The Harris poll was commissioned by the Business Software Alliance, which said the responses indicate a need for the software and entertainment industries to step up their efforts to dissuade kids from file-sharing. "It's a very good sign that a lot of kids and youth understand that creative works are protected by copyright law. [But if] they're still doing the wrong thing, that's not good," said a BSA spokeswoman. A spokesman for the Recording Industry Association of America, which has led an aggressive campaign against illegal music downloading, said the latest numbers show that "education is important, but without an enforcement component, it can only do so much to influence behavior." Meanwhile, the executive of a P2P networking company suggested it would be more productive to find ways for the two sides to cooperate rather than clamp down on music distribution. (Washington Post 18 May 2004)

Category 31.1 *Surveys, studies, audits of security*

2004-05-24 **online crime cybercrime scams phishing identity theft**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/articles/A53042−2004May 24.html

May 24, The Washington Post — Study: Online crime costs rising.

Online criminals are attacking corporate and government networks more frequently, costing businesses an estimated $666 million in 2003, according to a survey of computer security executives released Monday, May 24. The survey was conducted by CSO [Chief Security Officer] magazine in cooperation with the U.S. Secret Service and the CERT cybersecurity center. More than 40 percent of 500 executives polled said hackers have become the greatest cybersecurity threat to business and government networks. Computer systems falling prey to ever more sophisticated attacks are increasingly essential to the daily operations of businesses and government agencies, said Harris Miller, president of the Information Technology Association of America (ITAA). ITAA has long warned that many companies have not devoted enough time and money to cybersecurity. A taskforce reported to the Department of Homeland Security in April that most corporations fail to take cybersecurity seriously at the top levels of management. The report did not recommend that the government make cybersecurity a requirement for the private sector, but said that auditing firms should include cybersecurity readiness as part of the criterion for determining whether companies have adequate internal and financial safety controls.

Category 31.1 *Surveys, studies, audits of security*

2004-05-25 **authors source of viruses Russia organized crime denial of service DoS extortion**

DHS IAIP Daily; http://www.infoworld.com/article/04/05/25/HNrussianviruses_1 .html

May 25, IDG News Service — Viruses nip Russia after the Cold War.

For all its disadvantages, the former Soviet Union had one hugely overlooked advantage: it kept hackers, crackers and virus writers confined inside the country by restricting their access to the Internet. A decade later, Internet penetration is booming in the region, particularly in Russia, and viruses are epidemic. Russians are linked to some of the nastiest viruses the IT world has ever experienced: Bagel, MyDoom and NetSky, to name just a few. Security experts warn that the situation is likely to worsen as hacking, cracking and virus writing shift from being a mischievous hobby of young kids to a lucrative occupation of skilled professionals working hand-in-hand with hardened criminals. The motive is obvious: money--in some cases, big money, which fuels other traditional Mafia activities, such as drug smuggling and prostitution. Today, hundreds or even possibly thousands of skilled Russians desperate for cash are scouring the Internet looking for security vulnerabilities in the computer networks of companies, particularly in the U.S. and Europe. They are creating worms and Trojans for stealing credit card and other financial information, or turning inflected computers into zombie hosts to establish illegal spam farms, or extorting money by threatening companies with a distributed denial-of-service attack if they don't pay.

Category 31.1 *Surveys, studies, audits of security*

2004-09-03 **CIO Council federal managers information security privacy guidelines**

DHS IAIP Daily; http://www.fcw.com/fcw/articles/2004/0830/web−fea−09−03−04.asp

September 03, Federal Computer Week — CIO Council releases info-sharing guide.

Federal managers received new policy guidelines this week to help them minimize risks when sharing sensitive information online. The guidelines, issued by the federal Chief Information Officers Council, are supposed to help federal decision-makers balance the often-conflicting demands to guarantee information security and privacy and against demands to carry out their agencies' missions. For federal managers who are developing new information systems, the guidelines urge thinking about data privacy and data security as early as possible and at the highest levels possible. In an era of extensive information sharing, "information assurance specialists by themselves can no longer be charged to protect enterprise resources," the guidelines state. If agency managers follow the guidelines, they will find security and privacy controls affecting all aspects of information systems development and operations, including how they measure their systems performance, engineer workflow, design directory information, achieve interoperability and exchange data.

Category 31.1 *Surveys, studies, audits of security*

2004-09-06 **Internal Revenue Service IRS federal US government govt. security audit**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/story/0
,10801,95705,00.html

September 06, Computerworld — Federal audit raises doubts about IRS security system.

Software performance and functionality problems continue to plague the Security Audit and Analysis System (SAAS) designed to detect hacking and other unauthorized activities on computers at the Internal Revenue Service, according to auditors within the U.S. Department of the Treasury. The problems are limiting the ability of business managers and IT security workers at the IRS to identify improper uses of new applications that provide online tax services and information about refunds, the auditors said in a report issued last month by the Office of the Treasury Inspector General for Tax Administration. "Not having an effective audit-trail review process is a significant security weakness that should weigh heavily on whether to accredit future modernization applications," the report said. Daniel Galik, chief of mission assurance for the IRS, said that the system met all defined requirements and passed all tests before it was accepted. Galik wrote that the IRS is taking steps to correct the system problems and expects all the major components of SAAS to be fully functional by the end of October.

Category 31.1 *Surveys, studies, audits of security*

2004-09-20 **online atacks rise study survey Internet Security Threat Report Symantec botnets spammers vulnerabilities**

NewsScan

INTERNET ATTACKS JUMP SIGNIFICANTLY THIS YEAR

The semiannual Internet Security Threat Report, which is based on monitoring by computer security firm Symantec, indicates that in the first six months of 2004 there were at least 1,237 newly discovered software vulnerabilities and almost 5,000 new Windows viruses and worms capable of
compromising computer security. The numbers represent a dramatic increase over the same period in 2003. Even more troubling was the sharp rise in the number of "bot," or robot, networks, which comprise a large number of infected PCs that can then be used to distribute viruses, worms, spyware
and spam to other computers. The survey notes that in the first half of 2004, the number of monitored botnets rose from fewer than 2,000 to more than 30,000. The botnets, which range in size from 2,000 to 400,000 "zombie" machines, are often "rented out" to commercial spammers who use
them to distribute junk e-mail while concealing their identities. E-commerce was the industry most frequently targeted for attacks, accounting for 16% of the total, and report authors note that phishing
scams are responsible for pushing up the numbers in that category. "We're seeing a professional hand in development that was pretty startling in terms of malicious code," says Alfred Huger, senior director of engineering for security response at Symantec. The report's findings mirror those of
recent government-supported research. (New York Times 20 Sep 2004)

Category 31.1 *Surveys, studies, audits of security*

2004-09-30 **consumer cyberattacks attitude light National Cyber Security Alliance**

DHS IAIP Daily;
http://news.com.com/Study%3A%2BConsumers%2Btake%2Bcyberattac
ks%2Blightly/2100−7349_3−5390749.html

September 30, CNET News.com — Study: Consumers take cyberattacks lightly.

Consumers have a casual approach toward cybersecurity and fail to grasp the pervasiveness of online threats, according to a study release Thursday, September 30, by the non-profit National Cyber Security Alliance (NCSA). The results of a major study on cybersecurity are due in October. The NCSA has dubbed October as National Cyber Security month and will spend the month attempting to educate users.

Category 31.1 *Surveys, studies, audits of security*

2004-10-24 **cybersecurity survey America Online AOL spyware virus awareness education training firewall vulnerability**

NewsScan;
http://news.com.com/Plague+carriers+Most+users+unaware+of+PC+infections/2100-1029_3-5423306.html

CYBERSECURITY LARGELY IGNORED BY INDIVIDUAL USERS

A new study by America Online and the National Cyber Security Alliance indicates that about 80% of home PCs are infected with spyware, but most users aren't even aware of it. And while 85% of users had installed antivirus software, two-thirds of those had not updated it in the past week. In addition, about 20% had an active virus on their machines and two-thirds did not have a firewall installed. AOL chief trust officer Tatiana Gau says the results highlight just how vulnerable the average online user is to malicious hackers. "No consumer would walk down the street waving a stack of cash or leave their wallet sitting in a public place, but far too many are doing the exact same thing online. Without basic protections like antivirus, spyware and firewall software, consumers are leaving their personal and financial information at risk." (CNet News. com 24 Oct 2004)

Category 31.1 *Surveys, studies, audits of security*

2004-10-25 **Internet security weak survey report AOL NCSA DHS FTC**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/articles/A60199−2004Oct 25.html

October 25, Associated Press — Security for Internet users deemed weak.

Internet users at home are not nearly as safe online as they believe, according to a nationwide inspection by researchers. They found most consumers have no firewall protection, outdated antivirus software and dozens of spyware programs secretly running on their computers. The study released Monday, October 25, by America Online (AOL) and the National Cyber Security Alliance (NCSA) found that 77 percent of 326 adults in 12 states assured researchers in a telephone poll they were safe from online threats. When experts visited those same homes to examine computers, they found two-thirds of adults using antivirus software that was not updated in at least seven days. Two-thirds of the computer users also were not using any type of protective firewall program, and spyware was found on the computers of 80 percent of those in the study. The survey participants all were AOL subscribers selected in 22 cities and towns. NCSA, a nonprofit group, is backed by the Homeland Security Department and the Federal Trade Commission, plus leading technology companies. Study: http://www.staysafeonline.info/home-news.html

---

Category 31.1 *Surveys, studies, audits of security*

2004-10-28 **Department Homeland Security DHS information security deficiency report negative**

DHS IAIP Daily; http://www.fcw.com/fcw/articles/2004/1025/web−dhsig−10−28−04 .asp

October 28, Federal Computer Week — Report: DHS has 'significant deficiency' in info security.

The Homeland Security Department's (DHS) inspector general (IG) has completed an information security audit of the agency, which shows DHS officials are still struggling with internal cybersecurity issues. The report, released Wednesday, October 27, highlights areas in which DHS officials have improved the department's information security practices and policies. But the overall tone of the report is negative. The report cited the chief information officer's lack of authority to manage DHS' departmentwide information technology programs and spending as a significant factor in the department's struggle to secure its information systems. Steven Cooper, DHS' CIO, stated that while he generally concurred with the IG's findings, DHS officials have begun a comprehensive inventory of general support systems and major applications and will review data captured in the agency's automated systems. Report: http://www.dhs.gov/dhspublic/interweb/assetlibrary/OIG_04-41 .pdf

---

Category 31.1 Surveys, studies, audits of security

2004-11-01 **laptop portable security concern lax Europe survey lack of policy**

DHS IAIP Daily;
http://www.techworld.com/security/news/index.cfm?NewsID=2517

November 01, Techworld — Lax laptop policies create security concerns.

A new Europe-wide survey has revealed that laptops returning to company networks after their travels are now one of the biggest security hazards faced by many companies. Despite this, 70 percent of companies questioned offered no written guidance to employees on the use of their machines, and only a quarter imposed technological restrictions. The survey of employees in 500 companies across Europe on behalf of Websense, uncovered the tendency of many employees to treat laptops as unofficial personal possessions. As an absolute minimum, companies should start asking employees to sign up to reasonable use guidelines, while IT staff should treat any laptop connecting to the company network after returning from its travels as a major security risk.

Category 31.1 Surveys, studies, audits of security

2004-11-05 **e-governance e-voting UK Ireland Uganda**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A27612-2004Nov5.html?nav=headlines

E-GOVERNANCE FACES CHALLENGES ABROAD

Many overseas e-governance projects are failing, due to poor planning, political interference and bureaucratic bungling, according to World Bank information technology specialist Robert Schware. E-governance refers to efforts by governments to use Internet and computer technology to provide services to citizens and businesses. Schware notes that about 35% of all such projects in developing countries are a washout, with an additional 50% failing in some respect, leaving only about a 15% success rate. Schware cites $63 million spent by Ireland's government to test electronic voting technology before the project was abandoned due to doubts about its accuracy and privacy concerns. Uganda spent $22 million on an e-voting system, which performed poorly at the polls in 2001. And the U.K. pursued a $23.5 online university project that attracted only 900 students. One problem, says Schware, is that politicians sometimes want to speed up the timeline of the e-voting projects in order to win votes -- a process that usually ends up hurting the project. (AP/Washington Post)

Category 31.1 Surveys, studies, audits of security

2004-11-09 **computer security information assurance IA jobs work survey study**

WSJ;

INFOSEC Jobs on the Rise

IDC released a study in November 2004 showing that information assurance specialists continued to see growth in demand and salaries. Combinations of technological knowledge and business acumen were particularly highly in demand.

Category 31.1 Surveys, studies, audits of security

2004-11-16 **hackers getting better attack boom Internet security VeriSign**

DHS IAIP Daily; http://www.techweb.com/wire/security/53200186

November 16, TechWeb News — Better hackers behind attack boom according to Internet security firm.

Security events in the third quarter jumped 150 percent over the same period last year, fueled by more sophisticated hackers writing better code who are more interested in dollars than creating computer disasters, said Internet security firm VeriSign in a new report issued Tuesday, November 16. Hackers are not only getting bolder, but they're getting better at their "jobs," said Mark Griffiths, VeriSign's vice president of security services. "Viruses written to be malicious didn't need to be written very well, but now that their primary aim is money, they're writing better code," Griffiths said. That has had a direct impact on not only the sophistication of attacks, but also their number. Sample exploits, notes VeriSign in the report, once were of such poor quality that only a skilled programmer could edit the code to produce a working attack. In the past quarter, however, exploit code has been surprisingly simple to make work, which gives less technically-astute hackers a much better chance of wrecking havoc themselves as they massage the exploit code into a working worm or virus. Report:
http://www.verisign.com/static/017574.pdf

Category 31.1 *Surveys, studies, audits of security*

2004-11-30 **information security training government employees importance**

DHS IAIP Daily; http://www.fcw.com/geb/articles/2004/1129/web−secure−11−30−0 4.asp

November 30, Federal Computer Week — Stressing security training.

Teaching basic computer security has become an essential part of training government employees, and agency officials who neglect security education will regret it, said David Jordan, chief information security officer for Arlington County, VA. Employees who are aware of the pitfalls of using computers connected to the Internet are "the most powerful weapons against cyberthreats that you can have," Jordan said. He spends 15 to 20 minutes with all new county government employees talking to them about cybersecurity. And it's why he sends computer and network security information to employees on a biweekly basis via the county's electronic newsletter. Editors can help take a security officer's message and craft it to suit to the audience, Jordan said.

Category 31.1 *Surveys, studies, audits of security*

2004-12-17 **Department of Homeland Security DHS cyber security lagging report NIST guidelines NSA recommendations**

DHS IAIP Daily; http://www.securityfocus.com/news/10148

December 17, SecurityFocus — Report: DHS cyber security lagging.

The U.S. Department of Homeland Security (DHS) is having some homeland cyber security issues on its systems providing remote access to telecommuters, according to a newly-released report by the DHS Inspector General's office. Earlier this year security auditors spent five months probing hosts, attacking passwords and war dialing the Department. They found that some of the hosts designed to allow home workers and other trusted users access to DHS networks by modem or over the Internet lacked the authentication measures called for by official NIST guidelines and recommendations by the National Security Agency. The Inspector General's report recommends that DHS update the DHS Sensitive Systems Handbook to include implementation procedures and configuration settings for remote access to DHS systems, ensure that procedures for granting, monitoring, and removing user access are fully implemented, and ensure that all necessary system and application patches are applied in a timely manner. While Department CIO Steve Cooper concurred with the recommendations, he said some of the auditors' concerns were overstated: The systems suffering known vulnerabilities were waiting for patches to come out of testing, and any genuine effort at password hacking would be hobbled by the Department's policy of limiting failed login attempts. Report: http://www.dhs.gov/dhspublic/interweb/assetlibrary/rOIG_05-0 3_Nov04.pdf

---

Category 31.1 *Surveys, studies, audits of security*

2005-01-10 **poll attack Internet power grid P2P peer-to-peer**

NewsScan; http://www.pewinternet.org/PPF/r/145/report_display.asp

NO SURPRISES HERE -- A BIGGER ROLE FOR THE INTERNET PREDICTED

A majority of the 1,286 experts polled by the Pew Internet & American Life Project and Elon University believe that at least one devastating attack on either the networked information infrastructure or the U.S. power grid will occur in the next 10 years. Other areas of general agreement: The Internet will become more deeply integrated in our physical environments and high-speed connections will become more commonplace. When examining the impact of these trends, 59% agreed that government and business surveillance activities likely will increase as computing devices become embedded in appliances, cars, phones and even clothes; 57% said virtual classes will play a greater role in formal education, with students occasionally grouped by skill level or interest, rather than by age; 56% predicted a continued blurring of the line between work and leisure thanks to the expansion of telecommuting, and resulting in a changing family dynamic; and 50% thought P2P music file-sharing would still be available a decade from now. Schools came in for sharp criticism, with many of the experts noting how little educational institutions had changed, despite all the hype over "school wiring" during the past decade. And it was generally agreed that the "digital divide" was alive and well, with low income, rural and poorly educated people having significantly less access to the Internet than their wealthier, better educated and more metropolitan counterparts. (Pew Internet & American Life Project 10 Jan 2005)

Category 31.1 *Surveys, studies, audits of security*

2005-01-13 **national cybercrime survey Department Homeland Security DHS Justice DoJ 36000 businesses**

DHS IAIP Daily; http://fcw.com/fcw/articles/2005/0110/web−survey−01−13−05.as p

CYBERCRIME SURVEY PLANNED

In what they hope will become the premier measure of national cybercrime statistics, officials at the Department of Homeland Security (DHS) and the Department of Justice (DOJ) plan to survey 36,000 businesses this spring to examine the type and frequency of computer security incidents. Officials from both departments said there are currently no surveys that do what they envision the Computer Security Survey will do annually: provide statistically relevant national data on cybercrime across all U.S. businesses, especially those in critical infrastructure sectors. Patrick Morrissey, deputy director for law enforcement and intelligence in DHS' National Cyber Security Division, said no one really knows if the problem is getting better or worse or what sectors cybercriminals may be targeting. Better data could help form policy and improve resource allocation for government and the commercial sector, but few datasets are available on the national level.

Category 31.1 *Surveys, studies, audits of security*

2005-01-24 **Internal Revenue Service IRS information technology IT security plan improvement corrective action**

DHS IAIP Daily; http://informationweek.com/story/showArticle.jhtml?articleID=57703333

IRS NEEDS BETTER IT SECURITY PLAN, INSPECTOR GENERAL SAYS

The Internal Revenue Service isn't doing enough to assure the security of its IT systems, according to a Treasury Department Inspector General's report made public last week. The report says the IRS has prepared action plans and milestones to track program-level and system-level weaknesses, as required by the White House Office of Management and Budget. But the process the IRS employs to identify weaknesses and report progress is flawed and ineffective, the report states. That means the information the IRS provides Treasury and has been inaccurate and misleading. To ensure an effective system is established to monitor security weaknesses, the Inspector General's office recommends that the IRS chief of mission assurance and security services coordinate with the department's CIO and business-unit owners to develop plans that specifically identify all known security weaknesses. The IRS chief of mission assurance and security services agrees with the inspector general's recommendations, and has initiated a number of corrective actions. Report: http://www.ustreas.gov/tigta/auditreports/2005reports/200520 027fr.pdf

---

Category 31.1 *Surveys, studies, audits of security*

2005-02-01 **Virtual Private Networks VPN weakest security link three year study report NTA Monitor**

DHS IAIP Daily; http://www.vnunet.com/news/1160912

VIRTUAL PRIVATE NETWORKS (VPNS) ARE OFTEN THE WEAKEST SECURITY LINK, STUDY SAYS.

A three-year research project by security firm NTA Monitor has concluded that nine out of 10 virtual private networks (VPNs) have exploitable vulnerabilities. Most of the companies that had their VPNs tested as part of the project thought that they were invulnerable to hackers, but researchers found the same types of flaw repeated across the whole product range. The report stated that, in some cases, VPNs were actually the weakest security link in an organization. The most widespread flaw involved the hacking of user names. Other vulnerabilities center around password cracking. Report: http://www.nta-monitor.com/news/vpn-flaws/index.htm

---

Category 31.1 *Surveys, studies, audits of security*

2005-02-02 **survey study spyware surveillance Trojans**

RISKS; http://www.earthlink.net/spyaudit/press 23 70

SPYAUDIT REPORTS GROWTH IN MALWARE

Monty Solomon reports:

The most malicious forms of spyware, system monitors and Trojans, increased in the last three months of 2004, according to the quarterly SpyAudit report, the nation's next-generation Internet Service Provider, and Webroot Software, a producer of award-winning privacy, protection and performance software. The report also documents the complete SpyAudit results for 2004, which tracked the growth of spyware on consumer PCs since the report's inception on January 1, 2004. It shows the instances of system monitors rose 230 percent, while the instances of Trojans rose 114 percent from October 2004 to December 2004. Trojans, keystroke loggers and system monitors are capable of capturing keystrokes, online screenshots, and personally identifiable information like your social security number, bank account numbers, logins and passwords, or credit card numbers.

The number of SpyAudit scans performed during the fourth quarter also rose with an increase of 72 percent from October 2004 through December 2004. In total for 2004, more than 4.6 million scans were performed, discovering approximately 116.5 million instances of spyware, adware or potentially unwanted software. An average of 25 traces were found per SpyAudit scan for 2004. The complete report is available at http://www.earthlink.net/spyaudit/press . …

Category 31.1 *Surveys, studies, audits of security*

2005-02-08 **survey security insider threat greater hacker virus worm Ponemon Institute**

DHS IAIP Daily; http://www.networkingpipeline.com/showArticle.jhtml?articleID=59301819

SURVEY SAYS INSIDERS, NOT HACKERS, ARE MAIN CAUSE OF DATA BREACHES

Most network security breaches are caused by insiders, rather than by hackers, viruses, or worms, according to a new study released by the think tank Ponemon Institute. In the study, 69% of companies reported that their data security breaches were the result of either malicious employee activities or non-malicious employee error. The leading single cause of data security breaches was non-malicious employee error, at 39%. Only 16% of serious data leaks were linked to hackers or break-ins. Of the 163 companies surveyed, 75% reported that a serious security breach had occurred within the past year.

[MK notes: WHAT HAVE WE SECURITY PEOPLE BEEN TELLING YOU FOR THE LAST 25 YEARS?? WHAT ARE WE, CHOPPED LIVER???]
[****** (turns bright red)]
[SLAP (slaps forehead in frustration)]
[THUD (falls off chair]
[SCRABBLE SCRABBLE (gets back on chair)]

Category 31.1 *Surveys, studies, audits of security*

2005-02-09 **survey slide higher-ed it spending colleges universities analysts budgets performance hardware costs investments wireless networks**

EDUPAGE; http://chronicle.com/prm/daily/2005/02/2005020903n.htm

SURVEY PREDICTS SLIDE IN HIGHER ED IT SPENDING

A recent Market Data Retrieval survey of IT officials at more than 1,400 two- and four-year colleges and universities suggests a decline of 4 percent in IT spending this year compared to last year, itself a decline over the previous year. Analysts at the research firm said the decline is likely a result not only of tight budgets overall but also of increased performance of hardware, allowing lower costs for some investments. The overall drop of 4 percent is the net of a 13 percent slide in investments at public institutions and a 28 percent increase at private institutions. Private institutions continue to significantly outpace their public counterparts on IT spending per student, spending an average of $553 per student versus $203 at publics. The survey also found slightly lower rates of distance education offerings, down from 67 percent to 64 percent, and an increase in wireless networks, rising from 70 percent last year to 79 percent this year.

Category 31.1 *Surveys, studies, audits of security*

2005-02-13 **cybersecurity study competitive advantage bottom line boost Business Software Alliance BSA Information Systems Security Association ISSA**

DHS IAIP Daily;
http://www.scmagazine.com/news/index.cfm?fuseaction=newsDeta
ils&newsUID=87605d0f−ffc6−4169−93e4−3c7274412de7&newsType=La
test%20News

SC MAGAZINE — CYBERSECURITY BOOSTS BOTTOM LINE

Companies that make cybersecurity a priority say it increases their efficiency and gives them a competitive advantage in the market, according to a survey of information security professionals. The joint survey by the Business Software Alliance (BSA) and the Information Systems Security Association (ISSA) queried 850 ISSA members online between December 2004 and January 2005. The members represent large to small businesses. Seventy-six percent of the companies said raising security as a priority gives them a competitive advantage. Their systems are down less often, they're not losing customers due to lack of trust, and their brand is not threatened, said Robert Holleyman, BSA president and CEO. The survey also showed that in the last 12 months, more companies have raised security to the senior management level - 44 percent in 2004 versus 39 percent in the previous 2003 survey. Survey: http://www.bsa.org/usa/press/newsreleases/BSA-ISSA-Commissio ned-Survey.cfm

---

Category 31.1 *Surveys, studies, audits of security*

2005-02-15 **CIO IT Association of America managers survey system consolidation security priorities 2005**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/35066−1.html

CIOS SAY CONSOLIDATION AND CYBERSECURITY TOP PRIORITY LIST.

CIOs and IT managers will focus on systems consolidation and security through the end of the fiscal year. That's the chief finding from a new survey of CIOs from civilian, Defense Department, legislative and top-level executive offices. The driving factors behind IT consolidation are cutting costs and improving network cybersecurity, respondents said in the 15th annual Federal CIO Survey. CIOs also identified risk management, integrating physical and IT security, and assessing the vulnerabilities of less crucial systems as among their top priorities. The survey, conducted by the IT Association of America, found that CIOs want to reduce the number of e-mail, file and print servers in use as well as cut the number of data centers. Survey: http://www.itaa.org/news/docs/itaasurvey_f.pdf

---

Category 31.1 *Surveys, studies, audits of security*

2005-02-16 **federal government cybersecurity report card cyber attack**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A30342-
2005Feb16.html

FEDERAL AGENCIES GET FAILING GRADES ON CYBERSECURITY

At least half of all federal agencies received a grade of "D" or worse on the House Government Reform Committee's annual cyber-security report card. Agencies that received failing marks include the departments of Agriculture, Commerce, Energy, Health and Human Services, Housing and Urban Development, and Veterans Affairs. A grade of "D" was awarded to the departments of Defense and Treasury, as well as the National Aeronautics and Space Administration and the Small Business Administration. Committee Chairman Tom Davis (R-VA) was encouraged by the fact that the scores of the 10 agencies, as poor as they were, have actually improved since last year, but he warned they must still do better: "I hope it won't take some kind of major cyber-attack to wake everybody up." (Washington Post 16 Feb 2005)

Category 31.1 *Surveys, studies, audits of security*

2005-02-16 **companies education training Secure Software Forum colleges universities Oracle problems sophisticated automated tools flaws representatives**

EDUPAGE; http://news.com.com/2100-1002_3-5579014.html

COMPANIES POINT TO EDUCATION FOR POOR SECURITY TRAINING

In a panel discussion at the Secure Software Forum in San Francisco, a number of major software makers pointed to inadequate security training at colleges and universities as a main reason software continues to be plagued with security flaws. Mary Ann Davidson, chief security officer at Oracle, said, "Unfortunately, if you are a vendor, you have to train your developers until the universities start doing it." Although other problems were identified, including a lack of sophisticated, automated tools to identify flaws, representatives of other software companies included in the panel agreed that at least some of the blame falls on colleges and universities for not providing graduates with sufficient understanding of security issues. Fred Rica, a partner in PricewaterhouseCoopers' Threat and Vulnerability Assessment Services, disagreed, saying that "Functionality still trumps security." When companies must decide how to allocate development money, he said, they choose new features over security for existing applications. A study by Gartner noted that although companies cite lack of skills among developers as a significant problem, those same companies put relatively little funding into training programs.

Category 31.1 *Surveys, studies, audits of security*

2005-02-16 **American Electronics Association IT US student decline international competitive advantage leadership math science education**

DHS IAIP Daily; http://www.fcw.com/fcw/articles/2005/0214/web-aea-02-16-05.asp

AMERICAN ELECTRONICS ASSOCIATION FEARS I.T. DECLINE

A report from the American Electronics Association warns that the decreasing focus on science and technology inside the United States will weaken the country's competitive advantage. The trade group's report notes that federally sponsored research and development funding for information technology has declined during the past decade and a half as priorities have shifted to life sciences. Authors of "Losing the Competitive Advantage?" also argued the U.S. educational system fails to provide the math and science skills needed to compete in the workforce, while higher education does not graduate enough scientists and engineers to keep up with the high-tech industry's growth. Bob Cohen, a senior vice president at the Information Technology Association of America (ITAA), said ITAA members agree that some indicators suggest U.S. leadership in high technology may be at risk, if the country does not sharpen its competitiveness in global markets. Report: http://www.aeanet.org/Publications/idjj_CompetitivenessMain0 205.asp

---

Category 31.1 *Surveys, studies, audits of security*

2005-02-16 **US government cyber secuirty report card homeland security**

NewsScan; http://www.boston.com/business/technology/articles/2005/02/16/agencies_earn_d_plus_on_computer_security/

'D' IS FOR 'DISMAL' U.S. GOV'T CYBERSECURITY

Despite widespread agreement that computer security should be a top priority of U.S. government agencies, the latest cybersecurity progress report from Congress rates overall government efforts a D-, with seven of the 24 largest agencies earning a failing grade -- including the departments of Energy and Homeland Security, which, ironically, houses the National Cyber Security Division. "Several agencies continue to receive failing grades, and that's unacceptable," says Rep. Tom Davis (R-Va.), chair of the House Government Reform Committee. But on the bright side, says Davis, "We're also seeing some exceptional turnarounds." Those include the departments of Transportation (up from a D+ to an A-), Justice (up from an F to a B-) and the Interior (up from an F to a C+). Davis notes that problem areas include lax security at federal contractor computers; a lack of contingency planning for broad system failures; and scant training opportunities for employees responsible for computer security. (AP/ Boston.com 16 Feb 2005)

Category 31.1 *Surveys, studies, audits of security*

2005-03-04 **White House government auditors information technology IT report security improvement indication Congress presentation**

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml?artic leID=60405791

WHITE HOUSE REPORT SHOWS IMPROVEMENT IN IT SECURITY

Government auditors certified and accredited 77% of the federal government's 8,623 IT systems after undergoing risk assessments and security-control testing last fiscal year, up from 62% in fiscal year 2003, according to a White House report to Congress made public Friday, March 4. Several agencies, notably the departments of Labor and Transportation, showed remarkable improvements, with Transportation certifications rocketing to 98% from 33% and Labor accreditations leaping to 96% from 58%. Karen Evans, administrator for E-government and IT in the White House Office of Management and Budget, said at a press briefing that she was pleased with the progress, but the government must be diligent even when all systems are eventually certified. "You can't be 100% secure," she said. Report: http://www.whitehouse.gov/omb/inforeg/2004_fisma_report.pdf

---

Category 31.1 *Surveys, studies, audits of security*

2005-03-10 **Singapore first network technology readiness index United States US drop**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/articles/A23545− 2005Mar 10.html

SINGAPORE TOPS SURVEY OF TECH READINESS.

The United States is no longer first in making the best use of information and communications technology, a new study says. It dropped to fifth place this year and Singapore is now tops. Singapore's ranking in the so-called "networked readiness index" was based on several factors, including quality of math and science education and low prices for telephone and Internet services, said the World Economic Forum report. The United States' drop from first place last year "is less due to actual erosion in performance" than to the improvement of other countries, the report said. Report: http://www.weforum.org/site/homepublic.nsf/Content/Global+Co mpetitiveness+Programme%5CGlobal+Information+Technology+Repo rt

---

Category 31.1 *Surveys, studies, audits of security*

2005-03-15 **European information technology IT managers false sense Stress in Security study survey**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/story/0 ,10801,100397,00.html

STUDY: EUROPEAN IT MANAGERS HAVE FALSE SENSE OF SECURITY

Many European IT managers find their jobs extremely stressful, and even those who feel they have done as much as they can to protect their companies against emerging threats are operating under a false sense of security, according to a study released today. These conclusions were detailed in Websense Inc.'s "Stress in Security" survey of 500 IT managers across Europe. Although 91% of the managers said they believe their companies have good IT security, 70% said they leave gaps open to common Internet threats, according to the study. Many known Web-based threats are being overlooked, and a majority of respondents said they have no measures in place to protect against internal hackers or phishing attacks. "The biggest problem is that they are being reactive rather than proactive," said Websense spokesperson Rebecca Zarkos, who worked on the report. Eight percent of the European companies surveyed said they have no security measures beyond a basic firewall and an antivirus product in place. A possible reason behind the lax security is that IT managers aren't delegating enough responsibility to end users, and too few security policies are enforced, Websense said. Report Summary: http://ww2.websense.com/global/en/PressRoom/PressReleases/Pr essReleaseDetail/?Release=050315863

Category 31.1 *Surveys, studies, audits of security*

2005-03-25 **cybersecurity regulations challenge study report Department of Homeland Security DHS regulatory power**

DHS IAIP Daily; http://www.fcw.com/article88407−03−25−05−Web

STUDY SAYS CYBERSECURITY REGULATIONS WOULD BE CHALLENGING TO IMPLEMENT

Some lawmakers, concerned about the nation's vulnerability to cybercrime and possible cyberterrorism, are considering whether a larger federal government role in dealing with the problem is feasible. But a recent study by the Congressional Research Service, which conducts public policy studies, suggests that congressional leaders will face significant challenges if they try to create a regulatory framework to strengthen the nation's cyberdefenses. The report cites two possible models for greater government involvement in cybersecurity. One is the government response to the year 2000 computer crisis. The Securities and Exchange Commission set rules requiring companies to report on their Year 2000 preparedness, and Congress passed liability protections for companies that complied with the rules. The other is a food safety or environmental regulation model in which federal agencies set regulations and use inspectors to monitor compliance. But the report raises questions about the feasibility of either model. Despite being inconclusive, the report lays out several legislative options. The strongest option, according to the report, would be for Congress to provide the Department of Homeland Security or another agency with regulatory authority over cyberspace industries. Report: http://www.usembassy.it/pdf/other/RL32777.pdf

---

Category 31.1 *Surveys, studies, audits of security*

2005-04-04 **higher education colleges universities computer security below average**

EDUPAGE; http://www.nytimes.com/2005/04/04/technology/04data.html

HIGHER ED FARES BELOW AVERAGE FOR COMPUTER SECURITY

A recent spate of computer-security incidents at colleges and universities has drawn attention to the apparent tension between concerns over academic freedom and the need to protect sensitive information. Stanton S. Gatewood, chief information security officer at the University of Georgia, which suffered a security breach last year, noted that higher education is "built on the free flow of information and ideas," saying that college and university networks are designed based on that ideal. The result, however, is a tempting target for information thieves. According to the Office of Privacy Protection in California, colleges and universities in that state have accounted for more data incidents since 2003--close to 30 percent--than any other group. Although some states now prohibit using Social Security numbers as identifiers in many databases, their continued prevalence makes changing structures difficult. The University of Michigan, for example, spent seven years weaning itself off Social Security numbers. Because testing agencies and other organizations continue to use them, however, the university finds it still has to track them. New York Times, 4 April 2005 (registration req'd)

Category 31.1 *Surveys, studies, audits of security*

2005-04-06 **businesses information technology IT system downtime virus attack denial of service DoS study**

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml;jsess ionid=JEJIDQB3K21CEQSNDBGCKHSCJUMEKJVN?articleID=160501452

BUSINESSES SUFFER MORE DOWNTIME FROM VIRUSES

Damage to business IT systems caused by viruses continues to grow, and businesses are getting hit by more viruses, according to a new survey. IT systems were hit with 50% more viruses in 2004 than they were in 2003, reaching 392 incidents per 1,000 machines, according to a survey of 300 companies and government agencies sponsored by McAfee, Microsoft, Trend Micro, and other vendors, and conducted by ICSA Labs, a division of Cybertrust Inc. The Virus Prevalence Survey indicates that when 25 or more PCs or servers are infected, system downtime increased by 12% in 2004 compared with a year earlier. The amount of time it took in 2004 to recover from the infections increased by seven person days, year over year, and the actual costs of recovery averaged $130,000. Both of those figures were 25% higher than in 2003. Survey details: http://www.cybertrust.com/pr_events/2005/20050405.html

---

Category 31.1 *Surveys, studies, audits of security*

2005-04-07 **Government Accountability Office information security report testimony FISMA 2002 devastating consequences**

DHS IAIP Daily; http://www.gao.gov/cgi−bin/getrpt?GAO−05−483T

INFORMATION SECURITY: CONTINUED EFFORTS NEEDED TO SUSTAIN PROGRESS IN IMPLEMENTING STATUTORY REQUIREMENTS (TESTIMONY)

For many years, the Government Accountability Office (GAO) has reported that poor information security is a widespread problem that has potentially devastating consequences. This testimony reports on the federal government's progress and challenges in implementing the Federal Information Security Management Act of 2002 (FISMA) as reported by the Office of Management and Budget (OMB), the agencies, and Inspectors General (IGs). In its fiscal year 2004 report to the Congress, OMB reports significant strides in addressing long-standing problems, but at the same time, cites challenging weaknesses that remain. Fiscal year 2004 data reported by 24 major agencies generally show increasing numbers of systems meeting key statutory information security requirements compared with fiscal year 2003. Nevertheless, challenges remain. For example, only seven agencies reported that they had tested contingency plans for 90 to 100 percent of their systems, and six of the remaining 17 agencies reported that they had tested plans for less than 50 percent of their systems. Opportunities also exist to improve the usefulness of the annual FISMA reporting process. In addition, a commonly accepted framework for the annual FISMA mandated reviews conducted by the IGs could help ensure the consistency and usefulness of their evaluations.

Category 31.1 *Surveys, studies, audits of security*

2005-04-25 **survey study steep rise Website defacements 2004 hacktivism**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4480689.stm

SURVEY SHOWS STEEP RISE IN WEB SITE DEFACEMENTS

Attacks on Web sites jumped 36 percent in 2004, totaling nearly 400,000 incidents, according to Zone-H, an organization that tracks malicious Web activity. Of the attacks recorded by the organization, Web site defacements--in which a bogus Web page is substituted for a Web site's home page--constituted the vast majority of attacks. Roberto Preatoni of Zone-H pointed out, though, that "the techniques used by defacers are the same techniques used by serious criminals to cause more serious damage." According to the group's report, more than half of the successful hacks took advantage of a known weakness or careless administration, such as easily guessed passwords or unprotected systems. Zone-H reported that the frequency of attacks rises over the Christmas holidays and drops when schools reopen each year after summer break. BBC, 25 April 2005

Category 31.1 *Surveys, studies, audits of security*

2005-04-25 **unpatched computer machines major security threat McAfee analysis**

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml;jsessionid=ZWPITNXHXNCIMQSNDBCSKH0CJUMEKJVN?articleID=161502434

UNPATCHED MACHINES SEEN AS MAJOR SECURITY THREAT

Hackers will keep developing exploits that take advantage of known software vulnerabilities because, although patches are available, a minority of machines are fixed, security vendor McAfee said Monday, April 25. In releasing its quarterly security analysis, McAfee's "AVERT" virus research team noted that exploited vulnerabilities are becoming a dominant threat to both consumers and enterprises. According to AVERT's estimates, half or more of the computers connected to the Internet aren't properly patched or updated. Not good, especially when the number of vulnerabilities spotted in the first quarter of 2005 was up six percent over the same quarter last year. While traditional viruses may be on the way out, other threats, such as phishing, have stepped in to fill the gap said Vincent Gullotto, the vice president of AVERT. "I think we'll see a reduction in the number of traditional phishing sites that entice people to divulge information," he said. "Instead, we'll see programs that are pure spyware that can directly target the clientele they want, to get the data they need." AVERT Report: http://www.mcafeesecurity.com/us/about/press/corporate/2005/ 20050425_185320.htm

---

Category 31.1 *Surveys, studies, audits of security*

2005-05-02 **study antivirus software media playing hacking operating system autoupdate patching helpful security**

DHS IAIP Daily;
http://www.reuters.com/newsArticle.jhtml?type=technologyNews
&storyID=8359020

STUDY SHOWS HACKERS WIDENING FOCUS

Online criminals turned their attention to antivirus software and media players in the first three months of 2005 as they sought new ways to take control of users' computers, according to a survey released on Monday, May 2. While hackers continued to poke new holes in Microsoft's Windows operating system, they increasingly exploited flaws in software made by other companies as well, the nonprofit SANS Institute found. As more Windows users agreed to receive security upgrades automatically, hackers looked to take advantage of other software programs that might not be patched as frequently, the head of the cybersecurity training and research organization said. "Operating systems have gotten better at finding and fixing things and auto-updating, so it's less fertile territory for the hackers," said SANS Chief Executive Alan Paller. More than 600 new Internet security holes have surfaced in 2005 so far, SANS found. Report: http://www.sans.org/top20/Q1-2005update

---

Category 31.1 *Surveys, studies, audits of security*

2005-05-13 **US Government Accountability Office GAO emerging cybersecurity issues report FISMA**

DHS IAIP Daily; http://www.gao.gov/cgi−bin/getrpt?GAO−05−231

INFORMATION SECURITY: EMERGING CYBERSECURITY ISSUES THREATEN FEDERAL INFORMATION SYSTEMS (REPORT)

Spam, phishing, and spyware pose security risks to federal information systems. The blending of these threats creates additional risks that cannot be easily mitigated with currently available tools. Most agencies were not applying the information security program requirements of the Federal Information Security Management Act of 2002 (FISMA) to these emerging threats. Pursuant to FISMA, the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS) share responsibility for the federal government's capability to detect, analyze, and respond to cybersecurity incidents. However, governmentwide guidance has not been issued to clarify to agencies which incidents they should be reporting, as well as how and to whom they should report. The Government Accountability Office (GAO) recommends that the director, OMB, ensure that agencies address emerging cybersecurity threats in their FISMA-required information security program and coordinate with DHS and the Department of Justice to establish guidance for agencies on how to appropriately address and report incidents of emerging threats. OMB representatives generally agreed with GAO findings and conclusions and indicated their plans to address the recommendations. Highlights: http://www.gao.gov/highlights/d05231high.pdf

---

Category 31.1 *Surveys, studies, audits of security*

2005-05-17 **poll study firewall security lax e-mail virus executables phishing**

DHS IAIP Daily; http://www.vnunet.com/vnunet/news/2135301/lax−security−
leavi ng−networks−wide−open

LAX SECURITY LEAVES NETWORKS WIDE OPEN

Lax firewall security is leaving companies open to the installation of malicious software on their internal networks, a newly published Harris poll has warned. Fewer than half of companies block executable files from the Internet, and the same percentage fail to prevent such software coming in via instant messaging. Some 40 percent do not even block executables in email, the major cause of virus infections. The phishing threat was highlighted in the research as a major problem. Over 80 percent of those questioned indicated that their company had received phishing emails, and 45 percent said that employees had clicked through to the bogus websites. Lack of awareness is key to this problem, according to the poll. Two thirds of employees claimed not to know what phishing is, and half of all companies admitted to having no Internet security training.

Category 31.1 Surveys, studies, audits of security

2005-05-19 **Juniper Network study Internet Protocol IPv6 interest lagging**

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml?artic leID=163105617

INTEREST IN IPV6 LAGGING

Although it has been in the works for a decade, the next-generation Internet protocol IPv6 has failed to excite the interest of key decision makers in the federal government and private sector, according to a survey by equipment vendor Juniper Networks. Juniper's Federal IPv6 IQ Study found that less than 7% of respondents consider IPv6 "very important to achieving their IT goals," despite the fact that the protocol is designed to address, among other things, many of the quality of service, security, and network management issues that concern them. The Federal government is particularly indifferent to IPv6 and lags well behind the private sector in migration planning and awareness. Published by the Internet Engineering Task Force in RFC2460 in 1995, IPv6 provides a larger IP address space and provides native support for packet encryption, header authentication, Ipsec virtual private networking, multicasting and dynamic address configuration. Study: http://www.juniper.net/federal/IPv6/

Category 31.1 Surveys, studies, audits of security

2005-06-01 **survey study audit US Internet users exploitation risk fraud phishing privacy policy**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/story/0 ,10801,102155,00.html

STUDY: U.S. INTERNET USERS AT RISK FOR ONLINE EXPLOITATION

U.S. Internet users are dangerously ignorant about the type of data that Website owners collect from them and how that data is used, according to a new study by the University of Pennsylvania's Annenberg Public Policy Center. The lack of awareness makes U.S. Internet users vulnerable to online exploitation, such as misuse of personal information, fraud and overcharging, the study said. Titled "Open to Exploitation: American Shoppers Online and Offline," the study involved 1,500 adult U.S. Internet users who were asked true-or-false questions about topics such as Website privacy policies and retailers' pricing schemes. Respondents on average failed the test. According to the authors, some alarming findings include: seventy-five percent of respondents wrongly believe that if a Website has a privacy policy, it won't share their information with third parties and that almost half of the respondents couldn't identify "phishing" scam e-mailmessages. To address the problems identified by the study, the authors proposed replacing the term "Privacy Policy" with "Using Your Information," teaching consumer education and media literacy taught in elementary, middle and high schools in the U.S., and requiring online retailers to disclose what data they have collected about customers. Study: http://www.annenbergpublicpolicycenter.org/04_info_society/T urow_%20APPC_Press_Release_WEB_FINAL.pdf

---

Category 31.1 Surveys, studies, audits of security

2005-06-08 **US Army Fort Hood base information security problem consolidation**

DHS IAIP Daily; http://www.fcw.com/article89132−06−08−05−Web

CYBERSECURITY PLAGUES FORT HOOD ARMY BASE

Fort Hood, TX, the largest Army base in the world and home of the 4th Infantry Division -- the service's first digitized force -- has a huge information security problem, said Major General Dennis Moran, the Army's director of information operations, network and space in the Office of the Chief Information Officer. He spoke June 8 at the Army Information Technology Conference sponsored by the Army Small Computer Program. Some Army IT leaders think the best way to solve the information security problem at Fort Hood is to operate IT as an enterprise. For example, the base has 96 domains on the military's unclassified network. Consolidating e-mail, servers and storage systems would improve network management, operations and security, Moran said. But Fort Hood technology workers resisted the consolidation idea. The Army's IT leaders must resolve the tension between the Army's need to operate IT as an enterprise and IT workers' unique requirements at bases, Moran said.

Category 31.1 *Surveys, studies, audits of security*

2005-06-14 **Web Internet browser attacks increase virus decrease**

DHS IAIP Daily; http://news.com.com/Browser−based+attacks+increase+as+viruse s+decrease/2100−7349_3−5747050.html

BROWSER-BASED ATTACKS INCREASE AS VIRUSES DECREASE

As the threat to IT operations by viruses and worms dips, browser-based attacks are increasing, according to a technology trade organization. The Computing Technology Industry Association, or CompTIA, on Tuesday, June 14, released its third annual report on IT security and the work force. The survey of nearly 500 organizations, found that 56.6 percent had been the victim of a browser-based attack, up from 36.8 percent a year ago and a quarter two years ago, CompTIA said. Browser-based attacks often take advantage of security flaws in Web browsers and other components of the user's PC such as the operating system. The attackers' objective can be to sabotage a computer or steal private data, and the attacks can be launched when a person visits a Web page that appears harmless but contains malicious code. Still, viruses and worms continue to be the number one IT security threat, though the number of these attacks has dipped slightly. Two-thirds of organizations reported they had experienced such attacks in the past year, down slightly from 68.6 percent a year ago. Study Press Release: http://www.comptia.org/pressroom/get_pr.aspx?prid=620

Category 31.1 *Surveys, studies, audits of security*

2005-06-15 **security survey poll US citizens government Internet safer**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/content/article/2005/06 /15/AR2005061500175.htm

POLL: MOST AMERICANS WANT U.S. GOVERNMENT TO MAKE INTERNET SAFE

Most Americans believe the government should do more to make the Internet safe, but they don't trust the federal institutions that are largely responsible for creating and enforcing laws online, according to a new industry survey. People who were questioned expressed concerns over threats from identity theft, computer viruses and unwanted "spam" e-mails. But they held low opinions toward Congress and the Federal Trade Commission, which protects consumers against Internet fraud. The FBI scored more favorably among Internet users in the survey but still lower than technology companies. The survey was funded by the Washington-based Cyber Security Industry Alliance. "There are some mixed signals here," said Paul Kurtz, the group's executive director and a former White House cybersecurity official. "There is definitely a desire to see government provide more leadership, but there is some anxiety about what ultimately might come out." The survey said 71 percent of people believe Congress needs to pass new laws to keep the Internet safe. Survey: https://www.csialliance.org/resources/pdfs/CSIA_Survey_on_Spyware_and_Identity_Theft_White_Paper.PDF

Category 31.1 *Surveys, studies, audits of security*

2005-06-16 **US government audit survey study report agency security flaws failures weaknesses risk management summary**

RISKS; http://www.gao.gov/cgi-bin/getrpt?GAO-05-231 23 91

GAO SURVEY OF US GOVERNMENT AGENCY SECURITY FAILURES

Al Macintyre reported:

>The GAO surveyed what passes for computer security at scores of US Government agencies, and conducted some tests to see what is needed. This investigative arm of the US Congress determined that the fast majority of US Gov agencies are oblivious to most of the threats, detailing what they found in a 79 page report
http://www.gao.gov/cgi-bin/getrpt?GAO-05-231
with a 1 page summary
http://www.gao.gov/highlights/d05231high.pdf

Your pal Al read through the whole story and wrote up a 5 page summary which you can find in the archives of other discussion groups
http://groups.yahoo.com/group/e-com-sec/message/1729
http://groups.yahoo.com/group/TYR/message/23897
http://groups.yahoo.com/group/VeeWire/message/2736

<

Category 31.1 Surveys, studies, audits of security

2005-06-24 **survey IT managers gain core passwords easily**

DHS IAIP Daily; http://news.bbc.co.uk/1/hi/business/4618691.stm

COMPUTER PASSWORDS 'UP FOR GRABS' ACCORDING TO IT SECURITY FIRM

Half of IT managers employed by large-sized companies believe it would be relatively easy to gain the core passwords for their computer systems. That is the warning of a survey by IT security firm, Cyber-Ark. It said that ten percent of firms never changed their central administrative passwords. A further five percent did not even bother altering the manufacturer's default password that came with the system. The survey also found one IT boss who kept all passwords on his mobile phone. Less than a third of IT managers store key passwords digitally, the survey of 175 IT professionals revealed. The remainder continued to keep paper copies, stored everywhere from locked cabinets to safes. About 25% of IT staff could, as a result, access the core passwords without official permission, the survey said. The survey found that IT managers estimate 19% of general staff in their firms still keep their passwords on notepaper beside their computers. Cyber-Ark Press Release: http://www.cyber-ark.com/networkvaultnews/pr_20050608.htm

---

Category 31.1 Surveys, studies, audits of security

2005-06-28 **study security executives under pressure under-prepared difficult job**

DHS IAIP Daily; http://www.esecurityplanet.com/trends/article.php/3516156

SECURITY EXECUTIVES: UNDER PRESSURE AND UNDER-PREPARED

A new survey of corporate security executives shows that their jobs are more difficult to handle than just a year ago, and they're not prepared to handle some significant security issues. Nearly 100 percent of CSOs say they are well prepared to handle spam, malware, denial-of-service attacks, and hacker attacks, according to a survey by CSO Interchange at a conference held last week in Chicago, IL, for chief security officers. However, 88 percent say their organizations are least prepared to handle inadvertent loss of data, social engineering and inappropriate use. The survey also shows that sixty-four percent of CSOs are more concerned about compliance this year than they were last year, and 38 percent report their budget for compliance solutions grew during the past year; seventy-four percent say their organization must comply with more than five laws and regulations; sixty-eight percent say their security budget is less than 10 percent of their total IT budget; eighty-three percent outsource less than 10 percent of their security, and 40 percent do not outsource security processes at all, and seventy percent say they do not receive sufficient early warning for cyber attacks. Survey results: http://www.csointerchange.org/docs/2005-06-24-chicago-pollin g-results.pdf

---

Category 31.1 Surveys, studies, audits of security

2005-06-29 **Government Accountability Office GAO IPv6 transition security risks testimony**

DHS IAIP Daily; http://www.gao.gov/new.items/d05845t.pdf

IPv6: FEDERAL AGENCIES NEED TO PLAN FOR TRANSITION AND MANAGE SECURITY RISKS (TESTIMONY)

For its testimony, GAO was asked to discuss the findings and recommendations of its recent study of IPv6 (GAO-05-471). In this study, GAO was asked to (1) describe the key characteristics of IPv6; (2) identify the key planning considerations for federal agencies in transitioning from IPv4 to IPv6; and (3) determine the progress made by the Department of Defense (DOD) and other major agencies in the transition to IPv6. DOD has made progress in developing a business case, policies, timelines, and processes for transitioning to IPv6. Unlike DOD, the majority of other major federal agencies reported that they have not yet initiated key planning efforts for IPv6. In its report, GAO recommended, among other things, that the Director of the Office of Management and Budget (OMB) instruct agencies to begin to address key planning considerations for the IPv6 transition and that agencies act to mitigate near-term IPv6 security risks. Highlights: http://www.gao.gov/highlights/d05845thigh.pdf

---

Category 31.1 Surveys, studies, audits of security

2005-07-05 **study malicious code spike 2005 Sophos professional crimes Trojan horses**

EDUPAGE; http://news.com.com/2100-7349_3-5774841.html

MALWARE MUSHROOMS TO NEW LEVELS

Incidents involving malicious computer code have spiked this year, according to computer security firm Sophos, which attributes the sharp rise to growing numbers of professional criminals who are using the Internet to make money. The company said it has tracked nearly 8,000 new varieties of malware in the first six months of the year, an increase of 60 percent over the same period last year. Graham Cluley, senior technology consultant at Sophos, noted that the trend in malware has been toward Trojan horses and away from viruses and worms. Trojan horses can allow hackers to access information on a compromised system or to take over the system completely. It is these Trojans, said Cluley, that criminals are using to make money from unsuspecting users. Although Microsoft products remained at the top of the list of most frequently targeted applications, Cluley said malware is also being written to take advantage of Linux, UNIX, and Mac systems. CNET, 5 July 2005

Category 31.1 Surveys, studies, audits of security

2005-07-08 **communications program information warfare battlespace software quality assurance QA problems failures challenges schedule report investigation network**

RISKS; http://www.gcn.com/vol1_no1/daily-updates/36302-1.html 23 93

GAO REPORT SLAMS US ARMY'S FUTURE COMBAT SYSTEMS NETWORKS PROJECTS

The major communications programs that will support the Army's transformational Future Combat Systems initiative are in jeopardy of failing to meet technical challenges and an accelerated schedule, according to the Government Accountability Office. GAO found that each of the communications pillars of the Army's Future Combat Systems (FCS) program - two Joint Tactical Radio System (JTRS) clusters, the Warfighter Information Network-Tactical (WIN-T) program and the System of Systems Common Operating Environment (SOSCOE) - would likely fail to meet aggressive schedules due to immature technologies.

"As currently structured, the JTRS, WIN-T and SOSCOE programs are at risk of not delivering intended capabilities when needed, particularly for the first spiral of FCS," according to GAO. "They continue to struggle to meet an ambitious set of user requirements, steep technical challenges and stringent time frames."

FCS is designed to link 18 manned and unmanned weapons systems via a common computer network known as WIN-T and the System of Systems Common Operating Environment.

The Army restructured its FCS program last year into spirals, with officials announcing the first spiral would happen in fiscal 2008. But GAO said the first spiral may not demonstrate key networking capabilities.

GAO found the FCS program faces network, developmental and financial challenges that continue to slow progress. FCS' information network is dependent on the success of JTRS, WIN-T and SOSCOE - programs that are not included in FCS costs.

"Because JTRS, WIN-T and SOSCOE all rely on significant advances in current technologies and capabilities and must be fully integrated to realize FCS, there are substantial risks to this effort," wrote Paul L. Francis, GAO's director of acquisition and sourcing management, in the report.

[Abstract by Pete Mellor]

Category 31.1 Surveys, studies, audits of security

2005-07-18 **study cyber attack damages drop CSI FBI**

EDUPAGE; http://www.theregister.com/2005/07/18/csi_fbi_security_survey/

STUDY SHOWS DROP IN DAMAGES FROM CYBER ATTACKS

A new study shows a significant drop in the amount of damage caused by cyber attacks as well as a shift in the kinds of attacks that are most commonly reported. Researchers from the University of Maryland conducted the Computer Crime and Security Survey on behalf of the Computer Security Institute (CSI), with consultation from security experts at the FBI. The survey questioned IT security officials at 700 private companies, governmental agencies, and universities and found that the average cost per security incident was $204,000, down from $526,000 a year earlier. Viruses remain the most frequent type of attack (32 percent), but unauthorized access rose to second on the list at 24 percent. Chris Keating, director of CSI, noted that schemes to steal individuals' identities are a growing concern. The survey, he said, indicates "more financial damage due to theft of sensitive company data," a trend that should press network managers to ensure the security of enterprise systems. The Register, 18 July 2005

Category 31.1 *Surveys, studies, audits of security*

2005-07-19 **ComputerWeekly Mobile phones crisis London bombing security experts plans networks explosions Access Overload Control Gartner**

DHS IAIP Daily;
http://www.computerweekly.com/Articles/2005/07/19/210901/Mob

MOBILE PHONES OF LITTLE USE IN CRISIS

The London bombing highlighted important gaps in business continuity plans, according to security experts. Many firms discovered, to their cost, that their business continuity plans relied on being able to communicate with key staff via mobile phone networks, which were out of action or unreliable for most of the day the bombs exploded. Others found themselves in difficulty when key staff were unable to make it into work, said Andy Tomkinson, a director at the Business Continuity Institute. In the aftermath of the explosions police invoked a system called Access Overload Control, which shuts down large swathes of the mobile network, to free-up communications for the emergency services. Corporate e-mail systems also came under strain, which in some cases caused severe disruption to businesses. Some companies instructed staff to send text messages rather than make mobile phone calls--a lesson learned from the central London power cut two years ago. Analyst firm Gartner said that the attacks showed that organizations need to have viable, tested business continuity plans, which are focused on people, not just business assets.

Category 31.1 *Surveys, studies, audits of security*

2005-07-25 **study report SANS hacker new targets vulnerabilities patch update**

EDUPAGE; http://online.wsj.com/article/0,,SB112224497897894400,00.html

HACKERS FINDING NEW TARGETS

According to a new report from the SANS Institute, the number of computer hacking incidents is rising, and the targets of such hacks are increasingly software applications rather than operating systems. The organization found that the number of vulnerabilities reported was up
11 percent from the first quarter of the year to the second, and up nearly 20 percent from a year earlier. Alan Paller, SANS's research director, said the situation is getting worse. As operating systems become more secure, hackers are turning to applications, such as Apple's iTunes and RealNetworks's RealPlayer. Hackers are also focusing efforts on backup systems, particularly those of Computer Associates and Veritas Software. Because backup systems typically contain vast amounts of confidential corporate data, they represent an attractive target. SANS noted that the best way to avoid such hacking threats is to install all software patches, keep antivirus tools up to date, and be prudent in opening e-mail attachments. Wall Street Journal, 25 July 2005 (sub. req'd)

Category 31.1 *Surveys, studies, audits of security*

2005-07-27 **national policy reports recommendations telework research development children education awareness ethics**

RISKS; http://www.csialliance.org 23 95

THREE REPORTS FROM THE COMPUTER SECURITY INDUSTRY ALLIANCE

Gene Spafford ("Spaf") noted that the Computer Security Industry Alliance issued three reports of possible interest:

* CSIA Calls for Increased Adoption of Telework by the Federal Government: Cites Need to Ensure Continuity of Federal Operations in a Disaster
https://www.csialliance.org/resources/pdfs/CSIA_Telework.pdf

* CSIA Urges the Administration and Congress to Elevate Cyber Security and Research & Development Efforts: CSIA voices concern over the dissolution of a Presidential committee focused on information security issues and calls for a national vision for cyber security R&D.
Https://www.csialliance.org/resources/pdfs/CSIA_RD.pdf

* CSIA Calls for a National K-12 Cyber Awareness Program: A Focused, Organized National Effort is Needed to Teach Children Cyber Security, Cyber Ethics and Cyber Safety.
https://www.csialliance.org/resources/pdfs/K12_White_Paper.pdf

---

Category 31.1 *Surveys, studies, audits of security*

2005-08-03 **business encryption roll out trend key management complexity survey**

DHS IAIP Daily;
http://www.techworld.com/security/news/index.cfm?NewsID=4150
&Page=1&pagePos=2

KEY MANAGEMENT HOLDING BACK ENCRYPTION

Businesses are keener than ever to roll out data encryption, but are still struggling with the complexity of key management, a new survey has concluded. The survey was carried out by UK encryption specialist nCipher, sampling 237 "decision makers" at large enterprises across the globe. The main problem appears to be key management with nine percent of those surveyed having more than 10,000 keys on servers, and 11 percent having the same number on desktops. Further down the scale, 16 percent had 1,000 keys on servers, with almost a quarter having the same number of desktops. Underscoring this issue, 31 percent of managers with 500 or more keys in their organizations admitted they knew little or nothing about available key management systems. The survey found that encryption is rapidly becoming a mainstream technology, with its use now mandated across a wide range of applications. Drivers included government legislation, and private sector date protection standards developed by groups such as the Payment Card Industry. Survey: http://www.ncipher.com/crypto2005

Category 31.1 *Surveys, studies, audits of security*

2005-09-01 **study colleges higher education university computer security concerns vulnerabilities**

EDUPAGE; http://www.csmonitor.com/2005/0901/p12s02-legn.html

COLLEGES DEALING WITH COMPUTER SECURITY CONCERNS

As the number of computers on college campuses rises, and as IT becomes increasingly rooted in campus activities, higher education officials find themselves facing expanding numbers and kinds of threats to vulnerabilities in computer security. According to the Privacy Rights Clearinghouse (PRC), 50 million people have been involved in data breaches over the past seven months, including more than 30 incidents on U.S. college and university campuses. Complicating the challenge to IT security staff is the historically open nature of academic settings, a characteristic often at odds with strong computer security. Another factor making life difficult for IT staff are the computers that students bring to campus with them, often with inadequate or poorly configured security features. Jack Suess, vice president of information technology at the University of Maryland Baltimore County, however, noted that of the 11,000 to 12,000 computers on his campus this year, "there's probably only 200 or 250 I'm really worried about." Christian Science Monitor, 1 September 2005

Category 31.1 *Surveys, studies, audits of security*

2005-09-06 **online banking e-commerce stalling hacker cracking survey study**

EDUPAGE; http://news.com.com/2100-1038_3-5851061.html

GROWTH OF ONLINE BANKING STALLS AMID HACKING FEAR

A new survey by Ipsos Insight shows that the number of people who use the Internet for banking has reached a plateau, but that those who do their banking online are conducting growing numbers of transactions. According to the survey, roughly 39 percent of Americans use the Internet for personal banking--the same number as a year ago. Concern over online security for personal information was identified as a leading reason why more people are not turning to the Web for banking. Survey respondents expressed concerns about the possibility of hackers stealing sensitive information, about online scams that dupe users into revealing personal data, and about the practice among some banks of selling customers' personal information to third parties. Of those who conduct banking online, most are using the Web for growing numbers of financial transactions, including paying bills and managing retirement accounts, according to the survey. CNET, 6 September 2005

Category 31.1 *Surveys, studies, audits of security*

2005-09-13 **IM threats survey people unaware**

DHS IAIP Daily; http://www.webpronews.com/news/ebusinessnews/wpn−45−
20050913 MostPeopleUnawareofIMThreats.html

MOST PEOPLE UNAWARE OF IM THREATS

A recent survey conducted by IMLogic found that most people unknowingly expose their computers and company networks to security threats. The survey found that the 78% of uses belive there is no threat in instant messaging. In addition, 45% of users use IM at work because they believe their communication is unmonitored.

Category 31.1 *Surveys, studies, audits of security*

2005-10-14 **peer-to-peer P2P activity colleges survey network administrators security concern ResNet organization**

EDUPAGE; http://chronicle.com/daily/2005/10/2005101402t.htm

RESULTS OF RESNET SURVEY RELEASED

The ResNet Organization has released results from a survey it conducted earlier this year of those responsible for residential networks at 224 colleges and universities. The leading concern among network administrators is security, with P2P activity coming in at a distant second. Administrators also put security at the top of the list of issues they expect to take significant amounts of time and resources over the next couple of years, with wireless networking coming in second and P2P issues falling to seventh. David G. Futey, associate director of academic computing at Stanford University and a member of the ResNet Organization, said the survey provides new insight into "determining what a res-net service area is at institutions, the level of services it provides, and the technology supported through it." Futey commented that he was surprised to see that of the respondents to the survey, nearly half had not installed wireless networks. The survey also indicated that more than half of responding institutions charge technology fees but that at about half of those that charge a fee, no part of the fee supports residential networks. Chronicle of Higher Education, 14 October 2005 (sub. req'd)

Category 31.1 *Surveys, studies, audits of security*

2005-10-24 **IT planning bird flu pandemic threat outbreak businesses Companies laptops virtual network connections office**

DHS IAIP Daily; http://www.computerweekly.com/Articles/Article.aspx?liArticleID=212598&PrinterFriendly=true

IT PLANNING VITAL TO MEET BIRD FLU PANDEMIC THREAT

To prevent a loss of IT functionality in the case of a pandemic, Gartner analyst Dion Wiggins says that it is imperative that companies start planning for a potential outbreak and to look at ways they could use IT to help their businesses continue to function. Companies are encouraged to sign contracts to ship in laptops for staff at short notice, and to provide them with secure virtual private network connections to access office systems. In addition, firms that are heavily reliant on their IT departments should split key IT staff into shifts to maintain consistent coverage. Jim Norton, senior policy adviser at the Institute of Directors, says businesses that invest in broadband and e-commerce technologies are better placed to cope with a pandemic. Business continuity experts said a flu pandemic could cause far more disruption to businesses than the last major flu outbreak in 1968, when businesses were less dependent on a small number of staff with key skills and the smooth running of the transport system for just-in-time deliveries. Gartner Press Release: http://www.gartner.com/press_releases/asset_138278_11.html

---

Category 31.1 *Surveys, studies, audits of security*

2005-10-31 **survey census US computer Internet usage report increase**

DHS IAIP Daily; http://www.govtech.net/news/news.php?id=97088

U.S. CENSUS BUREAU RELEASES REPORT ON COMPUTER AND INTERNET USAGE

The U.S. Census Bureau has released the "Computer and Internet Use in the United States: 2003" report. The report states that 40 percent of adults used the Internet to obtain news, weather, or sports information in 2003 -- a sharp increase from only seven percent six years earlier. Also, more than half of adults (55 percent) used e-mail or instant messaging in 2003, which is a dramatic increase from the 12 percent who did so in 1997. Report: http://www.census.gov/population/www/socdemo/computer.html

---

Category 31.1 *Surveys, studies, audits of security*

2005-11-02 **study cybercrime fighting strategy effectiveness lack resources Trend Micro anti-virus vendor**

DHS IAIP Daily; http://www.snpx.com/cgi−bin/news55.cgi?target=115933550?−11434

CYBERCRIME-STOPPING STRATEGIES FALL SHORT ACCORDING TO STUDY

A Trend Micro study, indicates that smaller organizations, with a lack of IT support, are not able to handle security threats effectively. Requiring them to have security measures does not mean that they will actually be able to afford it. The study said that "resource-strapped organizations" with little or no IT support face a challenge in protecting themselves from malware, or attackers. said Steve Quane, general manager of Trend Micro's small and medium business operations, states "Encounters with security threats are rising faster in smaller organizations, but these same organizations are restricted by time, cost, and available resources." Within a matter of months all DMA members using e-mail for marketing are will be going to be required to use e-mail authentication systems that verify the authenticity of all e-mail messages they send. John A. Greco, Jr., president and chief executive officer of the DMA stated, "Consumers can have more confidence they are getting a legitimate, valid offer from a trusted source. Marketers get fewer false positives, increased deliverability and better protection for their brands from illegal use. It's a win-win for everybody."

Category 31.1 *Surveys, studies, audits of security*

2005-11-04 **survey IT executives insider threat worry concern security**

DHS IAIP Daily; http://www.esecurityplanet.com/prevention/article.php/3561761

INSIDER THREATS GIVING IT EXECS NIGHTMARES

Sixty-nine percent of 110 senior executives at Fortune 1,000 companies say they are 'very concerned' about insider network attacks or data theft, according to a study by Caymas Systems, a network security technology firm. Only 13 percent says they are not worried at all. Sanjay Uppal, a vice president at Caymas Systems, claims 30 percent of people who come in and work on your average network every day are temporary workers. And that brings up specific threat concerns. But he also says that IT and security administrators should not forget about permanent workers and the havoc they can wreak. Uppal says insider security threats definitely need to be dealt with quickly. Uppal recommends that workers should be limited as to what parts of the network they can access. Someone working in production shouldn't be able to access financials. And someone working in the financial department, should be able to access personnel records and reviews.

Category 31.1 *Surveys, studies, audits of security*

2005-11-07 **study survey computer problem carelessness cause virus worm hacking data loss**

EDUPAGE; http://chronicle.com/daily/2005/11/2005110701t.htm

CARELESSNESS CITED AS FACTOR IN COMPUTER PROBLEMS

An in-depth study of more than 300 computer and network problems at 36 colleges and universities identified carelessness of students and staff as one of the leading causes of such problems. Despite widespread perceptions that issues such as viruses and loss of confidential data are largely the result of malicious behavior, those involved in the study found that careless actions by students or staff were the primary cause for 40 percent of the incidents studied. Virginia E. Rezmierski, adjunct associate professor at the University of Michigan at Ann Arbor and leader of the research, said she was surprised to learn that external factors didn't play a larger role in computer problems. Primarily, she said, the problems resulted from inadequate training to help computer users avoid trouble and from insufficient policies to deal with problems that do arise. Rezmierski said the results support her contention that many colleges and universities moved too quickly to implement IT systems without necessary "rules and policies about how we want to operate in a shared-resource environment." Chronicle of Higher Education, 7 November 2005 (sub. req'd)

Category 31.1 Surveys, studies, audits of security

2005-11-09 **survey study online banking e-commerce security consumer worry**

EDUPAGE; http://news.com.com/2100-1029_3-5941531.html

CONSUMERS WORRYING OVER ONLINE BANKING

Even as federal regulators insist on tighter security controls for online banking, some consumers are deciding that the convenience is not worth the risk. Results of a survey announced this week at a forum on identity theft indicate that nearly one in five Americans who have conducted banking transactions online have limited or ended their online banking due to security concerns. The Federal Financial Institutions Examination Council, which includes the Federal Reserve and the Federal Deposit Insurance Corporation, recently issued guidelines requiring banks to add a second level of authentication for online banking transactions. That level could include smart cards, password tokens, or biometric identification. According to the Federal Trade Commission, 10 million Americans are victims of identity theft each year, and federal data estimate that each victim spends about 90 hours and $1,700 fixing matters. The survey also indicated that 94 percent of consumers would accept added online security, though 81 percent said they would not want to pay for such extra measures. CNET, 9 November 2005

Category 31.1 Surveys, studies, audits of security

2005-11-17 **security study telecom consolidation disaster recovery network reliability DHS**

DHS IAIP Daily; http://www.zra.com/docs/ZRAPR.pdf

STUDY FINDS TELECOM CONSOLIDATION WILL AID NETWORK RELIABILITY DURING DISASTERS

The current consolidation occurring in the telecommunications industry is a step toward ensuring network reliability following threats to our nation's security, according to a study released by homeland security expert Lee Zeichner. The study, entitled "State Public Utility Commissioners: Homeland Security & National Preparedness Responsibilities," concludes that state public utility commissioners' current review of major telecom mergers must address traditional regulatory issues as well as issues like network reliability and resilience. According to the study, "Telecommunications regulators can affect state and local government response to catastrophic disasters in profound and meaningful ways, directly impacting consumers as well as small to large-sized corporations." The study states that with multiple carriers and multiple networks, there is no comprehensive communications infrastructure map to guide disaster planning and response. "A certain amount of consolidation…is critical to support delivery of essential citizen services in the aftermath of a disaster." The study offers recommendations for state public utility commissioners to emphasize network reliability and resiliency while maximizing traditional regulatory issues. These include the need to consider issues related to communications resiliency during their deliberations and the adverse impact of divestiture requirements on resiliency during merger proceeding. They should also commit to resolving operational impediments. Study: http://www.zra.com/docs/UC&CR.pdf

---

Category 31.1 Surveys, studies, audits of security

2005-11-18 **report IT security information analytics software market billion dollars**

DHS IAIP Daily;
http://www.washingtontechnology.com/news/1_1/daily_news/2744 7−1.html

MARKET FOR INFORMATICS REACHES ONE BILLION PER YEAR

According to a report from C.E. Unterberg, Towbin Inc. of New York and business incubator Chesapeake Innovation Center of Annapolis, MD, intelligence and security informatics IT is now one billion a year. Since 9-11, the urgent need for homeland security and an increase in available government funding have been driving the market for advanced anti-terrorism IT. Sales of counterterrorism analytics and software for both private and public companies are expanding at an estimated 20 percent a year and have accounted for two billion in mergers and acquisitions in the last 18 months, according to a news release about the report. Report (registration required): http://www.cic-tech.org/register.html

---

Category 31.1 Surveys, studies, audits of security

2005-11-21 **survey business continuity data recovery disasters NIST new technology**

DHS IAIP Daily; http://www.gcn.com/24_33/tech−report/37577−1.html

DATA DISASTER: WHEN CONTINUITY-OF-OPERATIONS PLANS AREN'T ENOUGH

Disasters -- both natural and man-made – require that agencies ensure that data held on IT systems and devices remain accessible in order to support mission-critical operations. Continuity-of-operations plans—those that keep government going in the face of emergencies—are important, but far from foolproof. In a recent survey by Asigra Inc. of Toronto, 75 percent of respondents said their organizations had lost backed-up data because of unreadable, lost, or stolen media. Almost two-thirds of the respondents had run into unreadable backup tapes when trying to recover data. New data-handling techniques not designed for disaster recovery could apply to agencies trying to reconstruct critical information. One application being created by the National Institute of Standards (NIST) and Technology for courtroom investigations is high-resolution images of magnetic data that can tell an investigator when data has been written, erased or altered, said physicist David Pappas, project lead at NIST. The technique, called second harmonic magnetoresistive microscopy, uses powerful magnetic readers designed for server drives to image the fields on other magnetic media, such as tapes and disks. "You're actually taking a picture of the magnetic field above it, rather than just scanning it really fast and averaging the data," Pappas said.

Category 31.1 Surveys, studies, audits of security

2005-11-22 **report study SANS cross-platform applications network operation system hacker targets**

EDUPAGE; http://www.fcw.com/article91516-11-22-05-Web

SANS REPORT SHOWS DIRECTION OF HACKERS

A new report from the SANS Institute identified cross-platform applications and network operating systems as emerging targets for hackers. The applications cited include backup software, antivirus software, database software, and media players; operating systems for routers and other network devices were also singled out. The report, "20 Most Critical Internet Security Vulnerabilities in 2005," noted that 13 of the top 20 were in these two types of technology, which are among the least protected computer assets in many organizations. In the 2004 SANS report, neither category of technology was identified among the worst threats; the 2005 report indicates that these types of attacks account for 65 percent of the worst threats. Alan Paller, director of research at the SANS Institute, commented, "Six years ago, attackers targeted operating systems." Since then, makers of operating systems have improved protections and implemented automatic patching. "Now," he said, "the attackers are targeting popular applications, and the vendors of those applications do not do automated patching. Here we go again." Federal Computer Week, 22 November 2005

Category 31.1 Surveys, studies, audits of security

2005-11-22 **survey study SANS cyber criminal target popular applications network systems**

DHS IAIP Daily; http://www.sans.org/top20/ Source: http://fcw.com/article91516−11−22−05−Web

CYBERCRIMINALS TARGETED POPULAR APPLICATIONS, NETWORK SYSTEMS IN 2005

According to the SANS Institute's latest update to its 20 Most Critical Internet Security Vulnerabilities in 2005 report, cybercriminals have launched massive attacks on two largely undefended fronts in cyberspace, leaving government and industry more vulnerable than they have been in years to data theft and security breaches. Ten of the vulnerabilities were in cross-platform applications installed on millions of systems, including backup software, antivirus software, database software, and media players. Three affected network operating systems that control routers, switches, and other devices. Alan Paller, director of research at the SANS Institute, stated: "The bottom line is that security has been set back nearly six years in the past 18 months. Six years ago, attackers targeted operating systems, and the operating system vendors didn't do automated patching. In the intervening years, automated patching protected everyone from government to grandma. Now the attackers are targeting popular applications, and the vendors of those applications do not do automated patching." Since 2003, attackers have infiltrated Defense Department networks by exploiting vulnerabilities in hardware and software.

Category 31.1 *Surveys, studies, audits of security*

2005-12-01 **study Gartner research hurricane Katrina Wilma disaster data storage offsite**

DHS IAIP Daily;
http://www.computerworld.com/hardwaretopics/storage/story/0,
10801,106641,00.html

HURRICANES PROMPT MORE COMPANIES TO STORE DATA OFF-SITE

The number of companies making copies of data to protect it has dramatically risen in the wake of Hurricanes Katrina and Wilma this year, but most of those companies are keeping that duplicate data locally where it's still vulnerable to disasters, according to a survey released Wednesday, November 30, by Gartner Inc. The September survey of 104 North American IT managers showed that 45 percent of respondents back up or replicate data to another disk, up from just six percent who did so in 2004. But 70 percent of the respondents who make backups do so to a local device. Adam Couture, an analyst at Stamford, CT-based Gartner, said that if companies hope to truly protect their data, they have to electronically copy it to an off-site facility either owned by the company or a service provider. The Gartner survey also showed that IT managers are more comfortable considering managed storage services to copy data off-site. Over the past two years, Couture said, surveys have shown that between 30 percent and 40 percent of IT managers would never use a third-party service provider. But in the most recent survey, that number had plummeted to just six percent.

Category 31.1 *Surveys, studies, audits of security*

2005-12-06 **study report computer security threats 2005 increase worms viruses Trojan horses**

DHS IAIP Daily; http://www.techweb.com/wire/security/174901293

SECURITY THREATS INCREASE IN 2005

The number of new worms, viruses, and Trojan horses jumped 48 percent in 2005, a security company said Tuesday, December 6, as it detailed the year's security woes. United Kingdom-based Sophos detected nearly 16,000 new threats from January to November, 2005, a major bump from the 10,724 during the same period in 2004. Every month in 2005 posted larger-than-last-year numbers, but November, which was marked by the debut of a strong Sober.z worm, outpaced all others. By Sophos' records, 1,940 new viruses, worms, Trojans, and spyware threats were spotted last month, its largest-ever monthly increase. If that pace were to continue, the next 12 months would see 23,000 threats. Topping Sophos' top-10 chart was the long-running Zafi.d, a mass-mailed worm that made itself known almost a year ago: It accounted for 16.7 percent of all threats detected during the first 11 months of 2005. Netsky.p took second place, with 15.7 percent, while the new Sober.z came in at third, with six percent. "Given more time, Sober.z would have dominated the chart, but its emergence in late November prevented it from taking pole position," said Graham Cluley, senior technology consultant at Sophos.

Category 31.1 *Surveys, studies, audits of security*

2005-12-06 **technology return-on-investment ROI study academia industry difficult complex problem management issues**

EDUPAGE; http://www.fcw.com/article91625-12-06-05-Web

ACADEMY AND INDUSTRY STUDY ROI

A group of academic and industry researchers will work together on an initiative to create a methodology that organizations can use to study the return on investment (ROI) of technology projects. Governments are increasingly asked to demonstrate the value of taxpayer dollars invested in IT projects. Led by the Center for Technology in Government (CTG) at the State University of New York at Albany and SAP, the effort will include researchers from Harvard University's John F. Kennedy School of Government, Accenture, Gartner Research, Cisco Systems, and North American and European government agencies. Anthony Cresswell, deputy director of CTG, said that calculating ROI for IT projects "has been a complex and difficult problem." He said the new effort will "produce results that will make a major contribution to the ability of governments of all types to enhance the political, social, and economic value they obtain from IT investments." Federal Computer Week, 6 December 2005

Category 31.1 *Surveys, studies, audits of security*

2005-12-08 **study malicious software malware rootkits Sony BMG XCP**

DHS IAIP Daily; http://www.vnunet.com/vnunet/news/2147301/rootkits−storm −mal ware−chart

ROOTKITS STORM MALWARE CHART

The most common rootkit is a spyware application known as Apropos, according to data collected by security experts at F-Secure. Apropos collects system information and data on a user's browsing habits and sends the information back to the application's creators. It is also capable of recording keystrokes and launching a denial of service attack, and can download and install additional software on an infected computer. Rootkits have become a mainstream phenomenon ever since Sony BMG was caught bundling one as part of the XCP anti-piracy technology on some of its audio CDs. Sony used a rootkit to hide the technology, preventing users from uninstalling the application. Hackers originally started using rootkits to build backdoors into computers, but the technology has caught a second wind in recent months as malware creators use rootkits to hide worms and spyware from antivirus and anti-spyware software. In F-Secure's ranking Apropos surpassed the Sony BMG rootkit in the number of infections.

Category 31.1 *Surveys, studies, audits of security*

2005-12-15 **study information security attacks geeks squatters saboteurs insider threat**

DHS IAIP Daily; http://www.theregister.co.uk/2005/12/15/mcafee_internal_security_survey/

GEEKS, SQUATTERS AND SABOTEURS THREATEN CORPORATE SECURITY

Workers across Europe are continuing to place their own companies at risk from information security attacks. This "threat from within" is undermining the investments organizations make to defend against security threats, according to a study by security firm McAfee. The survey, conducted by ICM Research, produced evidence of both ignorance and negligence over the use of company IT resources. One in five workers let family and friends use company laptops and PCs to access the Internet. More than half connect their own devices or gadgets to their work PC and a quarter of these do so every day. Around 60 percent admit to storing personal content on their work PC. One in ten confessed to downloading content at work they shouldn't. Most errant workers put their firms at risk through either complacency or ignorance, but a small minority are believed to be actively seeking to damage the company from within. Five percent of those questioned say they have accessed areas of their IT system they shouldn't have while a very small number admitted to stealing information from company servers.

Category 31.1 *Surveys, studies, audits of security*

2005-12-28 **Criminals viruses security Windows outbreaks Symantec malicious wares inbox programs Sophos firms**

DHS IAIP Daily; http://news.bbc.co.uk/2/hi/technology/4521844.stm

CRIMINALS TARGET VIRUSES FOR CASH

At first glance, 2005 looks like it was a quiet year for computer security because there were far fewer serious Windows virus outbreaks than in 2004. According to figures gathered by security firm Symantec, there were 33 serious outbreaks in 2004. In 2005, there were only six such incidents. "We're talking about a substantial decrease in worldwide pandemics," said Kevin Hogan, senior manager in Symantec's security response team. This decline is taking place because virus makers have largely stopped spreading their malicious wares with mass-mailers that try to infect as many people as possible via their inbox. Instead, virus creators are cranking out more versions of malicious programs than ever before. Year-end statistics from Finnish anti-virus firm F-Secure show that there were 50 percent fewer virus outbreaks in 2005 but the number of malicious programs has grown by, on average, 40 percent for the last two years. Similarly Sophos reported that it found 1,940 new malicious programs in November 2005, the largest increase since records began. Security experts say this explosion in variants is partly driven by a desire to overwhelm anti-virus firms.

Category 31.1 Surveys, studies, audits of security

2005-12-30 **catalog data theft leakage security breaches catalog report summary resource**

Emergent Chaos; Privacy Rights Clearinghouse

CATALOGS OF SECURITY BREACHES

Those looking for summary information about loss of control over data for use in articles or lectures may find the following resources helpful:

* Adam Shostack has put together an extensive list of brief reports on security breaches on his Website. His entries have references but few URLs. By the end of 2005, the breaches catalog included over a hundred cases of data theft and data leakage for the year starting in March. See < http://www.emergentchaos.com/archives/cat_breaches.html >

* The Privacy Rights Clearinghouse has a list of bullet points summarizing hacking incidents, lost backup tapes, compromised passwords, insider attacks, and so on. The incidents start in February 2005 and include estimates of the numbers of victims. The entries have no URLs or citations. Their total of affected people is _at least_ 52 million (!).
See < http://www.privacyrights.org/ar/ChronDataBreaches.htm >

Category 31.1 Surveys, studies, audits of security

2006-01-03 **study survey instant messaging IM attacks jump 826% 2004 2005**

DHS IAIP Daily; http://www.securitypipeline.com/news/175800842 23

DECEMBER INSTANT MESSAGING ATTACKS JUMP 826 PERCENT OVER 2004

Attacks against public instant messaging (IM) networks soared over 800 percent in December 2005, compared to the same month last year, a security company announced Tuesday, January 3. According to IMlogic's Threat Center, December 2005's instant message exploits jumped 826 percent over December 2004, just the latest proof of the expanding threat facing IM users throughout the year. December, however, was slightly off the previous two months. The year's last month saw 241 new threats, said IMlogic, down from the 307 in November and the 294 in October. Combined, the three months showed a 13 percent increase in IM threats over the third quarter of 2005. IM attacks not only continue to grow in number, but also keep gaining in sophistication, said IMlogic chief technology officer Jon Sakoda. MSN was the most heavily-hit IM network in December, added IMlogic, and accounted for 48 percent of the total threats launched. America Online's AIM, meanwhile, tallied 41 percent, while Yahoo's instant messaging network came in a very distant third, with 11 percent. IMlogic year-end results of its IM tracking effort: http://www.imlogic.com/im_threat_center/index.asp

---

Category 31.1 Surveys, studies, audits of security

2006-01-10 **study survey instant messaging IM attacks increase 2005**

DHS IAIP Daily; http://news.com.com/Study+Instant−messaging+attacks+rose+in+ 2005/2100−7349_3−6025226.html?tag=cd.top 23

INSTANT MESSAGING ATTACKS ROSE IN 2005

Security attacks over instant-messaging (IM) networks became more prevalent in 2005, according to a new study. Microsoft's MSN network experienced the largest number of IM security incidents in both 2004 and 2005, while year-on-year incident growth rates were largest on AOL's AIM network, according to the report, published Monday, January 9, by IM security vendor FaceTime Communications. In 2005, MSN had a 57 percent share of the attacks, AOL had 37 percent and Yahoo had six percent, FaceTime said in its "Impact report: Analysis of IM & P2P Threats in 2005." While the incidence rate of attacks over IM is still low compared with e-mail-borne attacks, the rate appears to be increasing rapidly. There were 778 incidents recorded in the fourth quarter of last year compared with 59 in the first quarter, according to the report. Worms and rootkits were at the heart of the main incidents in 2005, said Chris Boyd, security research manager at FaceTime who also warned of the growing danger of cross-network attacks. FaceTime said that exploits can jump networks through IM "consolidation" applications, such as Trillian or Gaim, which let people combine contacts from multiple IM networks on one list. FaceTime's report is available by request: http://www.facetime.com/forms/impact_report2005.aspx

---

Category 31.1 *Surveys, studies, audits of security*

2006-01-11 **study survey Europe IT spending decline shrink**

DHS IAIP Daily; 23
http://www.channelregister.co.uk/2006/01/11/it_spending_shrinks/

EUROPEAN IT SPENDING SHRINKING

IT spending across Europe is under even more pressure and budgets will grow by just 1.6 percent in 2006, compared to 2.9 percent last year. Researchers from Forrester found that more than half of European firms plan to reduce IT budgets this year. The main priority across Europe is for spending on security, anti-virus and host intrusion detection. For IT services price pressure is the main concern, with nearly half of European firms saying that cutting costs is an important or critical priority for the year ahead. Miguel Angel Mendez, associate analyst at Forrester Research, said the caution on IT spending was at odds with people's more optimistic view of their own industries -- 60 percent of respondents expect the coming year to be good or okay for their industries. The feeling in the United Kingdom seems slightly more optimistic -- British firms expect to increase IT spending by 2.3 percent, but only 20 percent of this will go on new developments. Big technology brands such as Cisco, HP, IBM, Microsoft, SAP and Oracle get the lion's share of purchasing preferences.

Category 31.1 *Surveys, studies, audits of security*

2006-01-11 **FBI computer crime survey study attacks succeeding despite security investments**

DHS IAIP Daily; http://searchsecurity.techtarget.com/originalContent/0,28914 23
2,sid14_gci1157706,00.html

FEDERAL BUREAU OF INVESTIGATION SAYS ATTACKS SUCCEEDING DESPITE SECURITY INVESTMENTS

Despite investing in a variety of security technologies, enterprises continue to suffer network attacks at the hands of malware writers and inside operatives, according to an annual Federal Bureau of Investigation (FBI) report released Wednesday, January 11. The 2005 FBI Computer Crime Survey was taken by 2,066 organizations in Iowa, Nebraska, New York, and Texas late last spring, which survey organizers deemed a good sample of enterprises nationwide. The report is designed to "gain an accurate understanding" of computer security incidents experienced "by the full spectrum of sizes and types of organizations within the United States," the FBI said. The 23-question survey is not the same as the CSI/FBI Computer Crime and Security Survey. The survey addressed such issues as the computer security technologies enterprises used, what kinds of security incidents they've suffered and what actions they've taken. Among the findings: 1) Security software and hardware failed to prevent more than 5,000 incidents among those surveyed; 2) A common point of frustration came from the nonstop barrage of viruses, Trojans, worms and spyware; 3) Use of antivirus, antispyware, firewalls and antispam software is almost universal among those who responded. But the software apparently did little to stop malicious insiders. FBI 2005 Computer Crime Survey: http://www.fbi.gov/publications/ccs2005.pdf

---

Category 31.1 *Surveys, studies, audits of security*

2006-01-16 **study classic viruses decline PandaLabs**

DHS IAIP Daily; http://www.net−security.org/press.php?id=3761 23

NUMBER OF "CLASSIC" VIRUSES DROPPED DRAMATICALLY IN 2005

According to data released by PandaLabs, less than one percent of the new threats detected in 2005 were viruses, whereas threats like Trojans and worms still had a significant presence compared to the previous year. “Viruses, described as threats that add their code to other executable files in order to carry out their malicious actions, have reached rock bottom this year,” explains Luis Corrons, director of PandaLabs. “The aim of creators of this type of threat is usually fame. However, legislation against computer crime in many countries worldwide has led to a dramatic drop in the number of new specimens of this type. Now, almost nobody runs the risk if it does not lead to financial gain.” Of the new threats detected by PandaLabs in 2005, 42 percent were Trojans, 26 percent were bots, 11 percent were backdoor Trojans, eight percent were dialers, six percent were worms and three percent were types of adware/spyware.

Category 31.1 Surveys, studies, audits of security

2006-01-19 **denial of service DoS zombie PC survey study**

DHS IAIP Daily; http://news.bbc.co.uk/1/hi/technology/4625304.stm 23

ZOMBIE PCS TARGET VULNERABLE SITES.

Recently, denial-of-service (DoS) attacks by criminals who recruit so-called zombie PCs and use their net addresses to deluge sites with data, have become increasingly more prevalent. According to security firm CipherTrust, high profile websites are ripe for this cyber-crime, largely due to the ease with which attacks can be launched. Criminals intent on bringing down sites recruit mostly Windows PCs by infecting them with viruses or worms. They then use the net addresses of these zombie PCs to deluge targeted websites with a huge amount of data, causing the servers to fall over and forcing the website offline. CipherTrust has seen an alarming rise of nearly 50 percent in the number of infected machines being recruited over the past six months. The middlemen in these attacks tend to be home users. This is largely a result of the Sober virus which hit PCs around the world at last year. It estimates that 250,000 new machines are infected every day. "China has the most zombie PCs at the moment and the U.S. is regularly number two, with Germany at number three and the UK, with just three percent of infected machines, at number 10," said David Stanley, managing director of CipherTrust.

Category 31.1 Surveys, studies, audits of security

2006-01-23 **UK banks increase online security FSA study customers concern**

EDUPAGE; http://news.bbc.co.uk/2/hi/business/4637226.stm 23

U.K. CALLS ON BANKS TO INCREASE ONLINE SECURITY

The Financial Services Authority (FSA), a financial watchdog organization in Britain, has called on the country's banks to increase online security. According to the FSA, losses to online banking fraud tripled in the first half of 2005 compared to a year earlier. A study conducted by the FSA revealed that half of online banking customers are concerned about security and that three-quarters would stop banking online if they are forced to bear the costs of fraud. The group acknowledged that part of the responsibility lies with consumers, who need to understand the risks and the steps they can take to minimize them. Banks, however, must do more to increase security and to educate users, said the FSA. Some banks are piloting projects aimed at increasing online security. Lloyds TSB issued 30,000 electronic security devices that users must have to access their accounts. The devices generate new ID codes every 30 seconds and must be used in tandem with existing security measures.

Category 31.1 Surveys, studies, audits of security

2006-01-26 **prediction BIOS rootkits insider attacks**

DHS IAIP Daily; http://www.securityfocus.com/news/11372 23

RESEARCHERS: ROOTKITS HEADED FOR BIOS.

Insider attacks and industrial espionage could become stealthier by hiding malicious code in the core system functions available in a motherboard's flash memory, researchers said on Wednesday, January 25, at the Black Hat Federal Conference. A collection of functions for power management, known as the Advanced Configuration and Power Interface (ACPI), has its own high-level interpreted language that could be used to code a rootkit and store key attack functions in the Basic Input/Output System (BIOS) in flash memory, according to John Heasman, principal security consultant for UK-based Next-Generation Security Software. The researcher tested basic features, such as elevating privileges and reading physical memory, using malicious procedures that replaced legitimate functions stored in flash memory. "Rootkits are becoming more of a threat in general -- BIOS is just the next step," Heasman said during a presentation at the conference. "While this is not a threat now, it is a warning to people to look out." The worries come as security professionals are increasingly worried about rootkits. While some attacks have attempted to affect a computer's flash memory, the ability to use the high-level programming language available for creating ACPI functions has opened up the attack to far more programmers.

Category 31.1 *Surveys, studies, audits of security*

2006-01-30 **study ID theft decrease cost increase**

EDUPAGE; http://online.wsj.com/article/SB113858617249559658.html 23

NUMBER OF ID THEFTS DROPS, COSTS RISE

According to a new report from Javelin Strategy and Research and the Better Business Bureau, the number of individuals victimized by identity theft has fallen in recent years, but the amount of money lost to such malfeasance is climbing. Researchers found that about 8.9 million people suffered identity theft last year, compared to 9.3 million the year before. In 2003, the Federal Trade Commission estimated that identity thieves successfully targeted 10.1 million individuals. Experts said the decline in the number of victims indicates heightened awareness and better tools to combat identity crimes. Even as the number of victims has dropped, the total losses to such crimes has risen from $53.2 billion in 2003 to $56.6 billion last year. "Criminals are building up more expertise," said James Van Dyke, founder and principal analyst of Javelin, "and they have to soak victims for more money."

Category 31.1 *Surveys, studies, audits of security*

2006-02-03 **report Jupiter Research ISP filters forcing spam decline**

DHS IAIP Daily; 23
http://www.techweb.com/wire/security/178601917;jsessionid=5S
PNDZX55YKH4QSNDBOCKHSCJUMEKJVN

REPORT: ISP FILTERS FORCING DECLINE IN SPAM.

ISP filters are largely responsible for a decline in e-mail spam, which is expected to continue declining through 2010, according to a report released Friday, February 3, by Jupiter Research. Jupiter said the average e-mail consumer received 3,253 spams in 2005, but that number will drop to 1,640 in 2010. The company forecasts that the volume of spam messages per consumer will decrease by 13 percent a year until 2010. "The next five years will see a more organized e-mail marketing arena," said David Schatsky, senior vice president of research, in a statement.

Category 31.1 *Surveys, studies, audits of security*

2006-02-24 **Gartner research study cell phone threats increase**

DHS IAIP Daily; 23
http://news.com.com/Is+your+cell+phone+due+for+an+antivirus+ shot/2100−
7349_3−6042745.html

SECURITY EXPERTS: THREATS TO CELL PHONES ARE LIKELY TO INCREASE.

Programs that fight viruses have become a necessary evil on Windows PCs. Now the antivirus industry is turning its attention to mobile phones -- but it's running into reluctance from cell service providers, who aren't so sure that the handset is the best place to handle security. Verizon Wireless doesn't see a need for its customers to install antivirus software on cell phones. "At this point, that is absolutely not required by individual customers," spokesperson Jeffrey Nelson said. But makers of security software are eager to get their products onto handsets, a huge potential market. About 812 million mobile terminals -- such as cell phones and smart phones -- were sold in 2005, according to market researcher Gartner. That compares with an estimated 219 million PCs in the same period. The market research firm expects annual mobile device shipments to exceed one billion units for the first time in 2008. While the number of threats to cell phones is low, security experts and analysts agree that situation is likely to change. Gartner suggests a widespread attack could surface by the end of next year.

Category 31.1 *Surveys, studies, audits of security*

2006-02-27 **RSA security conference attendees report security breaches push improvement safeguard prevent accidental data leaks**

DHS IAIP Daily; 23
http://www.computerworld.com/printthis/2004/0,4814,109007,00.html

BREACHES PUSH COMPANIES TO IMPROVE INTERNAL SAFEGUARDS; SECURITY MANAGERS SHIFT FOCUS TO PREVENTING ACCIDENTAL DATA LEAKS.

After spending years implementing controls to protect network perimeters from external threats, companies are now guarding against internal data lapses, according to attendees at RSA Conference 2006 this month. Driving the trend are concerns about accidental data leaks or thefts resulting from internal miscues, a rash of recent data breaches caused by the mishandling of information, and regulations that require companies to exercise greater control over data they handle. "Even up to last year, there was a huge focus on strengthening the perimeter to make sure the hacker from outside didn't get in," said Stuart McIrvine of IBM. "Everyone was concerned about malware penetrating the perimeter." More recently, though, "there's been a big shift in focus to what's going on inside the enterprise," McIrvine said. Gene Fredriksen of Raymond James Financial Inc. said "Traditional information security has been very good at protecting structured data." But now, he added, there's a whole class of unstructured data in spreadsheets, Web forms, and other formats.

Category 31.1 *Surveys, studies, audits of security*

2006-02-27 **Internal Revenue Service IRS computer information security needs to improve tighten TIGTA**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/38341−1.html 23

IRS NEEDS TO TIGHTEN SECURITY SETTINGS.

The IRS has not consistently maintained the security settings it established and deployed under a common operating environment (COE), resulting in a high risk of exploitation for some of its computers, according to the Treasury Department's inspector general for tax administration (TIGTA). The IRS has adopted a common operating environment for security configurations on all of its workstations. The IRS has installed the master COE image on 95 percent of its computers, TIGTA said in its report released Monday, February 27. Of 102 computers tested, only 41 percent continued to be in compliance; 59 percent were not or contained at least one high-risk vulnerability that would allow the computer to be exploited or rendered unusable. Almost one-half of the compliant computers contained at least one incorrect setting that could allow employees to circumvent security controls established by the common operating environment. Also, at the time of the audit, the COE security settings had not been installed on more than 4,700 computers. Without them, computers were missing security patches and at high risk for viruses. Report: http://www.ustreas.gov/tigta/auditreports/2006reports/200620 031fr.pdf

---

Category 31.1 *Surveys, studies, audits of security*

2006-02-28 **study virus British UK businesses biggest security problem**

DHS IAIP Daily; http://news.bbc.co.uk/2/hi/technology/4755492.stm 23

VIRUSES PLAGUE BRITISH BUSINESSES.

Computer viruses are the single biggest cause of security problems for UK businesses, a survey by the Department of Trade and Industry (DTI) shows. Almost 50 percent of the biggest security breaches in the last two years were due to malicious programs. Viruses crippled key systems such as e-mail for more than a day while companies cleaned up, and the worst outbreaks sometimes took up to 50 days to fix. The survey revealed that the number of firms affected by viruses had dropped by almost one-third since 2004. This reduced infection rate is due to the of use anti-virus software. The survey found that firms that do get caught tend to get infected far more often; some were being infected once a day. Almost 25 percent of those surveyed said they had no defenses to protect them against spyware. As a result one in seven of the most serious incidents were caused by machines infected with spyware. The DTI survey questioned more than 1,000 businesses. The full results of the survey will be released in April.

Category 31.1 *Surveys, studies, audits of security*

2006-03-01 **study report OMB IT security positive gaps closing**

DHS IAIP Daily; http://www.fcw.com/article92474−03−01−06−Web 23

OMB DELIVERS POSITIVE IT SECURITY REPORT.

The Office of Management and Budget (OMB) Wednesday, March 1, presented its report, "FY2005 Report to Congress on Implementation of the Federal Information Security Management Act of 2002," to Congress. The report showed steady progress in closing security gaps in federal agencies. It found that 85 percent of IT systems to be certified and accredited and that the quality of the certifications and accreditations at the agencies also increased. OMB's report: http://www.whitehouse.gov/omb/inforeg/reports/2005_fisma_rep ort_to_congress.pdf

---

Category 31.1 *Surveys, studies, audits of security*

2006-03-07 **study computer viruses concern UK companies infection worst security incidents**

DHS IAIP Daily; http://www.businessweekly.co.uk/news/view_article.asp?articl e_id=10229 23

COMPUTER VIRUSES A GROWING CONCERN FOR UK COMPANIES.

Infection by viruses was the biggest single cause of the worst security incidents for UK companies in the past two years, accounting for roughly half of them, a new survey shows. Two-fifths of these were described as having a serious impact on the business, according to findings from the 2006 Department of Trade and Industry's biennial Information Security Breaches Survey, conducted by a consortium led by PricewaterhouseCoopers. The research showed that virus infections were more likely to have caused service interruption than other incidents. In addition, a quarter of UK businesses are not protecting themselves against the threat caused by spyware. The full results of the ninth, biennial survey will be published at the Infosecurity Europe exhibition and conference in London, April 25-27. Survey: http://www.ukmediacentre.pwc.com/Content/Detail.asp?ReleaseI D=1817&NewsAreaID=2

Category 31.1 *Surveys, studies, audits of security*

2006-03-07 **China malware software increase Symantec report finding**

DHS IAIP Daily; 23
http://www.infoworld.com/article/06/03/07/76162_HNchinamalware_1.html

CHINA MALWARE INCREASING, SYMANTEC SAYS.

The amount of malware coming from China rose 153 percent in the last six months of 2005, Symantec reported Tuesday, March 7. The increase came in remote-controlled "bot" attacks emanating from China during the period, said Dave Cole, a director with Symantec Security Response. Rising Internet use in China, and a lack of precautions taken by new users, may be contributing to the malware jump.

Category 31.1 *Surveys, studies, audits of security*

2006-03-07 **study report cyber criminals increase attacks Symantec**

DHS IAIP Daily; http://today.reuters.com/news/articlenews.aspx?type=technolo gyNews&storyid=2006−03−07T061445Z_01_N06313562_RTRUKOC_0_US− SYMANTEC−SECURITY.xml 23

REPORT: CYBER CRIMINALS STEPPING UP TARGETED ATTACKS.

Cyber criminals are stepping up smaller, more targeted attacks as they seek to avoid detection and reap bigger profits by stealing personal and financial information, according to a report issued on Monday, March 6. Symantec Corp.'s Internet Security Threat report said during the second half of 2005, attackers continued to move away from broad attacks seeking to breach firewalls and routers and are now taking aim at the desktop and Web applications. The latest report said threats such as viruses, worms and Trojans that can unearth confidential information from a user's computer rose to 80 percent of the top 50 malicious software code threats from 74 percent in the previous six months.

Category 31.1 *Surveys, studies, audits of security*

2006-03-08 **computer security attacks rise money risk theft fraud Symantec report study**

EDUPAGE; http://news.yahoo.com/s/nf/20060308/tc_nf/41987 23

ATTACKS ON THE RISE, WITH MORE MONEY AT RISK

In a new report, computer security firm Symantec says the number of Internet attacks is rising and that the motive for such attacks is increasingly money. The report is based on data gathered from 40,000 security devices from around the world and covers Internet mischief ranging from spam and adware to network attacks and phishing scams. Although many hackers formerly plied their trade merely to demonstrate what they could do, Internet scams such as phishing are designed to put money into the hands of online thieves. Symantec noted that the tools used to launch Internet attacks are becoming very sophisticated, and the report also highlights the fact that many networks remain poorly protected despite simple means to increase security against such threats. Javier Santoyo, development manager at Symantec Security Response, said, "Just letting users know about configuration management and maybe installing heuristics-based solutions on desktops goes a long way."

Category 31.1 *Surveys, studies, audits of security*

2006-03-16 **cybercrime more costly physical crime IBM survey**

DHS IAIP Daily; 23
http://www.theregister.co.uk/2006/03/16/ibm_cybercrime_survey/

CYBERCRIME COSTS BUSINESSES MORE THAN PHYSICAL CRIME.

Cybercrime is more costly to businesses than physical crime, according to a recent IBM survey of 600 U.S. businesses. Lost revenue, wasted staff time dealing with IT security attacks and damage to customer goodwill were rated as a bigger problem than conventional crime by 57 percent of firms in the healthcare, financial, retail and manufacturing industries. Of the respondents in the U.S. finance industry, 71 percent were the most concerned about the threat of cybercrime. According to the IBM survey, 83 percent of U.S. organizations believe they have safeguarded themselves against organized cybercrime but most concentrated on upgrading virus software, improving firewall defenses and implementing patch management systems. IBM said these procedures are a necessary first step but fail to go far enough.

Category 31.1 *Surveys, studies, audits of security*

2006-03-16 **federal agencies network security no improvement D+ average grade government efforts law enforcement homeland security**

EDUPAGE; http://www.fcw.com/article92642-03-16-06-Web 23

NO IMPROVEMENT FOR FEDERAL AGENCIES IN NETWORK SECURITY

The House Government Reform Committee has once again issued a failing report card on computer security at federal agencies. Despite the fact that five federal agencies were graded A+, overall, agencies earned a D+, the same grade as last year. The grades are based on performance metrics from the Office of Management and Budget. Agencies on "the frontline in the war on terror" were uniformly terrible, according to Rep. Tom Davis (R-Va.), chairman of the committee. The Department of Homeland Security's grade stayed the same this year as last: F. Meanwhile, the grade for the Department of Defense fell from a D to an F, the State Department went from a D+ to an F, and the Department of Justice dropped from a B- to an F. Representatives from federal agencies appeared before the committee, and many of those with failing grades offered explanations about why their scores have remained low. Members of the committee were generally dismissive of the explanations, however, saying that the agencies were simply making excuses.

Category 31.1 Surveys, studies, audits of security

2006-03-17 **audit ballistic missile defense system Star Wars flaws policy awareness information warfare vulnerability risks management government audit suppression report**

RISKS; FCW http://tinyurl.com/lpp2f; http://tinyurl.com/k6n2b 24 20

GOVERNMENT REPORT ON BALLISTIC MISSILE DEFENSE SYSTEM SECURITY FLAWS

Bob Brewin reported in Federal Computer Week for March 16, 2006 that "The network that stitches together radars, missile launch sites and command control centers for the Missile Defense Agency (MDA) ground-based defense system has such serious security flaws that the agency and its contractor, Boeing, may not be able to prevent misuse of the system, according to a Defense Department Inspector General's report." The results section of the report's Executive Summary was as follows:

"Missile Defense Agency officials had not prepared a System Security Authorization Agreement for the Ground-Based Midcourse Defense Communications Network. Additionally, available security documentation did not properly reflect current operations of the network. Missile Defense Agency officials also had not fully implemented information assurance controls required to protect the integrity, availability, and confidentiality of information in the Ground-Based Midcourse Defense Communications Network. Specifically, the Missile Defense Agency program office for the Ground-Based Midcourse Defense Communications Network did not provide information assurance awareness training to prior to being granted access, conduct reviews for unauthorized access, properly implement or document user access procedures and controls, and prepare contingency and incident response plans. Further, a Plan of Action and Milestones designed to assist managers in correcting security weaknesses had not been prepared. As a result, Missile Defense Agency officials may not be able to reduce the risk and extent of harm resulting from misuse or unauthorized access to or modification of information of the Ground-Based Midcourse Defense Communications Network and ensure the continuity of the network in the event of a disruption. Additionally, the Missile Defense Agency Chief Information Officer and the Designated Approving Authority may not be able to make appropriate management-level decisions relating to the security of the Ground-Based Midcourse Defense Communications Network if required key documents are not prepared, updated, or tested."

The report was removed from the government Web site shortly after publication of the news story.

Category 31.1 Surveys, studies, audits of security

2006-03-17 **cybercrime survey IBM loss US better prepared for threat**

EDUPAGE; http://news.com.com/2100-7350_3-6050875.html 23

SURVEY HINTS AT CYBERCRIME LOSSES

A recent survey conducted by IBM of CIOs in manufacturing, financial, health-care, and retail industries shows the growing threat of cybercrime on organizational resources. Of the 600 U.S. CIOs in the survey, 57 percent said cybercrime costs their companies more than conventional crime. About 75 percent said the threat from cybercrime comes in part from within their companies. Moreover, 84 percent said hackers are increasingly part of organized crime, not simply individuals working alone. Results from international CIOs in the survey closely followed those of the U.S. companies for most measures, but they diverged on several key points. Among U.S. CIOs, 83 percent said they were prepared to face the threats of cybercriminals, compared to just 53 percent of internationals.

Category 31.1 Surveys, studies, audits of security

2006-03-23 **GAO report IRS needs strengthen information security controls**

DHS IAIP Daily; http://www.gao.gov/highlights/d06328high.pdf Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−328 23

GAO-06-328: INFORMATION SECURITY: CONTINUED PROGRESS NEEDED TO STRENGTHEN CONTROLS AT THE INTERNAL REVENUE SERVICE (REPORT).

The Internal Revenue Service (IRS) has a demanding responsibility in collecting taxes, processing tax returns, and enforcing the nation's tax laws. It relies extensively on computerized systems to support its financial and mission-related operations. Effective information security controls are essential for ensuring that information is adequately protected from inadvertent or deliberate misuse, disruption, or destruction. As part of its audit of IRS's fiscal year 2005 financial statements, the Government Accountability Office (GAO) assessed (1) the status of IRS's actions to correct or mitigate previously reported information security weaknesses at two sites and (2) whether controls over key financial and tax processing systems located at the facilities are effective in ensuring the confidentiality, integrity, and availability of financial and sensitive taxpayer data. GAO recommends that the IRS Commissioner take several actions to fully implement an information security program. In commenting on a draft of this report, IRS concurred with our recommendations.

Category 31.1 *Surveys, studies, audits of security*

2006-03-23 **privacy violations survey Bentley College Watchfire California Online Privacy Protection Act**

EDUPAGE; http://chronicle.com/daily/2006/03/2006032301t.htm 23

SURVEY SUGGESTS WIDESPREAD PRIVACY VIOLATIONS

A study conducted by Bentley College and software company Watchfire indicates that nearly three-quarters of colleges and universities in California fail to comply with a state law concerning the collection and use of personal information. The California Online Privacy Protection Act of 2003 requires organizations that collect such information online to clearly post privacy policies on their home pages and on every page from which personal information is collected. According to the study, which examined the Web sites of 236 institutions, only 28 percent had privacy policies linked from their home pages. Moreover, every one of the 236 institutional Web sites had at least one page that collects personal data without encrypting it. Mary Culnan, management professor at Bentley and author of the report, said she hopes these results serve "as a wake-up call to students, alumni, and prospective students."

Category 31.1 *Surveys, studies, audits of security*

2006-03-31 **information security report GAO Security Exchange Commission needs improvement**

DHS IAIP Daily; http://www.gao.gov/cgi−bin/getrpt?GAO−06−408 23

GAO-06-408: INFORMATION SECURITY: SECURITIES AND EXCHANGE COMMISSION NEEDS TO CONTINUE TO IMPROVE ITS PROGRAM (REPORT).

The Securities and Exchange Commission (SEC) has a demanding responsibility enforcing securities laws, regulating the securities markets, and protecting investors. In enforcing these laws, SEC issues rules and regulations to provide protection for investors and to help ensure that the securities markets are fair and honest. It relies extensively on computerized systems to support its financial and mission-related operations. Information security controls affect the integrity, confidentiality, and availability of sensitive information maintained by SEC. As part of the audit of SEC's fiscal year 2005 financial statements, the Government Accountability Office (GAO) assessed (1) the status of SEC's actions to correct or mitigate previously reported information security weaknesses and (2) the effectiveness of the commission's information system controls in protecting the confidentiality, integrity, and availability of its financial and sensitive information. GAO recommends that SEC Chairman direct the Chief Information Officer to fully implement an agency-wide information security program. In providing written comments on a draft of this report, SEC said that GAO's recommendations are appropriate and actionable, and that it is focusing on fully implementing the recommendations. Highlights: http://www.gao.gov/highlights/d06408high.pdf

---

Category 31.1 *Surveys, studies, audits of security*

2006-04-03 **US Department of Justice DoJ National Crime Victimization Survey identity theft losses estimate survey study**

EDUPAGE; http://www.pcworld.com/news/article/0,aid,125291,00.asp 23

REPORT ESTIMATES EXTENT OF IDENTITY THEFT

According to data from the National Crime Victimization Survey, which is conducted by the U.S. Department of Justice, identity theft affected an estimated 3.6 million households--with losses totaling $3.2 billion--in the first six months of 2004. The survey contacts a random sample of 42,000 households every six months and follows them for three years. The new data are from the first instance of the survey to specifically address identity theft. The most common types of theft were from unauthorized use of credit cards. Households with annual incomes of more than $75,000 and those headed by individuals between 18 and 24 years old were more likely to suffer identity theft, though the survey did not investigate the possible reasons behind these trends.

Category 31.1 *Surveys, studies, audits of security*

2006-04-03 **study paper phishing scam fraud E*Trade**

EDUPAGE; http://news.zdnet.com/2100-1009_22-6057000.html 23

PROBING WHY PHISHING REMAINS SUCCESSFUL

A new paper published by three academics tries to explain why, after all the press about phishing scams, so many computer users continue to fall for them. "Why Phishing Works," written by Rachna Dhamija of Harvard University and Marti Hearst and J. D. Tygar of the University of California at Berkeley, points out that despite a general awareness of phishing rackets, most users are unable to discern the difference between a legitimate Web site and one spoofed to look like the site of a bank or other financial institution. In one exercise, the researchers created a fake bank site that fooled 91 percent of subjects participating in the experiment. Similarly, 77 percent misidentified a legitimate E*Trade e-mail as fraudulent. Experts attribute some of the problem to ignorance and some to users' not taking simple precautions, such as looking closely at the address bar of Web pages. Bernhard Otupal, a crime intelligence officer for high-tech crime at Interpol, noted that in one recent phishing scam, a number of users went to a site pretending to be that of a prominent bank and entered personal information even though they were not even customers of that bank.

Category 31.1 *Surveys, studies, audits of security*

2006-04-04 **British Phonographic Industry BPI illegal file sharing cost estimate piracy peer-to-peer P2P copyright intellectual property rights issues**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4875142.stm 23

FILE SHARING COSTS BRITISH MUSIC INDUSTRY NEARLY $2 BILLION

The British Phonographic Industry (BPI) estimates that illegal file sharing has cost nearly $2 billion (U.S.) over the past three years, and the International Federation of the Phonographic Industry (IFPI) has filed lawsuits against another 2,000 individuals suspected of file trading in 10 countries. The targets of the new lawsuits are said to be uploaders, those who make copyrighted music available to others for download. The lawsuits are extending to countries such as Portugal, which had not previously been included in such suits. In previous lawsuits, those found guilty of infringement or who settled with the IFPI paid several thousand dollars in fines. The IFPI also pointed out that parents are responsible for the actions of their children and can be made to pay damages on their behalf. Despite the legal action against file sharers and the emergence of legal online music services, data from research firm XTN indicate that in the United Kingdom, illegal downloading has risen 3 percent since September, now representing 28 percent of all music downloads.

Category 31.1 Surveys, studies, audits of security

2006-04-05 **junk fax FCC government enforcement audit report failures problems**

http://www.gao.gov/docdblite/details.php?rptno=GAO-06-425

WEAKNESSES IN PROCEDURES AND PERFORMANCE MANAGEMENT HINDER JUNK FAX ENFORCEMENT

The Telephone Consumer Protection Act of 1991 prohibited invasive telemarketing practices, including the faxing of unsolicited advertisements, known as "junk faxes," to individual consumers and businesses. Junk faxes create costs for consumers (paper and toner) and disrupt their fax operations. The Junk Fax Prevention Act of 2005 clarified an established business relationship exemption, specified opt-out procedures for consumers, and requires the Federal Communications Commission (FCC)--the federal agency responsible for junk fax enforcement--to report annually to Congress on junk fax complaints and enforcement. The law also required GAO to report to Congress on FCC's enforcement of the junk fax laws. This report addresses (1) FCC's junk fax procedures and outcomes, (2) the strengths and weaknesses of FCC's procedures, and (3) FCC's junk fax management challenges.

FCC has procedures for receiving and acknowledging the rapidly increasing number of junk fax complaints, but the numbers of investigations and enforcement actions have generally remained the same. In 2000, FCC recorded about 2,200 junk fax complaints; in 2005, it recorded over 46,000. Using its procedures to review the complaints, FCC's Enforcement Bureau (EB) issued 261 citations (i.e., warnings) from 2000 through 2005. EB has ordered six companies to pay forfeitures for continuing to violate the junk fax rules after receiving a citation. The six forfeitures totaled over $6.9 million, none of which has been collected by the Department of Justice for various reasons. EB officials cited competing demands, resource constraints, and the rising sophistication of junk faxers in hiding their identities as hindrances to enforcement. An emphasis on customer service, an effort to document consumers' complaints, and an attempt to target enforcement resources efficiently are the strengths of FCC's procedures; however, inefficient data management, resulting in time-consuming manual data entry, data errors, and--most important--the exclusion of the majority of complaints from decisions about investigations and enforcement, are weaknesses. FCC's guidance to consumers does not provide them with all of the information they need to support FCC's enforcement efforts. FCC faces management challenges in carrying out its junk fax responsibilities. The commission has no clearly articulated long-term or annual goals for junk fax monitoring and enforcement, and it is not analyzing the junk fax data. Without analysis, FCC cannot explore the need for, or implement, changes to its rules, procedures, or consumer guidance that might help deter junk fax violations or give consumers a better understanding of the junk fax rules. Most important, without performance goals and measures and without analysis of complaint and enforcement data, it is not possible to explore the effectiveness of current enforcement measures.

Full report at < http://www.gao.gov/new.items/d06425.pdf >.

Category 31.1 Surveys, studies, audits of security

2006-04-05 **security fear preventing deployment mobile devices businesses survey study**

DHS IAIP Daily; http://www.pcworld.com/news/article/0,aid,125319,00.asp 23

SECURITY FEARS HAMPER MOBILE DEVICES.

Around 60 percent of businesses are shying away from deploying mobile devices primarily due to security concerns, according to a new survey conducted by the Economist Intelligence Unit and commissioned by security vendor Symantec. Executives at 240 organizations worldwide were interviewed. One in five organizations said they have sustained financial losses due to an attack on mobile data platforms. Businesses also said they rated threats from viruses as the same or greater on mobile devices than on a fixed network.

Category 31.1 Surveys, studies, audits of security

2006-04-05 **Microsoft warning social engineering danger software vulnerabilities threat reinforcement**

DHS IAIP Daily; http://www.informationweek.com/news/showArticle.jhtml;jsessionid=3ISV1FYRRBVOWQSNDBGCKHSCJUMEKJVN?articleID=184429007 23

MICROSOFT: SOCIAL ENGINEERING IS JUST AS DANGEROUS AS SOFTWARE VULNERABILITIES.

Attacks that rely on "social engineering" tricks to fool users into visiting malicious Websites are just as dangerous as any that exploit software vulnerabilities, Microsoft security researcher Matt Braverman, argued. According to Braverman, a program manager with Microsoft's Anti-Malware Technology Team, data from the group's February update of its Malicious Software Removal Tool discovered an unusually high number of Alcan.b worms on users' PCs. "Alcan.b does not exploit any software vulnerabilities. Instead, it spreads through popular peer-to-peer applications and its prevalence is likely due to effective social engineering...Threats like this reinforce the idea that malware that exploits user weakness can be as dangerous as those threats which exploit software vulnerabilities," claimed Braverman.

Category 31.1 *Surveys, studies, audits of security*

2006-04-05 **botnet zombie computer networks trend study smaller smarter MessageLabs**

DHS IAIP Daily; http://www.gcn.com/online/vol1_no1/40334−1.html 23

TRENDS IN BOTNETS: SMALLER, SMARTER.

Some recent statistics on e-mail traffic provide more evidence of the trend toward smarter, more targeted online attacks. Botnets -- networks of compromised computers taken over by spammers and hackers -- are getting smaller. Rather than hundreds of thousands of zombie computers spitting out unwanted e-mail and malicious code, they now consist of tens of thousands. "They stay under the radar for longer," said MessageLabs chief technology officer Mark Sunner. "The return is still equal, if not greater, because the attacks are more targeted." Sunner said he expects continued refinement in attacks to be the distinguishing trend this year for spammers, hackers and purveyors of malicious code.

Category 31.1 *Surveys, studies, audits of security*

2006-04-18 **study security flaws vulnerabilities fix slow**

DHS IAIP Daily; http://news.bbc.co.uk/2/hi/technology/4907588.stm 23

FIRMS SLOW TO FIX SECURITY FLAWS.

Hackers are getting a helping hand from firms taking too long to fix software vulnerabilities, research shows. A study carried out for security firm McAfee found that 19 percent of companies take more than a week to apply software patches to close vulnerabilities. A further 27 percent said it took two days to apply fixes for software loopholes. Across Europe, the French took the longest to apply patches. It took 27 percent of French firms a week to fix loopholes and a further 39 percent had them applied in 48 hours.

Category 31.1 *Surveys, studies, audits of security*

2006-04-23 **malicious software sneaker insidious prevalent study**

DHS IAIP Daily; 23
http://www.usatoday.com/tech/news/computersecurity/infotheft /2006−04−23−bot−herders_x.htm?POE=TECISVA

MALICIOUS-SOFTWARE SPREADERS GET SNEAKIER, MORE PREVALENT.

At the height of his powers, Jeanson James Ancheta felt unstoppable. From his home in Downey, CA, the then-19-year-old high school dropout controlled thousands of compromised PCs, or "bots," that helped him earn enough cash in 2004 and 2005. But Ancheta got caught. In the first case of its kind, he pleaded guilty in January to federal charges of hijacking hundreds of thousands of computers and selling access to others to spread spam and launch Web attacks. In separate cases, federal authorities last August also assisted in the arrest of Farid Essebar, 18, of Morocco, and last month indicted Christopher Maxwell, 19, of Vacaville, CA, on suspicion of similar activities. The arrests underscore an ominous shift in the struggle to keep the Internet secure: Cybercrime undergirded by networks of bots -- PCs infected with malicious software that allows them to be controlled by an attacker -- is soaring. Bot networks have become so ubiquitous that they've also given rise to a new breed of low-level bot masters, typified by Ancheta, Essebar and Maxwell. Tim Cranton, director of Microsoft's Internet Safety Enforcement Team, calls bot networks "the tool of choice for those intent on using the Internet to carry out crimes."

Category 31.1 *Surveys, studies, audits of security*

2006-04-24 **password overload IT security breach study UK**

DHS IAIP Daily; http://www.infoworld.com/article/reuters/2006−04−25_L2447182 0.html 23

PASSWORD OVERLOAD HITTING FIRMS' IT SECURITY: STUDY.

Security breaches from computer viruses, spyware, hacker attacks and theft of equipment are costing British business an estimated $18 billion a year, according to a survey on Tuesday, April 25. The loss is 50 percent higher than the level calculated two years ago, said the study by consultancy PricewaterhouseCoopers for the Department of Trade and Industry. One area of concern for security, the study warned, was the increasing number of user IDs and passwords employees were having to remember. Virtually every UK company uses anti-virus software, but a quarter of businesses are not protected against the newer threat of spyware. In addition, one in five corporate wireless networks is completely unprotected.

Category 31.1 Surveys, studies, audits of security

2006-04-25 **study report progress hackers Department of Trade and Industry computer attacks**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4939386.stm 23

STUDY SAYS BUSINESSES MAKING PROGRESS AGAINST HACKERS

A survey conducted by PricewaterhouseCoopers for the Department of Trade and Industry indicates that British businesses are making strides in their efforts to thwart computer attacks. Overall, the number of U.K. businesses to suffer computer incidents dropped from 74 percent in 2004 to 62 percent in 2005, according to the Information Security Breaches survey. By far the largest drop was seen in computer viruses, which fell by one-third, while other sorts of attacks and accidental data loss stayed relatively steady, said Chris Potter, who led the survey. He noted that the reduction of incidents follows an increase in security spending in the business sector, which now spends between 4 and 5 percent of technology budgets on security, compared to just 3 percent in 2004. Still, said Potter, many businesses, particularly smaller ones, continue to leave themselves vulnerable to computer attacks. In fact, the survey showed that the number of computer incidents affecting small businesses has risen by 50 percent since 2004.

Category 31.1 Surveys, studies, audits of security

2006-05-01 **SANS safe technology list Mac OS X vulnerabilities rank number one**

DHS IAIP Daily; http://www.darkreading.com/document.asp?doc_id=93759 23

SANS EXPOSES 'SAFE' TECHNOLOGIES.

For the first time, Mac OS X vulnerabilities ranked number one in the SANS Institute's quarterly Top 20 Internet Security Vulnerabilities report, which was published Monday, May 1. Experts at the SANS Institute said the vulnerabilities clarify an important point about non-Windows systems. "There's a difference between 'safer' and 'more secure,'" says Ed Skoudis, director of the SANS "Hacking Exploits" course curriculum and a senior security analyst at Intelguardians. "There are fewer users on systems like the Mac or Mozilla, which makes them less of a target for attackers, and therefore safer. But there's nothing inherent in those systems that makes them more secure." SANS Top 20 Internet Security Vulnerabilities report: http://www.sans.org/top20/2005/spring_2006_update.php

---

Category 31.1 Surveys, studies, audits of security

2006-05-02 **top ten malware threats hoaxes Sophos report April 2006 businesses**

DHS IAIP Daily; 23
http://www.sophos.com/pressoffice/news/articles/2006/05/topt enapr06.html

TOP TEN MALWARE THREATS AND HOAXES REPORTED TO SOPHOS IN APRIL 2006.

Sophos has revealed the top ten malware threats and hoaxes causing problems for businesses around the world during the month of April 2006. The report, compiled from Sophos's global network of monitoring stations, reveals that Netsky-P, which recently celebrated its second birthday, has returned to the top of the virus chart, replacing Zafi-B. However, as a proportion of all malware, e-mail viruses and worms continue to decline -- 86 percent of the threats reported to Sophos during April were Trojan horses used by hackers to download malicious code, spy on users, steal information or gain unauthorized access to computers. The top ten viruses in April 2006 were as follows: W32/Netsky-P; W32/Zafi-B; W32/Nyxem-D; W32/MyDoom-AJ; W32/Netsky-D; W32/Mytob-FO; W32/Mytob-C; W32/Mytob-Z; W32/Dolebot-A; W32/Mytob-AS.

31.2 Estimates, guesses, predictions, forecasts concerning security

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2000-02-11 **awareness post-hoc reaction stupidity foolishness blindness obtuseness industry commerce naive beginners incompetents incompetence risk assessment ignorance police LEO law enforcement evaluation software**

NewsScan, San Jose Mercury News
http://www.sjmercury.com/svtech/news/breaking/ap/docs/198908l.htm

Investigators struggling to find the people behind [the early-February] attacks on major Web sites note that, if nothing else, the assaults jarred people out of their complacency. Months ago, a Carnegie Mellon University team issued a warning about attacks like those that have occurred this week, but the public reacted with a collective yawn. Over New Year's weekend, the FBI posted free software on its site that would let PC owners detect if denial-of-service tools had been secretly placed on their machines. Few showed any interest. "This week's events did more than we have ever been able to do with white papers and posting fixes on our Web site to alert the private sector to the dangers out there," said a spokesman for the attorney general's office. The Clinton Administration this week sought $37 million to set up 10 regional computer labs and train state and local officers as computer response experts. (AP/San Jose Mercury News 10 Feb 2000)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2000-02-11 **estimates market value security industry**

NewsScan, WP http://www.washingtonpost.com/wp-dyn/business/A37615-2000Feb10.html

[The early-February] cracker attacks have served as a wake-up call to the e-marketplace, and as a boon to security software firms that represent the best line of defense against further incidents. Online ventures have spent big to gain name recognition and build their reputations for service. But if customers can't get through, or if the security of their transactions isn't protected, they will abandon ship, and quickly. Suddenly, many e-businesses are realizing that the reputations they've carefully built can be wiped out by one intruder with an attitude. Shares of security software manufacturers surged for a second day Thursday, up as much as 36% for the week. "It's definitely a reaction to the news stories on hackers," said one analyst. "E-commerce and security go hand in hand. You can't have e-commerce without security." (Washington Post 11 Feb 2000)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2000-03-14 **Internet growth**

NewsScan, Washington Post http://www.washingtonpost.com/wp-dyn/articles/A2613-2000Mar13.html

At a high-tech conference in Virginia Michael S. Dell, founder of Dell Computer, predicted that there will be 500 million Internet users by 2003 and Internet pioneer Vinton G. Cerf, now with MCI WorldCom, said that by 2006 there will be more than 900 million devices linked to the Internet, equal to the number of telephones in the world. But Dell said $370 billion will have to spent in 2003 on new Internet infrastructure because only about 5% of network servers now in place will be usable in a few years and capable of supporting faster connections demanded by Internet users. (Washington Post 14 Mar 2000)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2000-09-11 **information warfare penetration industrial espionage proprietary information intellectual property IP survey study losses estimate**

NewsScan, MSNBC http://www.msnbc.com/news/457161.asp

Teenage hackers who deface government sites or steal credit card numbers attract a lot of attention, but experts say the real problem of cybercrime is corporate-sponsored proprietary information theft committed by professionals who rarely get caught. According to the American Society for Industrial Security, Fortune 1000 companies sustained losses of more than $45 billion last year from thefts of proprietary information, and a survey by the Computer Security Institute indicates over half of 600 companies polled said they suspected their competitors were a likely source of cyberattack. "Your competitors no longer have to be across town, or even across the country; they're in other countries that have different laws and business ethics," says Richard Power, who conducts the annual CSI survey. "Culpability is much less. There is a lawless frontier in terms of theft of trade secrets." Experts agree that while juvenile hackers often leave calling cards enabling them to be traced, professional information thieves are almost impossible to catch. What's even more frustrating is that many firms never know their systems have been breached. "It's difficult for people to see the theft of information," says the owner of a security firm. "Information is the only asset that can be copied or stolen but nothing can appear to be missing. You can still have the information... but have lost the value of that information." (MSNBC 11 Sep 2000)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2000-10-04 **security software sales**

NewsScan, E-Commerce Times
http://www.ecommercetimes.com/news/articles2000/001004-1.shtml

Sales of security software are taking off, fueled by an epidemic of hacker attacks and vicious viruses, according to a study by Gartner Group's Dataquest division. Spending will soar from $2.5 billion in 1999 to more than $6.7 billion in 2004, as management software vendors, such as Computer Associates, IBM/Tivoli and Hewlett-Packard, increasingly focus on security in their core software offerings. According to the report, the top security software seller is antivirus protection, with 31% of the current market. According to the FBI, 9 out of 10 companies have reported computer security breaches — including hacking, viruses, fraud and sabotage — since March 1999. That study was based on a survey of 600 companies and government agencies. (E-Commerce Times 4 Oct 2000)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2000-10-17 **e-commerce security violations vulnerabilities exploits losses damage availability quality assurance QA frustration incompetence bad design speed response time slow**

NewsScan, E-Commerce Times
http://www.ecommercetimes.com/news/articles2000/001017-1.shtml

Technical and procedural glitches could cost e-tailers as much as $15 billion in lost sales this holiday season, warns a new report by Creative Good. "The Holiday 2000 Online Shopping Report" concludes that nearly half of all would-be online shoppers will leave Web sites without making a purchase, and without contacting customer service. "If sites can simply make the buying experience easier, they stand to gain huge increases in revenue and a larger customer base who will return to shop after the holiday season is over," says a Creative Good analyst. "The sites that cannot convert shoppers to buyers this holiday season are likely to shut down in 2001." The survey, which looked at Gap.com, LandsEnd.com, Amazon.com, Barnesandnoble.com, BestBuy.com, Buy.com, eToys and KBKids.com, found that 43% of shoppers who visit a site intending to buy abandon their efforts due to frustration. Many of them then flee to bricks-and-mortar stores. The No. 1 reason for leaving the Web, cited by 40% of shoppers who changed their minds, was a cumbersome checkout process. Additional problems included slow-loading pages and inability to find the desired merchandise. (E-Commerce Times 17 Oct 2000)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2000-10-19 **infrastructure protection law enforcement criminal hackers cybercrime attacks penetrations intrusions denial of service DoS meeting conference international Internet OECD**

NewsScan, Financial Times http://news.ft.com/news/industries/infotechnology

The head of the National Infrastructure Protection Center, part of the FBI, warned that computer break-ins like the ones that plagued Yahoo!, Amazon and eBay last spring are likely to recur. Michael Vatis told policymakers and industry leaders meeting in London to discuss strategies for fighting cybercrime that it was "probable there would be another attack at least as successful" in the coming months. "All of the efficiencies and advances in productivity that have been created by the Internet have a downside. They make businesses more vulnerable." Organization for Economic Cooperation and Development officials warned that electronic breaches in the first two quarters of 2000 have outstripped all those for 1999, and said if the trend continues, it could undermine consumer trust in e-commerce. "The outlook is not encouraging," said Risaburo Nezu, head of OECD's directorate for science, technology and industry. "The response from consumers to new Internet business models is becoming cautious." The OECD is proposing it assume a larger role in tracking security breaches worldwide. (Financial Times 19 Oct 2000)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2001-01-29 **spam junk unsolicited bulk e-mail costs fees**

NewsScan

ONLINE MARKETERS WILL SOON HAVE TO PAY TO SPAM
Online marketers soon will have to pay for the privilege of sending promotional e-mail to consumers, says Jupiter Research, which predicts that 268 billion advertising messages will be sent in 2005 -- 22 times the number sent in 2000. The trend will open up a substantial new revenue stream for portals, ISPs and Web-based e-mail services, but will raise the costs of e-mail marketing campaigns significantly. Jupiter says that sending solicitation messages to a user's "bulk" e-mail in-box likely will still be free, but that marketers will have to pay a premium for profiled delivery, based on individual usage behavior. The research firm suggests marketers should be working now to establish strategic partnerships with major e-mail service providers in the hope of securing reduced rates in the future. (NUA Internet Surveys 29 Jan 2001)
http://www.nua.ie/surveys/?f=VS&art_id=905356392&rel=true

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2001-03-27 **junk unsolicited bulk e-mail spam international cooperation**

NewsScan

EC STUDY TARGETS JUNK E-MAIL
A new report issued by the European Commission predicts that unsolicited e-mails could in the future cost about US$10 billion a year to download, and calls on governments to coordinate efforts to stem the tide. Fueling the growth in unsolicited mail will be a sharp increase in legitimate, non-spam messages sent by companies with which the recipient might already have a business relationship. According to Jupiter Media Metrix, the number of commercial e-mails received each year by the average U.S. consumer will grow from 40 in 1999 to 1,600 in 2005. Meanwhile, Forrester Research is predicting that more than 200 billion e-mail messages will be sent by marketing companies in 2004, an average of nine per household every day. And while U.S. companies rely on consumers to "opt out" of receiving unwanted mail, European authorities are moving in the opposite direction. Five countries -- Austria, Denmark, Finland, Germany and Italy -- have legislated for an "opt in" system that prohibits sending e-mail to consumers unless they've indicated they wish to receive them. Marketing experts on both sides of the Atlantic say it will be difficult to resolve the differences between the two systems, and some have urged a differentiation between straight spam, mail sent by third parties, and mail sent to a company's existing customer database. (Financial Times 27 Mar 2001)
http://news.ft.com/news/industries/internet&e-commerce

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2001-04-19 **music intellectual property copyright peer-to-peer networking violations infringement intellectual property effects results sales**

NewsScan

ONLINE MUSIC CUTS INTO MUSIC SALES IN U.S.
The U.S. record industry is blaming online music and the economic slowdown for a drop in music sales. Annual figures from the International Federation of the Phonographic Industry show sales of singles fell by 38% in the U.S., and cassettes by 46%. "The downturn in the USA brought down the overall sales figures," says a spokesman for the IFPI. "We also saw the first evidence of the impact of free online music, as well as damage done by unauthorized CD-R copying in some major markets." France, Italy and Germany also reported lower sales, which they attributed to illegal copying. Meanwhile, the bright spot was the UK, where a 6.2% increase in unit sales helped boost the European market overall. (Ananova 19 Apr 2001)
http://www.ananova.com/news/story/sm_263235.html?menu=news.technology

---

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2001-05-21 **software piracy copyright intellectual property theft losses survey study guesswork estimate**

NewsScan

37% OF PROGRAMS USED IN BUSINESS ARE PIRATED
Software piracy grew in 2000 for the first time in more than five years, according to the Business Software Alliance, which estimates that 37% of all software programs used by businesses worldwide are illegal copies. The Asia-Pacific region -- where more than half of all software in use last year was stolen -- tops the list in terms of dollars (an estimated $4 billion) lost to piracy. Meanwhile, Eastern Europe has the highest piracy rate, with 63% of its software illegally copied in 2000. In the U.S., 24% of programs are pirated copies. Although progress is being made in some regions, BSA director of enforcement Bob Kruger takes little comfort. "That's kind of like saying that I'm having fewer heart attacks than I used to. But the damage that's being caused by piracy is still devastating. It can be counted in the thousands of jobs and billions of dollars lost." (AP 21 May 2001)
http://news.excite.com/news/ap/010521/07/software-piracy

Analyses in the RISKS Forum Digest 21.44 were highly critical of the methodology of this study. Critics pointed out, among other criticisms, that many assumptions were used in projecting piracy from the numbers of computers sold versus expected numbers of software licenses sold. Contributors also noted that the BSA has a vested interest in inflating such estimates and that members of the BSA were consulted during analysis of the results before publication.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2001-05-28 **Internet vulnerabilities weakness collapse virus**

NewsScan

INTERNET "WAITING FOR ITS CHERNOBYL," SAYS SECURITY EXPERTS
Internet security experts such as Peter G. Neumann of SRI International and Bruce Schneier of Counterpane Internet Security believe that security on the Internet is very poor. Schneier characterizes the Internet as "just too complex to be secure," and Neumann predicts: "The Internet is waiting for its Chernobyl, and I don't think we will be waiting much longer; we are running too close to the edge." In the process of compiling material for a New Yorker magazine article on Internet security issues, journalist Michael Specter hung out with network "crackers" in Amsterdam and observed them take over the Los Angeles Police Department computer system, steal passwords from a university in Korea, and break into his own Web site. He also received a lesson in creating viruses and produced one that erased all the data on one of his computers. (New Yorker 28 May 2001) print only

---

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2001-08-01 **software piracy copyright infringement intellectual property survey estimates losses costs**

NewsScan

SOFTWARE BANDITS "ARE EVERYWHERE" The software industry estimates that illegal copies of software robbed it of $12 billion in revenue last year, an amount equivalent to 15% of the industry's total sales. A director of the corporate security firm Kroll Associates says: "Like drug trafficking, the counterfeit problem is so massive you don't know how to get a handle on it. The bandits are everywhere." And in recent years organized crime has taken over the software black market, according to Microsoft's head of investigations and a former FBI and Drug Enforcement Agency official. Criminal cases have confirmed involvement in the software black market by Chinese gangs, the Italian mafia, the Russian mob, the Irish Republican Army, and Middle Eastern terrorists. The Business Software Alliance, a trade association, estimates that 37% of the software sold worldwide is counterfeit. (USA Today 1 Aug 2001)
http://www.usatoday.com/life/cyber/tech/review/2001-08-01-software-piracy.ht m

---

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2001-08-30 **security measures inadequate reliability industry problems widespread academic research government regulation proposal**

NewsScan

PETER NEUMANN SAYS ORGANIZATIONS LAGGING IN SECURITY MEASURES
The well-known security expert Peter Neumann, principal scientist at SRI International's computer science laboratory, told a congressional subcommittee yesterday that corporations are not making sufficient use of security and reliability measures developed by academic research. Neumann urged the government to find ways to encourage corporations to remedy that failing. (San Jose Mercury News 30 Aug 2001)
http://www.siliconvalley.com/docs/news/svfront/secur083001.htm

---

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2001-09-18 **e-mail growth usage wireless survey prediction**

NewsScan

MASSIVE E-MAIL GROWTH PREDICTED
E-mail use is set to grow 138% over the next four years, according to researchers at IDC, who are forecasting 1.2 billion e-mail mailboxes by 2005. By that time, the number of personal e-mail messages sent in an average day will exceed 36 billion. Growth will be fueled by increased use of free Web-based services, such as Hotmail, and the proliferation of Web-enabled devices, such as cell phones and PDAs. "Wireless access through e-mail devices will offer new ways for e-mail users to remain connected longer while on the move," says IDC researcher Mark Levitt. (Ananova 18 Sep 2001)
http://www.ananova.com/news/story/sm_401552.html

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2001-10-01 **critical infrastructure protection cyberterrorism**

NewsScan

WARDING OFF CYBERTERRORIST ATTACKS
Internet experts believe that the threat of cyber-attacks are increasing, though not necessarily from Osama bin Laden's AlQaida network, which seems focused on destroying physical targets and killing civilians. Georgetown University computer science professor Dorothy Denning says, "It's my understanding that they're not teaching this in the terrorist-training camps," but rather that the danger comes from "these thousands of affiliates or sympathizers." Stephen Northutt, who runs an information warfare simulation for the SANS Institute, warns that terrorist could "potentially paralyze commerce" and might be able to "accomplish a cascading failure of the electronic grid." (San Jose Mercury News 1 Oct 2001)
http://www.siliconvalley.com/docs/news/depth/cyber100101.htm

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2001-10-30 **steganography terrorism guess estimate Web content**

NewsScan

THE DEVIL IS IN THE DETAILS (AND ON THE WEB) [6 Feb 2001]
Law enforcement officials in the U.S. and elsewhere are saying that international terrorists are increasingly used encrypted files on the Web to hide terrorist communications on sites supposedly devoted to pornography, sports, or other activities. Defense expert Ben Venzke says that encrypted terrorist information could be hidden in images that might "look no different than a photograph exchanged between two friends or family members," and notes: "There is a tendency out there to envision a stereotypical Muslim fighter standing with an AK-47 in barren Afghanistan. But Hamas, Hezbollah and bin Laden's groups have very sophisticated, well-educated people. Their technical equipment is good, and they have the bright, young minds to operate them." (USA Today 6 Feb 2001)
http://www.usatoday.com/life/cyber/tech/2001-02-05-binladen.htm

TERRORISTS MAY BE HIDING MESSAGES IN DIGITAL PHOTOS [30 Oct 2001]
Terrorists may be hiding messages in digital photos sent over the Internet, using a process called "steganography" (from the Greek for "hidden writing") to embed secret messages in graphic or audio files to make them undetectable to the unaided human eye or ear. George Mason University professor and steganography expert Neil F. Johnson says that in the past two years, the number of steganography tools available over the Internet has doubled: "It's 140 and growing." He adds, "I have no reason to think that Al Qaeda is not using steganography." French law enforcement authorities who recently apprehended a man planning to blow up the U.S. embassy in Paris learned that the terrorist group of which he is a member had been instructed by a bin Laden associate to conduct all of its communications through pictures posted on the Internet. (New York Times 30 Oct 2001)
http://partners.nytimes.com/2001/10/30/science/physical/30STEG.html

---

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2002-01-04 **criminal hacker targets home PC wireless networking firewalls antivirus education awareness vulnerability warnings predictions**

NewsScan

HOME PCs -- THE NEXT HACKER TARGET
Computer hackers are turning their sights to the humble home PC, which is now faster, more powerful and less secure than ever before. Fueling the onslaught are several factors, including the trend toward home-based DSL or cable connections that are "on" all the time, and the lackadaisical attitudes of most home PC owners who generally don't keep up to date with the latest antivirus and firewall software. In addition, many home users are naïve about the potential threat and willingly click on unsolicited e-mails that could be infected with malicious programs. "Home users have generally been the least prepared to defend against attacks," warns Carnegie Mellon's Computer Emergency Response Team Coordination Center. "In many cases, these machines are then used by intruders to launch attacks against other organizations." Antivirus firm Message Labs reported that it detected one virus per 370 e-mail messages in 2001, double the rate of the previous year. Meanwhile, Amit Yoran of computer security firm Riptech says the advent of wireless networking will increase the risk of attack significantly: "The standard itself is insecure What we're faced with is the widespread adoption [of wireless networks] throughout corporate America and throughout consumer markets and people haven't really thought through how to protect." (AP/Wall Street Journal 4 Jan 2002)
http://interactive.wsj.com/articles/SB101010408230416276O.htm (sub req'd)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2002-01-10 **copyright intellectual property music sales prediction analysis royalties fees**

NewsScan

2002: THE YEAR OF THE COPYRIGHT? "The recording industry has vowed to make 2002 the year of the copyright," says columnist Patti Waldmeir. To further that goal, record labels are experimenting with CDs that include technology that prevents them from being copied, even by owners for their own use, and several online music subscription services set to launch this year will be engineered to prevent unauthorized reproduction. If the technology is successful, it could be the year of ascendancy for copyright holders, who will find themselves wielding more power than was ever intended under U.S. copyright law or the constitution, says Stanford University law professor Lawrence Lessig. Lessig argues that by extending the term of copyrights 11 times in the last 40 years, Congress has exceeded its constitutional authority, granting copyright holders terms that extend long beyond a human lifetime. Lessig argues that these over-lengthy terms violate the constitution's command to "promote the Progress of Science and the useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries." Under today's technology, the copyright on a locked CD may expire, but the CD would remain locked. In Lessig's recent book, "The Future of Ideas: The Fate of the Commons in a Connected World," he recommends a radical revision of copyright law: copyright protection should be cut to five years, renewable 15 times. If a copyright is not renewed, the work would enter the public domain. (Financial Times 10 Jan 2002)
http://news.ft.com/news/industries/media

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2002-01-11 **copy protection music piracy countermeasures prediction public rejection resistance**

NewsScan

PHILIPS SAYS COPY-PROTECTED CDs WON'T LAST LONG
Philips Electronics, which invented the compact disc, says the controversial attempts by the recording industry to market "copy protected" CDs will fail because consumers just don't like it. As inventor of the CD standard and the industry's licensing body, Philips says it could refuse to license the new discs as genuine CDs or pursue some kind of legal action, but thinks the copy-protected CDs will disappear on their own as consumers reject them. "Any kind of legal action would take years and we don't expect these [discs] to last that long," says Gary Wirtz, general manager of the Philips Copyright Office. "At the moment we are trying to reason with people rather than sue them. [The technology is] not going to work, because any hacker can still make copies. It's only going to affect legitimate consumers and we know there have already been considerable complaints." Philips opposes the technology because it can make legitimate CDs unplayable in some older players and in-car audio systems. Critics maintain that the technique used to block copying can also impair the quality of a disc's audio content over time. (New Scientist 11 Jan 2002)
http://www.newscientist.com/news/news.jsp?id=ns99991783

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2002-02-06 **survey study statistics prediction security budgets spending industry**

NewsScan

CORPORATE SPENDING ON INFORMATION TECHNOLOGY
A Goldman Sachs survey of information technology executives at 100 large corporations suggests that tech spending will be flat in the year ahead. The only areas that would see increases are expected to be security software, data networking, database software, storage software, and disaster recovery. (Reuters/San Jose Mercury News 6 Feb 2002)
http://www.siliconvalley.com/docs/news/svfront/057894.htm

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2002-06-17 **online medicine e-commerce privacy confidentiality**

NewsScan

DOCTORS TO MAKE VIRTUAL 'HOUSE CALLS'
Medem Inc., the for-profit Internet company backed by the American Medical Association and other physician groups, is launching a new service that will enable doctors to offer online consultations to established patients for a fee. The Medem service allows patients to pay upfront with a credit card, which alleviates one of most doctors' biggest concerns -- problems with payment. However, most patients will be footing the bill for online consultations themselves -- outside of a few trial programs, e-mail consultations aren't reimbursed. Physicians interviewed suggested they'd probably charge $20 to $30 a virtual visit. (Wall Street Journal 17 Jun 2002)
http://online.wsj.com/article/0,,SB1024265768750036320.djm,00.html (sub req'd)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2002-06-19 **covert channels wireless communications tooth biological interface**

NewsScan

'TOOTH PHONE'
Engineers in the UK say they've developed a tooth implant that incorporates a tiny vibrator and a radio wave receiver, and is capable of functioning like a tooth-based cell phone. The implant does not yet have its own microchip installed, but inventors James Auger and Jimmy Loizeau say the technology has been tested, and that a fully functional phone is feasible. Sound, received as a digital radio signal, would be transferred to the inner ear by bone resonance, enabling information to be received anywhere and at any time, with no one else the wiser. The invention raises the possibility of financial traders receiving the latest stock market updates while taking in a movie, or politicians receiving a secret briefing on the issues while being quizzed by reporters. (Reuters 18 Jun 2002)
http://news.com.com/2100-1033-937253.html

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2002-06-19 **hacktivism Web vandalism penetration hacker attack information warfare**

NewsScan;
http://news.bbc.co.uk/hi/english/sci/tech/newsid_2052000/2052320.stm

PRO-ISLAMIC GROUPS ENGAGE IN 'HACKTIVISM'
UK security firm mi2g says there's mounting evidence that individual hacker groups with a pro-Islamic agenda are working together to disrupt Web sites in India, Israel and other target countries. "Political motivation is an increasingly rising factor in digital attacks," says mi2g CEO DK Matai. "The primary reason why Web attacks are increasing is political tensions between Israel and Palestine, India and Pakistan, and China and Taiwan." Israel has suffered a barrage of attacks since the beginning of the latest Palestinian uprising in September 2000, and during the recent tensions between India and Pakistan over Kashmir, several groups (including Unix Security Guards, Anti-India Crew and World Fantabulous Defacers) have carried out hundreds of attacks on Indian educational and business Web sites. Despite the increase in attacks, the total number of new viruses has actually been decreasing, says mi2g, following a peak in 1997. However, each new virus is capable of causing more trouble because of the large number of computers that are now networked together. "When one catches a cold the entire global organization catches it," says Matai. (BBC News 19 Jun 2002)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2002-06-21 **wireless Internet service in-flight**

NewsScan

IN-FLIGHT INTERNET GETS ANOTHER BOOST
Boeing's efforts to bring in-flight high-speed Internet access to airline passengers received a major boost when it announced British Airways as its second trial customer. Up until now, Lufthansa has been the only other airline signed on for Connexion's pilot project. Boeing is struggling to keep the project on track following the decision of three U.S. airlines -- American, United and Delta -- to back out of plans to take an equity stake in the venture following last September's terrorist attacks. British Air marketing director Martin George says he's confident the trial will be a success: "What our customers are saying to us is we would like the option (of broadband access) onboard. This is the future of in-flight entertainment. I would like this in the cabin of all our long-haul aircraft as soon as possible." The Connexion system eventually will supply live TV and can also be used to transmit data about the aircraft back to the ground. (Financial Times 13 Jun 2002)
http://news.ft.com/servlet/ContentServer?pagename=FT.com/StoryFT/FullStory&c=StoryFT&cid=1023858976044&p=1012571727248

MITSUBISHI, BOEING TEAM UP ON IN-FLIGHT INTERNET SERVICE
The Mitsubishi Electric Corporation will manufacture antennas for an in-flight Internet service that Boeing Aircraft will offer as "Connexion by Boeing," with tests of the service beginning in next January [2003]. Boeing's announcement was enthusiastic, with an executive proclaiming that the service is "about choice. It's about tomorrow. It's about a good partnership we're excited about. We can't imagine a better partner." (AP/San Jose Mercury-News 21 Jun 2002)
http://www.siliconvalley.com/mld/siliconvalley/3516860.htm

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2002-07-02 **click-through e-mail ads spam study survey estimate**

NewsScan

ONLINE ADS FAIL TO CLICK WITH VIEWERS
Consumers are tired of online ads, according to a recent study by eMarketer, which estimates that the average click-through rate on e-mail ads is a paltry 1.8%. That's down from 3% last year, and reflects what eMarketer senior analyst David Hallerman calls a radical shift in consumer psychology: people are so overwhelmed with the daily avalanche of e-mail advertisements, that they just aren't as curious about what they're selling as they used to be. The findings are consistent with recent estimates from DoubleClick, which pegged the average click-through rate for all online ads in June at 0.84%. During the heyday of online advertising, companies could expect a click-through rate as high as 15% for some promotions. Unfortunately, the technology's success is what's leading to its demise -- companies will blast consumers with more than 430 billion e-mail ads this year; by 2006 it's expected to rise to more than 960 billion. "The same thing happened to paper-based direct mail when it first became popular in the early 1980s," says a Forrester analyst. "By the mid-1980s, scores of companies were doing it, and everyone's mailboxes were jammed so they began standing over their trash baskets making the quick decision. Today, they are opening their e-mail boxes and often they are just hitting the delete key." (Wall Street Journal 2 Jul 2002)
http://online.wsj.com/article/0,,SB1025554487479274320.... (sub req'd)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2002-07-30 **broadband network ISP Internet service providers growth prediction**

NewsScan

BROADBAND: GROWING BUT SLOWING
The research firm In-Stat/MDR predicts is predicting that the number of broadband subscribers worldwide will increase by 50% this year, reaching about 46 million). That's quite a change from the period 1999 to 2001, when the growth rate exceeded 100% annually. The company also says that in the U.S. there were 7.12 million cable modem subscribers at the beginning of 2002, compared with 4.6 million subscribers for DSL; and it predicts that DSL will take the lead in the U.S. market by 2004. (New York Times 30 Jul 2002)
http://www.nytimes.com/pages/technology/index.html

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2002-08-07 **e-commerce online sales**

NewsScan

AUTO INDUSTRY RETHINKS ITS INVOLVEMENT WITH E-COMMERCE
Just three years ago, automakers GM, Ford, and DaimlerChrysler seemed frantic to get on the e-commerce train before it left the station. All of them committed millions of dollars to online sales efforts and created whole new divisions to support those efforts. But now it's quiet time, and automakers are resisting new online ventures until they feel completely sure that those ventures will generate profit. So the current situations is quite a contrast from the old, old e-commerce days (1999 or so). Karen Francis, Ford's former e-commerce chief, explains what it was like then: "You didn't know what you didn't know. You had to get in. You had to place a bet because the initial hype was such that this was going to provide unprecedented, fill in the blank, and no company wanted to be caught with their competitors having an unprecedented advantage." But that was then, this is now: time for taking a rest and closing the eyes. (AP/USA Today 6 Aug 2002)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2002-08-14 **Linux growth operating system prediction**

NewsScan

MCNEALY PREDICTS 30% ANNUAL GROWTH IN LINUX USERS
Addressing participants at the Linux World Conference and Expo, Sun Microsystems CEO Scott McNealy predicted Tuesday that the number of Linux users will grow by 30% a year for the next several years, and urged companies to embrace the open-source software movement. Documenting his own company's commitment, McNealy noted that Sun has at least 400 full-time employees dedicated to Linux and pledged to abide by the ethical standards of the Linux community, which is made up of thousands of grassroots enthusiasts worldwide who collaborate on software projects. "We're going to share in the lifestyle and be a capitalist," said McNealy. "We'll share our thoughts but we don't think it's broken so we're not going to try to fix it," he said, referring to fears that companies could take the open source code and factionalize it by creating competing proprietary versions. (AP 13 Aug 2002)
http://apnews.excite.com/article/20020813/D7LCONLO1.htm

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2002-08-15 **wireless telephones cellular mobile study predictions**

NewsScan

THE UNFIXED LIFE
Some stats on telephone use: the FCC says there were 122.4 million wireless subscribers nationwide at the end of 2001, and industry analyst Keith Mallinson predicts that number will grow to 200 million by 2006. That's about 70% of the total U.S. population. Mallinson also expects that the number of people who rely completely on a wireless phone will rise from the current 3% of the population to somewhere between 5% and 10% in the next five years. (San Jose Mercury News 15 Aug 2002)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2002-08-28 **online banking e-commerce study survey analysis**

NewsScan

ONLINE BANKING SLOW TO GO
A report from the Federal Reserve Bank of New York says that the acceptance of online bill-paying has been "very slow, falling far short of initial projections," because of a chicken-or-egg dilemma in which billers are reluctant to adopt electronic payment systems until they're confident they can sharply reduce their traditional paper-based systems, and customers are reluctant to put themselves in a situation in which they have to maintain both electronic and traditional methods of paying their bills. It has been estimated that the total cost of processing an individual check can range between $1 and $5, compared to less than one dollar for a fully electronic payment. (Dow Jones/AP/San Jose Mercury News 28 Aug 2002)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2002-08-29 **infowar information warfare attacks penetrations criminal hackers homeland defense infrastructure prediction survey**

NewsScan

THE CHANCES OF FUTURE CYBERATTACKS
A survey of chief security officers taken by the new CSO Magazine found that 49% of 1,009 survey respondents believe that terrorists will launch a major strike through computer networks within the next 12 months. President Bush's Critical Infrastructure Protection Center shares that concern; CIPC official Tiffany Olsen says that all citizens have to do their share: "The average American doesn't necessarily recognize that he or she has a responsibility to protect their bit of cyberspace by using anti-virus software, firewalls, etcetera." (Reuters/San Jose Mercury News 29 Aug 2002)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2002-09-17 **wireless communications phones growth market**

NewsScan

WIRELESS USE TO DOUBLE IN THE U.S. BY 2006
The number of monthly minutes of wireless use in the U.S. is expected to nearly double by 2006 from 2001 levels, according to a study by the Yankee Group. "Although only 3% of U.S. consumers use their mobiles as their only phone? 26% of mobile users' minutes are already being displaced from wireline to wireless and 45% of mobile users indicated at least some substitution," says the research firm, citing survey results. Analyst Keith Mallinson says he sees a strong demand for wireless services in the future, with the number of subscribers increasing to nearly 200 million by 2006 as 70% of Americans become mobile phone users, up from nearly 50% today. However, the industry's current stagnation could derail these predictions, Mallinson warns: "Buoyant market demand for mobile services? is in danger of being wrecked by a stalemate on the supply side. Limited scope for differentiation in the national marketplace has resulted in a price war, with too much capital and too many competitors resulting in anemic financial performance." (Reuters 16 Sep 2002)
http://makeashorterlink.com/?Z271222D1

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2002-09-27 **prognostications guesses predictions error gurus experts**

NewsScan

HITS & MISSES IN HIGH-TECH PROGNOSTICATIONS
MIT Media Lab founder Nicholas Negroponte admits that he's missed the mark a few times in his predictions about the future of the high-tech industry, but he's got plenty of company — Novell CTO Alan Nugent and Negroponte both thought people would be conversing with their computers years ago. Nugent also predicted that computers would be able to emulate human thought, but so far the only example of that ability is IBM's chess-playing computer, which still falls short of Nugent's expectations. Accenture chief scientist Glover Ferguson said his worst prediction was that the future of programming would focus on computer-aided software, and Concept Labs director Peter Cochrane said he mistakenly thought that voice-over-IP technology would be a dud. Michael Earl, dean of Oxford University's Templeton College said he greatly overestimated the ability of e-commerce to become a mainstream profit center, but that he's ready to predict that the future focus of the Internet will be much more on information than transactions. Meanwhile, Negroponte and Cochrane are betting that there will be a grassroots movement to supplant some of the services now offered by traditional telecom companies. The growth of Wi-Fi networks in the U.S. and the movement in Europe by local municipalities and universities to build and operate their own telecom networks will change the way telecom services operate forever, says Negroponte. "Telecom could invert itself and become a bottom-up phenomenon." (Wall Street Journal 27 Sep 2002)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2002-09-30 **spam e-mail volume denial of service DoS prediction content filtering overload**

NewsScan

PREDICTION: E-MAIL WILL BECOME DOUBLE-TROUBLE IN 3 YEARS
IDC, the technology research firm, is predicting that within just three years, the number of e-mail messages sent worldwide will increase from the current level of 31 billion daily to more than 60 billion daily. Most of it will be spam (unsolicited commercial messages), and if the problem of spam is not dealt with by more effective message-filtering, the usefulness of e-mail as an effective business and personal communications tool will be endangered. IDC executive Mark Levitt says, "Like water flowing out of a hose, e-mail has the potential to fill our inboxes and workdays, overwhelming our abilities to navigate through the growing currents of content." (VNUNet 30 Sep 2002)
http://www.vnunet.com/News/1135485

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2002-10-03 **robotics study predictions market growth**

NewsScan

U.N. REPORT PREDICTS BIG JUMP IN ROBOT USE
The World 2002 Robotics Report, compiled by the U.N. Economic Commission for Europe, predicts that sales of all kinds of robotic devices for domestic use, excluding toys and games, will jump from 21,500 in 2001 to more than 700,000 during the 2002-2005 period. "Prices are going to come down just as they did for personal computers. When PCs started to be used by private people, they were pretty expensive," says Jan Karlsson, a UNECE expert who worked on the report. Sales of robots for all uses fell sharply last year, primarily as a result of plummeting demand in Japan and a depressed U.S. economy. But over the long haul, sales will soar and could even help alleviate a predicted worker shortage due to aging populations. The report forecasts a 50% jump in robot use in Europe by 2005, and a 30% rise in North America over the same period. (Reuters 3 Oct 2002)
http://makeashorterlink.com/?O1A161EF1

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2002-10-08 **copyright intellectual property music software piracy Internet broadband bandwidth speed**

NewsScan

BROADBAND THREATENS ASIAN ANTIPIRACY EFFORTS
Broadband technology is undermining efforts by software and entertainment companies to combat copyright piracy in Asia, say industry executives. "As broadband becomes more accessible and home PCs become more pervasive, the Internet is evolving as a whole new canvas for piracy," says Sanjay Mirchandani, Southeast Asia president for Microsoft. According to IDC Asia Pacific, 19% of South Koreans and 11.5% of Hong Kong residents have access to broadband, and these countries are among the worst offenders, says Harry Hui, Southeast Asia president for Universal Music. "Countries with broadband see the most downloads" of music from illegal Web sites, says Hui. Compounding the problem are the burgeoning number of illegal optical-disc factories in countries such as China, Malaysia and Indonesia. According to the Business Software Alliance, 50% of all business software used in Asia is copied or counterfeit, with China, Vietnam and Indonesia some of the worst offenders. (Wall Street Journal 8 Oct 2002)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2002-10-16 **terminology data volume Greek prefixes**

NewsScan

STORAGE INDUSTRY MAXING OUT ON GREEK SUPERLATIVES
Having made short work of "mega" ("megas" is Greek for great), "giga" (giant) and "tera" (monster), the computer storage industry is scrounging around for new prefixes to describe the ever-increasing numbers of bytes it manages. In the near term, companies will be dealing with petabytes (from Greek "penta") and exabytes ("hexa"), but rapidly growing e-mail volumes and the increased value of e-mail will demand novel solutions. "We are already dealing with petabytes of data with video clips, and new services such as instant messaging will serve only to push demand further," says Veritas CTO Greg Valdez. "Companies must have a strategy for managing all of this data. If you don't have a strategy you are just going to keep adding more and more storage on the back of the e-mail servers." Valdez says future storage management software will be "smarter": "You need a smart file system to make it easier to access archives. Traditional file systems operate only at the block level and this is no longer enough. You must be able to manage it right down to the transaction level." Meanwhile, some software suppliers, like KVS, use data compression techniques to keep data volumes down. At least so far, no one's yet talking about "hepta" and "octa" bytes. (Financial Times 16 Oct 2002)
http://makeashorterlink.com/?D5DF21622

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2002-11-14 **cyberterrorism attacks exaggeration infowar information warfare homeland defense study analysis surveys**

NewsScan

CYBERTERRORISM THREAT OVERHYPED, SAYS REPORT
A new report by the British firm mi2g says despite the scare-mongering tactics of government officials warning against "cyberterrorist" attacks, actual numbers of such attacks on government networks are declining worldwide. In the U.S., reported intrusions into government networks fell from 386 in 2001 to 162 in the first 10 months of 2002. Worldwide, such attacks have declined by a third — from 2,031 last year to a projected 1,400 in 2002. The report was issued just a day after the U.S. Congress approved a $903 million bill for beefing up government computer security and the Justice Department indicted a British cracker for breaking into military and NASA computer systems. Meanwhile, the overall number of computer attacks has doubled, from 31,322 in 2001 to 64,408 this year — a trend that doesn't surprise Lawrence Walsh, editor of Information Security magazine: "Most of the attacks today are made by unsophisticated 'script kiddies' using off-the-shelf tools. What's the incentive for them to go after government systems? There are more rewards available from attacking small and medium-sized businesses — like credit card information and financial data. And these networks are typically not as well-defended." (Wired.com 14 Nov 2002)
http://www.wired.com/news/politics/0,1283,56382,00.html

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2002-11-27 **intellectual property music copyright violations theft piracy**

NewsScan

FIGHT AGAINST INTERNET FILE-SWAPPING CALLED HOPELESS
Four Microsoft researchers (speaking only for themselves) have told an ACM workshop that the attempt to stop people from using digital file-swapping services is entirely futile; they believe that the technology is moving too fast to be stopped, and explain that previous services (such as Napster) could be forced out of business only because relatively few people provided most of the material. In contrast, the newer services such as Kazaa are attracting too many contributors to keep a rein on. The researchers (Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman) argue that the only way the music and video industries can compete with Kazaa and similar services is to make music and video products much less expensive and much easier to obtain. (BBC 27 Nov 2002)
http://news.bbc.co.uk/1/hi/technology/2502399.stm

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2002-12-10 **Wi-Fi wireless ISP Internet service provider study analysis**

NewsScan

WI-FI: THE FUTURE ISN'T HERE YET
Wireless communications analyst Dylan Brooks of Jupiter Research says the industry is in "a bit of a bubble... We've had more than $2 billion in venture capital money flowing in, more than total revenues." (Sounds like the Internet of yesteryear, doesn't it.) Everyone seems to agree that Wi-Fi is the future — but the future won't be here for at least another few years. Synergy Research predicts that the industry's revenues won't top $3 billion (1% the worldwide telecom equipment market) before 2003, and WiFi has yet to crack into the corporate market — which is where the money is. Giga Information Group analyst Stan Schatt explains, "Most corporations are holding back because the suppliers cannot provide good security or tools for closely monitoring how the networks are performing." (New York Times 9 Dec 2002)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2002-12-13 **cyberterror homeland defense infowar information warfare critical infrastructure study analysis prediction**

NewsScan

IDC'S CRYSTAL BALL SEES CYBERTERROR IN THE FUTURE
Research firm IDC has released its list of prognostications for 2003, and high on its list is a prediction that a major cyberterrorism event will occur, disrupting the economy and crippling the Internet for a day or two. "The war with Iraq will galvanize hackers," says John Gantz, chief research officer for IDC. On the sunnier side, IDC forecast: a 6% rise in spending on information technology and telecommunications, a rebound in sales of midrange server computers; and a boost in Linux's market share at the expense of Unix. "We're saying that Linux will eat Unix," says Gantz. Other predictions include: a stagnant or shrinking IT services market as companies scale down project size and turn to IT outsourcing; a booming wireless LAN market, which will delay the introduction of so-called third-generation wireless communications networks; and a 27% increase in online messaging, with the total number of e-mail messages sent each day rising 30% to 40 billion a day. "There will be more spam in your life," says Gantz. (CNet News.com 12 Dec 2002)
http://news.com.com/2100-1001-977780.html

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2002-12-16 **control licensing regulators ISP Internet service providers**

NewsScan

KEEP THE INTERNET NEUTRAL, SAYS LESSIG
Stanford Law School professor Lawrence Lessig says the time is ripe for regulators to take a stand on ensuring that access to the Internet remain neutral, and preventing access providers from controlling how consumers use the network. The Internet is essentially an "end-to-end" design, comparable to the electrical grid or the highway system, says Lessig. All the innovation comes from people using, not from the network itself. "But increasingly, U.S. broadband companies are trying to ensure that they have the power to decide which applications and content can run. Under such a regime, if Microsoft wants to sell Xboxes to run on the broadband network then it will have to pay the network providers for that privilege. Or if Disney wants to stream movies on the Internet, it too will have to pay the network tax," says Lessig. And while some people may think taxing Microsoft and Disney is not such a bad thing, the precedent it sets would stymie the growth and potential for innovation on the network. "It might seem strange that this lesson in preserving the original values of the Internet should come from Microsoft and Disney — two companies that have suffered a great deal of criticism from network activists. But on this issue both deserve praise. Policymakers must see that what makes innovation possible on the Internet is the freedom to innovate without the permission of a network owner." (Financial Times 13 Dec 2002)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-01-07 **cyber terrorism threat estimate overrated national security**

NIPC/DHS

January 07, Computerworld — Think Tank says the threat of cyberterrorism is overrated.

A research paper released last month by the Center for Strategic &International Studies (CSIS), a Washington-based Think Tank, argues that computer networks and critical infrastructures are distinct entities and that the threat from cyberterrorism is far less serious than the government and the media contend. "While many computer networks remain very vulnerable to attack, few critical infrastructures are equally vulnerable," argues James A. Lewis, a CSIS analyst. "Computer network vulnerabilities are an increasingly serious business problem, but their threat to national security is overstated." However, Brenton Greene, deputy director of the National Communications System, an executive-branch agency responsible for maintaining and restoring communications during times of national crisis, said the physical and cyber aspects of critical infrastructure protection can't be separated. Major physical events will have digital ramifications and vice versa, said Greene. That's also the conclusion of the recently released annual report of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction, led by former Virginia Governor James S. Gilmore. "Cyberspace has been isolated and specialized, thus limiting its perceived relevance to day-to-day outcomes and even its relevance to what are viewed as clear and present homeland security threats," the commission stated.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-01-07 **outsourcing concern secure coding vulnerablities threat**

NIPC/DHS

January 06, New York Times — Experts see vulnerability as outsiders code software.

As American companies increasingly move their software development tasks out of their own offices to computer programming companies here and abroad, new concerns are being raised about the security risks involved. The companies providing outsourcing services say that they take all necessary precautions to limit risk. But the question of whether the booming business in exporting high-tech jobs is heightening the risk of theft, sabotage or cyberterrorism from rogue programmers has been raised in discussions at the White House, before Congress and in boardrooms. "I can't cite any examples of this happening - but what that means is we haven't found any," said James Lewis, director of the technology program at the Center for Strategic and International Studies in Washington. While operations in some countries, like the United States, Britain and India, are considered generally safe for such software outsourcing, nervousness is beginning to grow at companies and in the government about the possibility of abuse by hackers, organized crime agents and cyberterrorists in nations like Pakistan, the Philippines and Russia. It is easy to see why companies find the economics of outsourcing compelling; cost savings can be 25 to 40 percent. Forrester Research of Cambridge, Massachusetts, predicted in a recent report that the acceleration in outsourcing would result in 3.3 million American jobs' moving offshore by 2015. Forrester estimates that 70 percent of these jobs will move to India, 20 percent to the Philippines and 10 percent to China.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-01-14 **malware viruses worms instant messaging predictions**

NewsScan

BRACE FOR ONSLAUGHT OF NEW VIRUSES
Computer users will be plagued with a host of new viruses this year, particularly worms deployed into instant messaging systems, predicts a senior technology consultant with UK-based Sophos. "Virus writers are most interested in creating the next super Windows worm, spread by e-mail or instant messaging, as these mass-mailing viruses carry the greatest impact," says Graham Cluley. "We expect more executable e-mail-aware worms this year, while more viruses are written which use instant messaging services." Sophos also expects to see an increase in the number of so-called "Backdoor Trojans," which can open up holes in operating systems so that crackers can control them from a remote location. Windows users are particularly at risk, as nine out of 10 of last year's top viruses were spread via e-mail on Windows platforms, with the most prolific being the Klez worm. So far, PDAs and mobile phones have remained largely free of virus problems, says Cluley. "There is no indication yet that we will see an avalanche of new viruses affecting mobile devices — virus writers are not interested in targeting the mobile phone until it becomes more developed and has a bigger, common platform." (Reuters 14 Jan 2003)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-01-17 **music piracy sales projections prediction copyright intellectual property infringement**

NewsScan

AND THE MUSIC GOES 'ROUND AND 'ROUND — AND DOWN AND DOWN
As a result of music piracy over the Internet coupled with a general economic downturn, the music industry is reeling — global recorded music sales are set to fall this year for the fourth straight year. Media analyst Michael Nathanson says, "2003 will be the tipping point. The fundamentals continue to deteriorate and consolidation will have to happen." Industry critics say that the business of selling physical copies of music is hopelessly out-of-date in the Internet age, and music company executive are bewailing the creation of new generations of music fans who simply refuse to pay for music, when they can skirt laws to get it free on the Internet. Jay Berman, the chief executive of the trade association IFPI (International Federation of the Phonographic Industry), sees the challenge this way: "This is a time when different sectors of the music industry, for all their diverging interests, have one big common interest: namely to develop a new online music business and to fight piracy." (Reuters/USA Today 17 Jan 2003)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-02-11 **Moore's Law growth technology density cost computational power nanotechnology**

NewsScan

MORE LIFE IN MOORE'S LAW
Moore's Law, which predicts that the number of transistors on a chip will double every two years, will "slow down" a bit in the coming years, says Intel co-founder Gordon Moore, for whom the law is named. "You really get bit by the fact that the materials are made of atoms." Alternatives to conventional chipmaking techniques, such as nanotechnology, are still in development, but haven't evolved to the point that they can take on silicon, says Moore, who notes that crafting single transistors is one thing, but "housing a billion of them on a chip is another." Still, scientific ingenuity has overcome conventional thinking in the past: "I remember we didn't think we could go beyond 1 micron because of optical lithography." (CNet News.com 9 Jul 2002)
http://news.com.com/2100-1001-942671.html?tag=fd_top

MOORE'S LAW GOOD FOR ANOTHER 10 YEARS
Moore's Law — the theory espoused by Intel co-founder Gordon Moore that the number of transistors on a computer chip would double every 18 months or so — is still valid, says Moore, who sees "no apparent roadblocks" for at least another decade. "It gets complicated and expensive, but the technological solutions seem to be there? Even if we get to the point where we can't squeeze any more [transistors] in there, we'll be putting billions of transistors on a chip. It's certainly not the end of creativity in the industry." Moore predicted that growth in the semiconductor industry would equal growth in the world's gross domestic product by 2017 if the industry continues at its current pace. (AP 10 Feb 2003)
http://apnews.excite.com/article/20030211/D7P4C9S81.htm

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-02-12 **National Infrastructure Protection Center NIPC global hacking advisory**

NIPC/DHS

February 11, NIPC — Advisory 03-002: National Infrastructure Protection Center "Encourages Heightened Cyber Security as Iraq - US Tensions Increase".

The NIPC is issuing this advisory to heighten the awareness of an increase in global hacking activities as a result of the increasing tensions between the United States and Iraq. Attacks may have one of several motivations: 1) Political activism targeting Iraq or those sympathetic to Iraq by self-described "patriot" hackers; 2) Political activism or disruptive attacks targeting United States systems by those opposed to any potential conflict with Iraq; 3) Criminal activity masquerading or using the current crisis to further personal goals. Regardless of the motivation, the NIPC reiterates such activity is illegal and punishable as a felony. The U.S. Government does not condone so-called "patriotic hacking" on its behalf. Further, even patriotic hackers can be fooled into launching attacks against their own interests by exploiting malicious code that purports to attack the other side when in fact it is designed to attack the interests of the side sending it. During times of potentially increased cyber disruption, owners/operators of computers and networked systems should review their defensive postures and procedures and stress the importance of increased vigilance in system monitoring.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-02-13 **forecast prediction cyber attack terrorism Internet subvert financial network**

NIPC/DHS

February 11, Newsday — In cyber-attack, the system bends, doesn't break.

Experts met last weekend at the annual CyberCrime convention in Mashantucket, CT to model a scenario where cyber-terrorists decide to strike first in a potential cyber-war against unspecified enemies. Richard Hunter of Gartner, the research firm that proposed and conducted the high-tech war games, says the "significant" threat to the Net is not its collapse, but the possibility that terrorists could build an undetectable control network on top of it to monitor and filter Internet traffic. Then, Hunter said, the terrorists could "subvert the Internet and take it for their own purposes." At the same time he noted that diligent maintenance of computer networks in the private and public sector would prevent 90 percent of those attacks, and suggested a seat-belt law-like model could prod slackers into cleaning up their network acts. As it turns out, the greatest potential threat against the country's infrastructure is one against the nation's financial networks — an attack that requires little technical savvy, Hunter said. Terrorists with clean credentials could buy or even start a bank and get access to the financial clearing house. Done the day after Thanksgiving, the biggest shopping day of the year, and also the day when Social Security checks and half of private corporation paychecks are processed, the terrorists could then introduce a massive onslaught of fraudulent bills into the system, causing it to choke on all the unacceptable volume.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-02-24 **cyber terrorism alert United Kingdom UK**

NIPC/DHS

February 20, The Times — Firms in the United Kingdom warned of IT terrorists.

Terrorist groups may try to infiltrate the computer systems of some of Britain's biggest companies, government departments and emergency services if a war is launched against Iraq, the Home Office of the United Kingdom has cautioned. Stephen Cummings, director of the National Infrastructure Security Co-ordination Centre (NISCC), said key IT systems were under threat of cyber attack by Islamic extremists. He said: "There will be groups attacking U.S. Government and defense websites and similar groups carrying out activity against the websites of any country involved in military action." Cummings urged businesses to step up security ahead of a possible war in the Gulf. He gave warning that terrorist groups might try to infiltrate activists into the IT departments of leading firms. "My view is that terrorist groups have identified the potential value in having people inside organizations rather than just responding passively as they have done in the past. There are already non-cyber examples of this," he said. Since NISCC was set up three years ago to monitor the threat of electronic attack against the UK, the number of digital attacks on "critical" organizations has soared. Cummings said that "there have been companies perceived to be in line with U.S. support for Israel in the past which have been attacked by pro-Palestinian groups. We could expect to see the same thing again from different sources."

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-02-28 **mobile phone handheld device hacking spread**

NIPC/DHS

February 26, ZDNet (Australia) — Experts say mobile phone hacking may spread.

United States-based security company @stake has released a security advisory detailing a Denial of Service (DoS) vulnerability in the Nokia 6210 GSM mobile phone. "This is a good example of why all newly introduced product functionality should be reviewed to ensure that no new security vulnerabilities will also be introduced. A cursory source code audit would find an error of this type," the advisory said. The vulnerability is not serious — affected users can simply "reboot" their phones — but it could be a sign of worse things to come. John Papandriopoulos, a wireless communications researcher based in Melbourne, Australia, says that current generation handsets are not necessarily a popular target because there's little that can be done even if an attacker is able to compromise them. "I think it's more likely that the motivation would be to inconvenience people," he said. As for a mobile phone worm, spreading by sending itself to phonebook entries, John says this isn't likely to happen for some time. However, as standardized client software becomes a standard feature on mobile handsets it's only a matter of time before malicious hackers start paying more attention to wireless worms, according to security consultant Daniel Lewkovitz of Sydney, Australia.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-03-17 **cyber crime India infrastructure threat Central Bureau of Investigation CBI FBI**

NIPC/DHS

March 14, SiliconIndia.com — Cyber crime a threat to Indian infrastructure.

The director of the Central Bureau of Investigation (CBI) in India said that cyber crime and organized corruption have assumed serious proportions. "Cyber crimes like hacking, e-mail fraud and other information security breaches linked to computers are turning out to be very serious problems," P.C. Sharma told journalists during a visit to Assam, India. Fears have been expressed that a new breed of criminals could damage telecommunications or rail links, disrupt power supplies and harm other important parts of India's infrastructure using cyber tools. The CBI has launched a massive drive to tackle the threat, honing the skills of its elite officers and modernizing the agency's computer network. Experts from the U.S. Federal Bureau of Investigation (FBI) visited India last year and trained policemen in dealing with cyber offences.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-03-19 **Department Homeland Security DHS system threat attack forecast warning Iraq war**

NIPC/DHS

March 18, Government Computer News — DHS warns about systems threats as war looms.

The Department of Homeland Security (DHS) on Tuesday reminded Internet users to be vigilant for cyberattacks in light of the ultimatum President Bush issued Monday that Iraqi President Saddam Hussein leave his country or face military invasion. The department and other federal agencies are monitoring "the Internet for signs of a potential terrorist attack, cyberterrorism, hacking and state-sponsored information warfare," a Homeland Security statement said. "Industry and public Internet users are reminded of the importance of employing sound security practices and reporting unusual activity or intrusion attempts to DHS or local law enforcement."

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-03-19 **CERT CC Internet net attack forecast warning**

NIPC/DHS

March 17, eWEEK — More net attacks loom, CERT says.

The recent rash of Internet worms has produced an army of hundreds of thousands of compromised machines that could ultimately be used to launch a massive distributed-denial-of-service attack at any time, according to security officials. Officials at the CERT Coordination Center said the organization is monitoring at least five large networks of compromised machines installed with so-called bots. The bots connect compromised PCs or servers to Internet Relay Chat servers, which attackers commonly use to execute commands on the remote systems. At least one of these networks has more than 140,000 machines, officials said. CERT's dire warning is underscored by last week's emergence of the Deloder and Code Red.F worms. While neither worm does any immediate damage to infected machines, both install back doors that enable attackers to use compromised machines for future, much more damaging operations, such as DDoS attacks. At the heart of this new trend, according to security experts, are poor security practices. But more important is the mistaken belief by corporate IT that once crises such as those caused by Code Red or SQL Slammer die down, the trouble's over. In fact, after an initial flurry of advisories, warnings and patches, there are often months or years of sustained infections and residual DDoS attacks, Marty Lindner of CERT said. Also problematic are the many affected machines belonging to home users, few of whom do any logging of the activity on their PCs. As a result, attackers can easily hide their tracks by using these anonymous computers, according to the experts.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-03-20 **virus worm malware cost business survey study estimates**

NewsScan

THE COST OF VIRUSES
Based on an analysis of 306 U.S. companies, computer-security company ICSA Labs says that disaster-causing viruses in 2002 cost an average of $81,000 each, compared to $69,000 in 2001. A "disaster" is defined in the company's report as having affected at least 25 machines and causing significant financial loss or damage to data. ICSA Labs says a stronger breed of viruses has increased a victimized company's recovery costs. (Dow Jones/AP/San Jose Mercury News

---

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-03-28 **music piracy downloading file-sharing recording industry**

NewsScan

INTERNET VS. RECORDING INDUSTRY
Media analyst Eric Garland of Big Champagne has told California lawmakers that the growth of music file-sharing on the Internet is "fundamentally unstoppable," because 61 million Americans and millions more worldwide are already downloading music and only 9% of them think they're doing something wrong. "We see only one trend. More people are downloading more copyrighted material." Garland's advice for the recording industry is to embrace digital distribution rather than institute lawsuits or education campaigns, but such advice is not well-received by industry executives, who are routinely urged by Internet enthusiasts to accommodate to technological realities. Phil Corwin, a lobbyist for Internet music service Kazaa, told the same group of state legislators: "The record business, in the digital revolution, has been a day late and a dollar short." [A dollar may not be the final figure.] The fight goes on. (AP/San Jose Mercury News 28 Mar 2003)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-04-02 **Chinese criminal hacker attack hacking US UK Websites vandalism defacement Iraq war prediction warning forecast**

NIPC/DHS

March 31, Washington Post — DHS: Chinese hack attacks likely.

Chinese hacker groups are planning attacks on U.S.- and U.K.-based Web sites to protest the war in Iraq, the Department of Homeland Security (DHS) warned in an alert Monday. The hackers are planning "distributed denial-of-service" attacks, which render Web sites and networks unusable by flooding them with massive amounts of traffic. They also are planning to deface selected Web sites, according to the alert, though the government said it did not know when the attacks would occur. The DHS said it got the information by monitoring an online meeting that the hackers held last weekend to coordinate the attacks.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-04-15 **cyber attacks physical damage repercussion virtual network bank account idea**

NIPC/DHS

April 14, New York Times — Cyberattacks with offline damage.

Most experts think of cyberattack as something that will happen in the virtual world, with effects on computer networks or access to bank accounts. But in a new paper, Aviel D. Rubin of the Information Security Institute at Johns Hopkins University, describes cyberattacks involving the use of online tools against the offline world. Using tools that have been published by search engines like Google that allow programmers to automate searches on a large scale, the paper describes a relatively simple program that could set the victim up to receive catalogs from hundreds of thousands of Web sites that have sign-up forms. Rubin's attack could be enormously disruptive to the target, and could paralyze the local post office that has to deal with the onslaught. As the report notes, the exploit could be used as a diversion to accompany a deadly terrorist act, like mailing an envelope containing anthrax spores. The paper can be found at www.avirubin.com/scripted.attacks.pdf

---

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-04-16 **cyber terrorism chances increase CERT incidents**

NewsScan

CYBERATTACK STATISTICS: UP, UP AND AWAY
Although computers have up to this point been spared a major cyberattack from terrorists or rogue nations, there have been plenty of smaller acts of vandalism by individual troublemakers. The Computer Emergency Response Team (CERT) tracked 52,658 online security incidents in 2001, more than double the number reported in the previous year, and more than four times the number reported the year before that. Figures for 2002 are not yet available. (Reuters/USA Today 16 Apr 2003)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-04-21 **warning threat security RSA conference**

NIPC/DHS

April 18, CNET News.com — New attack may draw government intervention.

Security experts warned Thursday that business executives need to take network protection more seriously before a major cyberattack results in government intervention. Although the Bush administration has indicated it doesn't intend to dictate how companies should handle security, another Code Red or Nimda incident could change that stance, Roger Cressey, president of Good Harbor Consulting, said during a panel discussion this week at the RSA Conference in San Francisco. "If we do have a major cyberincident, there will be a critical mass of pressure for regulation, and (Congress) will take out a sledgehammer when a scalpel is needed," Cressey said. Two months ago, the Bush administration released the National Strategy to Secure Cyberspace, a document that mainly suggested solutions for protecting the Internet and critical infrastructure. The only mandates in the document were directed at government agencies. That's the correct approach, Lawrence Dietz of Symantec said at the panel. Instead, Dietz said, the government should wield its wallet and put restrictions on companies that want to do business with federal agencies.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-04-29 **security terrorism uncertainty Department Homeland Security DHS cost-benefit analysis**

NIPC/DHS

April 25, Computerworld — Lack of terrorist activity leads to complacency.

The changing of the cybersecurity guard at the Department of Homeland Security (DHS), coupled with complacency on the part of some corporate executives, has put a higher premium on information-sharing and cooperation between the private sector and the government. Michael Hershman of Virginia-based security consulting firm Decision Strategies LLC says companies have started to slow their efforts to boost security because there has been no terrorist activity recently. "I'm afraid that they may be drawing back into complacency," he said last week at a U.S. Chamber of Commerce conference in Washington that addressed the roles and responsibilities of the government and private sector in homeland security efforts. "Corporations in America have spent billions of dollars for security, with very little cost-benefit analysis," said Hershman.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-04-30 **cyber-crime warning National High Tech Crime Unit NHTCU Great Britain InfoSecurity Europe**

NIPC/DHS

April 30, vnunet — British law enforcement issues stark cyber-crime warning.

The head of the National High Tech Crime Unit (NHTCU) of the Great Britain has called on businesses to take cyber-crime more seriously. Detective superintendent Len Hynds told delegates attending the Infosecurity Europe 2003 show that cyber-crime is no different from any other criminal activity and needs to be treated as such. Hynds's remarks came as the NHTCU released the results of a survey on UK cyber-crime. Three quarters of the 150 UK businesses surveyed had suffered some form of high-tech crime. More than one in five companies didn't even conduct regular security audits.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-05-05 **DHS CIO Pearl Harbor digitally Steven Cooper government IT safeguard risk chat online**

NIPC/DHS

May 05, InformationWeek — DHS CIO: no 'digital Pearl Harbor' likely.

"It's highly unlikely that the United States will experience a crippling "digital Pearl Harbor," the CIO of the Department of Homeland Security (DHS) says. "While this is a possibility, the probability is relatively low," Steven Cooper said in an online chat sponsored by The Washington Post. "We have done a lot in the federal arena to provide multilayered security for our digital environments and continually 'red team' our networks and applications to find vulnerabilities." The government spends millions of dollars on technology to safeguard IT, and Cooper said he isn't overly concerned about individuals who might compromise the government's IT infrastructure. "I would agree that it is always a risk," Cooper said. "However, all personnel working in the department, including contractors, must pass a security clearance and additional reviews and background checks, depending on level of clearance."

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-05-05 **security offshore coding U.S. software companies economy rish India Pakistan Russia China Techo-Security Conference**

NIPC/DHS

May 05, Computerworld — Offshore coding work raises security concerns.

IT professionals are raising questions about the U.S. software industry's reliance on overseas software developers, arguing that the practice puts companies and the U.S. economy at risk. A recent study by Gartner Inc. predicts that by 2004, more than 80% of U.S. companies will consider outsourcing critical IT services, including software development, to countries such as India, Pakistan, Russia and China. But some users at last week's Techno-Security Conference in Myrtle Beach, S.C., said the trend needs to be reconsidered in light of recent changes in the global security environment. Of particular concern is the work that is being sent to China. While not yet a major provider of outsourcing services, China has a significant economic espionage program that targets U.S. technology, the users noted. Also of concern are countries in Southeast Asia, particularly Malaysia and Indonesia, where terrorist networks are known to exist.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-05-05 **Nemertes Research IT security government regulations companies corporate real-world requirements**

NIPC/DHS

May 05, Network World — Corporate security spending not in line with real-world requirements.

Technology research firm Nemertes Research last week released its "Effective Security Solutions" report, which says the average 2% to 3% of the overall IT budget that companies allocate for security will not adequately prepare most of them for government regulations, new applications and/or Web services architectures. Johna Till Johnson of Nemertes Research says companies must spend at least 5% of their overall IT budgets on security to comply with government regulations passed in the past eight years or so. The security requirements in legislation such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Gramm-Leach-Bliley Financial Modernization Act of 1999, the Sarbanes-Oxley Act of 2002 and ongoing Department of Homeland Security initiatives, represent a significant concern for companies currently underspending, says Johnson. "The fine print in these pieces of legislation has the CEO or the security officer potentially going to jail if found in violation of these acts," she says.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-05-07 **emergency backup systems information data FEMA Federal Management Agency WTC World Trade Center Pentagon attacks**

NIPC/DHS

May 07, National Journal — IT officials emphasize need for emergency backup systems.

Many government offices must do better at backing up their information systems to preserve important data and ensure "continuity of operations" in the event of a terrorist attack, several federal technology officials said on Tuesday at a homeland security conference sponsored by the Armed Forces Communications and Electronics Association. FEMA's continuity-of-operations plan for many other systems typically amounts to "a pile of tapes" containing archived data, said Robert Coxe, deputy CIO of the Federal Emergency Management Agency (FEMA). Redundant communications and information systems proved invaluable after the attacks on the World Trade Center and the Pentagon, according to Lt. General Harry Raduege of the Defense Information Systems Agency. He recalled that one military agency avoided major data losses during the Pentagon attack because its computer systems had "double backup" capabilities. But he said officials in another Pentagon organization had stored "everything they had" on only one system that was destroyed in the attack. "They lost every bit of that data," he said.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-05-15 **e-mail instant message GoToMyPC.com impression management idle bankruptcy**

NewsScan

THE NEW WHITE-COLLAR CRIME: TECHNO-SLACKING
It's getting easier than ever to convince your customers, supervisors and employees that you're hard at work — firing off e-mail messages and opening files on your office PC while you're really attending your kids' soccer game or sleeping in. Services like GoToMyPC.com enable users to manipulate their office computers by remote control — even going so far as to move the cursor on the screen, open documents and print them on the networked office printer. E-mail timers allow workers to compose messages during the day and then queue them to be sent hours after they've gone to bed, giving the impression that they're up burning the midnight oil. Instant Message software can be reconfigured so that the "idle" message that pops up signaling inactivity is disabled, making users look perpetually available. And BlackBerry aficionados can change their settings to make on-the-road e-mail look like it came straight from the office PC. Psychologists call these activities "impression management," but other see signs of a disturbing trend: "If you're out playing golf, and you look like you've spent four hours in the office… If everybody does that, the company goes bankrupt," says Stuart Gilman, director of the Ethics Resource Center in Washington. A recent survey conducted by the Society for Human Resource Management found that 59% of HR professionals had personally observed employees lying about the number of hours they'd worked, and 53% said they'd seen employees lying to a supervisor, a jump of eight percentage points in six years. (Wall Street Journal 15 May 2003)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-06-03 **digital pearl harbor Carnegie Mellon SEI software engineering institute disgruntled insiders foreign terrorsits greatest cuyber security threat terrorism Al-Qaeda steganography**

NIPC/DHS

June 03, National Journal — Computer security officials discount chances of 'digital Pearl Harbor'.

The notion that the cyberterrorism against the United States could create a "digital Pearl Harbor" is fading three computer-security experts said Tuesday. Casey Dunlevy of Carnegie Mellon's Software Engineering Institute (SEI), and Richard Hunter of Gartner Group, said disgruntled insiders, not foreign terrorists, pose the greatest cybersecurity threat to companies. "But could [cyber terrorism] be a force multiplier in terrorist attacks" by, for example, disabling all traffic lights after a bombing? "I think we have to consider that," said Dunlevy. He said computers recovered from Afghanistan demonstrated al Qaeda's use of steganography, a technique for embedding secret data within pictures or text. "We will eventually see a cyber element to terrorist activity," Dunlevy said. But both he and Hunter said terrorist groups also are likely to continue to engage in money laundering and cybercrime as a means of purloining resources.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-06-04 **PKI Public Key Infrastructure Tim Polk NIST businesses IT security momentum encryption**

NIPC/DHS

June 04, Post Newsweek Tech Media — PKI momentum builds, program manager says.

A dozen years after the start of the federal push for a public-key infrastructure, the technology is gaining momentum, and more agencies will be using PKI in a matter of months, a federal program manager predicts. By year's end, Tim Polk, the PKI program manager at the National Institute of Standards and Technology, estimated, eight to 10 agencies will be heavily engaged in PKI, nearly twice the number involved today. Polk spoke today at a conference on IT security in Washington sponsored by the research and advisory firm Gartner Inc. As governments and businesses move from paper to electronic documents, PKI holds promise as an effective way to protect and validate those documents and verify identities. PKI also is being used with employee identification smart cards.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-06-12 **security software viruses Trend Micro**

NewsScan

SECURITY SOFTWARE BUSINESS DUE FOR A SHAKE-UP
As the nature of computer viruses changes, the business of selling security software is changing, too, says Steve Chang, head of antivirus software firm Trend Micro. With viruses morphing into ever-more-complex forms, antivirus firms will need to shift from selling software to selling security services aimed at minimizing customers' downtime. Chang says the security software industry used to compare itself to the pharmaceutical business, developing new antidotes for each virus that cropped up. But the ubiquity of the Internet and the advent of such virulent viruses as Nimda, Slammer and Bugbear have changed all that. Now, the ability of a company to avoid infection depends as much on the security measures taken by other companies it does business with and employees working in their home environments as on its own vigilance. That means companies increasingly are seeking an ongoing service which, in addition to protecting them from malicious attacks, speeds up the recovery time following a security breach so that everyone can get back to work. "You buy a drill because you want a hole," says Chang, "not because you want a drill. Customers do not want a security product. They just want to improve their productivity without downtime." (BBC News 12 Jun 2003)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-07-11 **surveys estimates data disaster disconnect IT vulnerable**

NewsScan

BUSINESS/TECHNOLOGY DISCONNECT ON DATA DISASTER
U.S. business executives may be a bit overly optimistic in their estimates of the impact a major data disaster would have on their operations. A survey sponsored by data storage firm EMC indicates that only 14% of senior business executives regard their company's data as very vulnerable, compared to 52% of senior IT executives. And only 9% of business execs said it would take three days or more to get back to normal following a data disaster, compared with 23% of tech executives. "Our customers tell us that their greatest challenge isn't backing up their information — it's recovering and resuming operations in a timely manner. We don't believe U.S. business leaders are being misled by their IT teams. Instead, it is likely a misperception that, if the data is backed up, there is no issue," says an executive VP for EMC. Meanwhile, European executives were more in synch with their IT counterparts regarding the likely vulnerability of their data — 40% of business executives and 44% of technology executives regarded their data as very vulnerable. (CNet News.com 11 Jul 2003)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-07-28 **e-mail essential downtime traumatic IT lose jobs**

NewsScan

E-MAIL DOWNTIME MORE STRESSFUL THAN DIVORCE?

A study sponsored by data-storage firm Veritas Software found that for 34% of chief information officers and IT managers, a weeklong failure of the corporate e-mail system would be more traumatic than a minor car accident, moving to a new home, or getting married or divorced. Smooth-running e-mail systems are essential to the enterprise, and 68% of the companies polled reported workers becoming irate within as little as 30 minutes after an e-mail system goes down. In the case of a failure lasting as long as 24 hours, one fifth of IT managers said their jobs would be on the line at that point. "E-mail has become far more than a communication tool, placing a huge responsibility on organizations to ensure that e-mail is always available," says Mark Bregman, Veritas' executive VP for product operations. "When IT managers fail to keep the systems running, they inhibit the ability of the entire organization to conduct business." (CNet News.com 28 Jul 2003)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-07-30 **outsourcing litigation bill**

NewsScan

TECH EXODUS: 500,000 JOBS MOVING OVERSEAS
One out of 10 jobs in the U.S. computer services and software sector could move overseas by the end of next year, according to a new report from Gartner Inc. And while professionals in the computer industry will be especially hard-hit, IT jobs in other sectors such as banking, health-care and insurance will feel the impact also, with one in 20 being exported to emerging markets such as Russia, India or other countries in Southeast Asia. "Suddenly we have a profession — computer programming — that has to wake up and consider what value it really has to offer," says Gartner VP and research director Diane Morello. Morello estimates that based on her preliminary calculations, at least 500,000 jobs will be lost to offshore outsourcing by then end of 2004. The trend toward "offshore outsourcing" is heating up as a political issue, with legislators in five states proposing bills that would require workers hired under state contracts be American citizens or fill a special niche that citizens cannot. (Reuters/CNN.com 30 Jul 2003)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-08-04 **country coded computer worms Jonath Wignall information warfare internet protocol**

NIPC/DHS

August 04, New Scientist — Country-coded computer worms may be ahead.

Jonathan Wignall of the UK's Data and Network Security Research Council highlighted techniques that worm creators might use to make their code spread more effectively during a presentation at the security conference Defcon 11 in Las Vegas, NV, on Sunday, August 3. One of these techniques could also limit a worm's geographic range, which would turn a computer worm into an effective weapon for information warfare, he said. Instead of attacking internet-connected computers at random it could be used to attack a specific country. After infecting a host computer, a worm normally scans randomly for further machines that could be infected. But Wignall says a worm could download a prepared list of internet protocol (IP) addresses to attack from a single server or a group of machines. This would prevent duplicate requests being sent to each machine, a common cause of bottlenecking with existing worm design. Nicholas Weaver, a computer scientist at the University of California in Berkeley says this is just one way that a worm could, in theory, be used to target a specific country. Another way is to avoid computers running a particular language, he says.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-08-28 **computer viruses anti-virus worms predictions propagate Sobig.F Microsoft Windows operating systems target fight**

NIPC/DHS

August 28, Washington Post — Fight against viruses may move to servers.

Computer viruses are becoming so aggressive and sophisticated that they may soon be able to elude anti-virus programs installed on individual computers, according to many in the security industry. Analysts say the speed with which viruses and worms now propagate require technologies that predict outbreaks before they happen. Such predictive systems require intensive computing power beyond the capacity of desktop machines. Computer worms and viruses are getting more sophisticated, are spreading faster and are capable of doing more damage than those of the past. Viruses such as Sobig.F can change during their attacks by receiving updates and new instructions from other computers. Some analysts point out that while no software or hardware is perfect, it's much easier to spread viruses when so much of the computing world depends on the Microsoft Windows operating system. Advocates of the Unix, Linux, Macintosh and other operating systems argue that they are more secure than Windows, but others note that those systems simply have not been targeted as much.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-09-01 **Digital vandalism internet government computer virus attachs security experts breaches terrorist damaging**

NIPC/DHS

September 01, New York Times — Digital vandalism spurs a call for oversight.

The Internet is not subject to government oversight, and many see the Internet's openness as crucial to its success as a platform for innovation. But the increasing severity of computer virus attacks may have muted the antiregulatory reflex. Some security experts now advocate direct regulation, in the form of legislation that makes software companies liable for damage caused by security flaws in their products. Advocates of increased regulation say a California law that requires companies conducting business in the state to disclose computer security breaches if they result in unauthorized access to residents' personal information could serve as a model. A survey released Sunday, August 31, by the Pew Internet and American Life Project said that nearly 60 percent of Internet users say they favor the government's requiring American corporations to disclose more information about their vulnerabilities. Half of those surveyed said they worried about terrorists damaging the Internet.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-09-02 **attack anti-virus software market growth**

NewsScan

SOFTWARE MAKERS FIND SILVER LINING TO NET VANDALISM
Business analysts expect to see continued growth in the anti-virus market, and Sarah Friar of Goldman Sachs predicts the market will climb 18% to $2.6 billion this year and improve to $2.8 billion in 2004: "This last wave of viruses perked people up to say, 'My God, I need to protect my computer.'" Nitsan Hargil of investment bank Friedman Billings Ramsey adds: "Fear sells, especially among consumers, who aren't as well-protected as corporations." Since August 11th, Symantec shares are up 22%, Network Associates shares up 30%, and Trend Micro shares up 33%. (USA Today 2 Sep 2003)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-09-11 **unpatched holes Internet Explorer Microsoft new vulnerabilities Thor Larholm former black hat heighten security**

NIPC/DHS

September 11, Sydney Morning Herald (Australia) — Thirty unpatched holes in IE, says security researcher.

As Microsoft releases details of new vulnerabilities, it is yet to tackle the 30 unpatched holes in Internet Explorer which have been documented by well-known security researcher Thor Larholm. Larholm, a former black hat and now a senior security researcher with a private company, said on Friday, September 12, that seven more vulnerabilities had been added to the list he maintains, all of them having been discovered by Chinese researcher Liu Die Yu. "One of these new vulnerabilities exploits a new attack vector that has surfaced in IE lately, namely misdirecting user input," Larholm said. According to Larholm, "This allows you to redirect a user's mouseclick to (for example) the OK button on a dialog asking for security confirmation by moving the browser window prior to the mouse being released. This resurrects the debate on whether to disable some core functionality to heighten security. Similarly, several of the vulnerabilities that remain unpatched are known to be under active investigation by the Microsoft Security Response Center, and I am confident that a secure patch is being prepared for prompt release."

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-09-29 **spam estimates marketing filtering masking blocking**

TechWeb http://www.techweb.com/wire/story/TWB20030929S0020

Gartner Group estimated that spam would be 50% of all e-mail on the 'Net by the end of 2003 and 60% by mid-2004. They also found that permission-based, well-designed, targeted e-mail could produce as much as a 15% response rate — much higher than the 1% for banner ads and the fraction of a percent for broadcast print mail advertisements.

David Legard, writing in Network World, summarized the Gartner findings as follows (quoting):

* E-mail marketers no longer have to comply with 36 state laws and, although the bill requires a valid opt-out mechanism, it does not make clear who should be responsible for implementing the unsubscribe or do-not-contact request.

* Businesses, ISPs and vendors filtering inbound e-mail will have to develop increasingly sophisticated technology and practices to decide between legitimate advertising material and spam, both of which will have to carry the 'ADV' tag in the subject line

* Disreputable spammers will ignore the legislation and if they feel under threat, will use offshore ISPs beyond the reach of U.S. jurisdiction to send material.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-10-01 **virus threat damage Microsoft software Symantec report**

NewsScan

NEW VIRUSES USE 'BLENDED THREATS' TO WREAK DAMAGE
Computer viruses are increasing in frequency, speed and sophistication, according to the latest Internet Security Threat Report from Symantec, adding that hackers are using "blended threats" that combine various types of viruses to carry out their attacks. Not surprisingly, the target of most of these attacks is Microsoft software, says Tony Vincent, Symantec's lead global security architect. "There's a continued focus by the bad guys on vulnerabilities based on Microsoft's Web server product and Internet Explorer." The report also cites a narrowing gap between the discovery of a potential vulnerability and the launch of a virus designed to exploit it. "The speed of propagation of blended threats is also increasing. Symantec expects to see greater worm propagation resulting in overloads to network hardware, crippling network traffic, and seriously preventing both individuals and businesses from using the Internet." (Reuters 1 Oct 2003)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-10-19 **cyber crime Bucharest Romania litigation defraud US**

NewsScan

CYBERCRIME HOTSPOT: BUCHAREST
There now exists a loosely organized network of young Romanians conspiring with other accomplices in Europe and the U.S. to defraud consumers through bogus Internet purchases, extort cash from companies after hacking into their systems, and release worms and viruses. Romanian lawmaker and former programmer Varujan Pambuccian says: "We want a good name for our country. I'm very angry that Romania is so well-known for ugly things — for street dogs, street children and hackers." Mihai Radu, a computer security expert in Bucharest, believes that Romania's law enforcement officials are not up to the job of defeating the vandals: "The Romanian police aren't qualified. They don't have the tools, the skills, the software." (AP/San Jose Mercury News 19 Oct 2003)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-12-02 **worm network cell phone handset vulnerability Internet enabled**

NIPC/DHS

November 28, New York Times — Beware the worm in your handset.

As more consumers begin surfing the Web and sending e-mail messages on cellphone and hand-held devices, along comes a new worry: worms and viruses spread via Internet-enabled handsets. The problem is still small, with only a few cases reported globally. But as operating systems in cellphones become standardized, hackers will probably begin focusing on vulnerabilities in those systems as they have with personal computers. And as cellphones and personal digital assistants connect to the Internet at ever faster speeds, more users will be able to download files with attachments—some of which may be infected. Asia, where high-speed networks and text messaging on mobile phones are common, is the most vulnerable to these threats. As carriers in Europe and North America adopt similar technology, they will confront the same kinds of hazards. Telecommunications companies currently spend as much as $8 billion a year fixing handsets with programming errors, faulty mechanics and other problems. Now some are scrambling to prevent virus attacks that could cost carriers millions of dollars more in repairs and lost business.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2003-12-04 **computer virus crime authors successful Microsoft piracy**

NIPC/DHS

December 03, Reuters — Web virus authors 'winning battle' — Microsoft.

Creators of computer viruses are winning the battle with law enforcers and getting away with crimes that cost the global economy some $13 billion this year, a Microsoft official said Wednesday, December 3 at a cybercrime conference in Germany. Counterfeit centers are shifting from California and Western Europe to countries including Paraguay, Colombia and Ukraine said David Finn. In Asia, pirate plants have emerged in Vietnam, Macao, and Myanmar (Burma) in addition to more established facilities in Indonesia, Malaysia and Thailand. "So far they are getting away with it...Very few have been identified or prosecuted or punished," Finn said. He cited estimates by Business Week that financial damage this year from bugs like the Blaster worm and the SoBig.F e-mail virus, which crashed systems and disrupted Internet traffic around the world, would total some $13 billion. The cost of protecting networks against such cyberattacks was put at $3.8 billion. Finn said "we shouldn't be surprised" if terror organizations were looking to recruit computer expertise. Len Hynds, head of the National High-Tech Crime Unit in Britain, said gangs were recruiting people with IT skills not only to help them commit cybercrime but to secure their own communications networks and avoid detection. He said companies needed to recruit more carefully.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2004-01-06 **open source database technology growth**

NIPC/DHS; http://news.com.com/2100−7344−5134836.html

January 05, CNET News.com — Open-source databases gaining favor.

Big companies are warming up to open-source database software, according to a new study. "Concerns over stability, expense and how well a database plays with others are leading a quickly growing number of...companies to seriously consider and implement an open source database solution," says Evans Data analyst Joe McKendrick. "We expect this trend to continue as the open source offerings are continually improved upon." Database companies, also touting speed and the ability to handle very demanding processing tasks, have boosted efforts to make databases more reliable and cheaper to operate.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2004-01-08 **Anti-Spam Anti-Spyware Earthlink ISP security email blocking**

NewsBits; http://www.internetnews.com/xSP/article.php/3296851

From Anti-Spam to Anti-Spyware: ISPs Beef Up their Defenses

Roy Mark reviewed efforts by Internet service providers (ISPs) to increase their customers' security and antispam capabilities. ISPs have been integrating measures to fight spyware, spam, viruses, pornography and hackers.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2004-01-20 **IP network attack easy report survey estimate infrastructure protection**

NIPC/DHS; http://news.com.com/2100−7349−5141386.html?tag=cd_top

January 15, CNET News — Report: IP networks easy prey for cyberattackers.

The increasing use of Internet Protocol (IP) technology in power stations, railroads, banks and other critical infrastructure could spell big trouble, and soon, according to analysts. Although an actual act of cyberterrorism or cyberwarfare has never been recorded, the potential exists and is being facilitated by an increasingly connected world, according to a report released on Wednesday, January 14, by market-research firm Gartner. Cyberwarfare could be a reality by 2005, the company said. Technologies such as VoIP and the trend towards voice and data convergence give benefits cost and flexibility to businesses, but they also expose vital telecommunications networks to traditional forms of Internet attack, such as worms and viruses, according to the report. Gartner claims that, unlike traditional circuit-switched networks, VoIP networks have an inherent weakness when it comes to latency—any delay to the packets carrying the voice traffic disrupts communication. A massive denial-of-service attack could "degrade call performance by slowing voice packet arrival at a given destination" and effectively cut off voice communication, the report says. Other weaknesses flagged include the Supervisory Control and Data Acquisition interfaces used to connect a significant portion of critical infrastructure elements such as dams, railroads, electrical grids and power stations.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2004-01-20 **virus worm damage cost expense Trend Micro**

DHS/IAIP Update / Reuters

TREND MICRO SAYS 2003 VIRUSES CAUSED $55 BILLION DAMAGE.

Trend Micro Inc. said on Friday, January 16, that computer virus attacks cost global businesses an estimated $55 billion in damages in 2003, a sum that would rise this year. Companies lost roughly $20 billion to $30 billion in 2002 from the virus attacks, up from about $13 billion in 2001, according to various industry estimates. "The economic and financial impact of virus attacks will continue to climb in 2004," Lionel Phang, Trend Micro's Managing Director. Spam threats and network viruses will likely become more prevalent in 2004, he said. Blended threats also will remain the standard way to attack networks, where one virus file will create four to five different activities within the system." Viruses can also gain entry into computer networks via instant messaging channels, Phang added. "Spammers are going to put viruses and worms in email attachments, so (junk email) will become more than just a nuisance," said Natasha David, an analyst with International Data Corp. Analysts said the number of attacks between January and June 2003 exceeded 70,000, which is about twice the rate for 2002. "About 20 to 40 new and variant virus threats were reported to Trend Micro on a daily basis worldwide in 2003," Phang said.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2004-01-20 **virus worm damage cost expense Trend Micro**

NIPC/DHS; http://www.reuters.com/newsArticle.jhtml;jsessionid=K4R53JRC
ZZC24CRBAEKSFFA?type=technologyNews&storyID=4138782

January 16, Reuters — Trend Micro says 2003 viruses caused $55 billion damage.

Trend Micro Inc. said on Friday, January 16, that computer virus attacks cost global businesses an estimated $55 billion in damages in 2003, a sum that would rise this year. Companies lost roughly $20 billion to $30 billion in 2002 from the virus attacks, up from about $13 billion in 2001, according to various industry estimates. "The economic and financial impact of virus attacks will continue to climb in 2004," Lionel Phang, Trend Micro's Managing Director. Spam threats and network viruses will likely become more prevalent in 2004, he said. Blended threats also will remain the standard way to attack networks, where one virus file will create four to five different activities within the system." Viruses can also gain entry into computer networks via instant messaging channels, Phang added. "Spammers are going to put viruses and worms in email attachments, so (junk email) will become more than just a nuisance," said Natasha David, an analyst with International Data Corp. Analysts said the number of attacks between January and June 2003 exceeded 70,000, which is about twice the rate for 2002. "About 20 to 40 new and variant virus threats were reported to Trend Micro on a daily basis worldwide in 2003," Phang said.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2004-02-01 **outsourcing India globalization Wired**

NewsScan

INDIA: THE NEW FACE OF THE SILICON AGE

An interesting long article in the new Wired magazine gives a good picture of India as it becomes the "new face of the Silicon Age." Journalist Dan Fink writes of Indian engineers doing outsourced programming work: "What begins to seep through their well-tiled arguments about quality, efficiency, and optimization is a view that Americans, who have long celebrated the sweetness of dynamic capitalism, must get used to the concept that it works for non-Americans, too. Programming jobs have delivered a nice upper-middle-class lifestyle to the people in this room. They own apartments. They drive new cars. They surf the Internet and watch American television and sip cappuccinos. Isn't the emergence of a vibrant middle class in an otherwise poor country a spectacular achievement, the very confirmation of the wonders of globalization — not to mention a new market for American goods and services? And if this transition pinches a little, aren't Americans being a tad hypocritical by whining about it? After all, where is it written that IT jobs somehow belong to Americans — and that any non-American who does such work is stealing the job from its rightful owner?" (Wired Feb 2000)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2004-02-02 **spam e-commerce adverse affect customers shoppers scared away Transatlantic Customer Dialogue**

NewsScan

SHOPPERS SPOOKED BY SPAM

Spam is putting a damper on e-commerce, according to a survey published by the Transatlantic Consumer Dialogue, which indicates that 52% of respondents are shopping less on the Internet or not at all because of concerns that information disclosed in such transactions will generate more junk e-mail. "It is very clear that the majority of citizens are very troubled by unsolicited commercial e-mails. It is also very clear that bona fide businesses are losing money because the disreputable image of spam is making consumers uneasy about engaging in e-commerce." The results were released at an anti-spam summit held by the Organization for Economic Co-operation and Development (OECD), which is calling for international cooperation in tackling the scourge of spam and restoring consumer confidence in electronic commerce. "Most governments do view the Internet as a key to global economy. Spam certainly has the capacity to interfere with that," says Peter Ferguson, chairman of the OECD working party on information security and privacy. (Reuters/Washington Post 2 Feb 2004)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2004-04-23 **grammar poor technology sociolinguistics SMS instant messaging IM**

NewsScan

TECHNOLOGY MARCHES AHEAD, GRAMMAR GETS WORSE

Text messages, e-mail and the push for faster and more efficient communications are taking their toll on grammar, language experts believe. Queensland University of Technology sociolinguistics lecturer Jo Carr notes that people using e-mail and SMS text messaging are unconcerned about grammar and punctuation: "Grammar rules used to be an indication of social class and literacy in the past but today's society are doing things differently because language today serves the purpose of speed and social interaction." Macquarie Dictionary editorial committee member Sue Butler says grammar and punctuation are increasingly underused in Australia and around the world. "We now do get a failing in standards of punctuation that can be disconcerting," she notes. Media such as television advertisements and public billboards often sacrifice grammar and punctuation to engage audiences in the most efficient, shortest time possible, and correct grammar also is a low priority on live radio and television when politicians and news presenters make mistakes because they have to think and speak faster, says Butler. (The Age 23 Apr 2004, rec'd from John Lamp, Deakin University)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2004-05-19 **companies accountable vulnerable software corporations 150 lobbying unsecure Business Roundtable**

NewsScan

CORPORATE EXECS BLAST TECH INDUSTRY FOR SHODDY PRODUCTS

The Business Roundtable, a trade group for executives of 150 large U.S. corporations, has launched a lobbying campaign to make technology companies accountable for software that they say is vulnerable to hackers and overly complex to use. The group is urging tech firms to improve software design, make software easier to manage, and to continue tech support for software products that have been superseded by newer versions. "Up until now, the IT suppliers have deflected criticism and redirected criticism to end users… We would challenge the software industry to create products that are easier to use, where security is a default component of the software. It shouldn't require somebody with a technology degree to manage a home computer," says a Roundtable spokeswoman. The Roundtable's complaints mirror those made by some consumer groups and security experts, but were met with skepticism by technology representatives. "Cybersecurity is everybody's responsibility, including the vendors, the users, enterprises and government agencies," says a spokesman for the Information Technology Association of America. "No serious commentary will say that the user has no responsibility. We all have responsibilities to lock our doors in our homes and to buckle up when we get in cars." (AP 19 May 2004)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2004-08-03 **security spending prediction forecast increase 2005 decrease 2006**

DHS IAIP Daily;
http://www.itweb.co.za/sections/business/2004/0408031150.asp
?A=SEC&S=Security&O=FPT

August 03, ITWeb — Security spending to hit high in 2005.

Next year will be the high mark in corporate IT security spending, after which spending will drop to around 5% of IT budgets, says Gartner analyst Rich Mogull. "The reason for this will be because corporations would have to build more secure networks to protect the enterprise," Mogull said at the Gartner Symposium/ITxpo Africa being held in Cape Town this week. According to Gartner's predictions, by 2006, information security spending will drop to 4% or 5% of IT budgets on average as enterprises improve security management and efficiency. The lowest-spending 20% of organizations, the most efficient ones, will safely reduce the share of security in the IT budget to between 3% or 4% in two years. However, Mogull said security managers should include estimates of measurable security improvement with every request for spending. Business units should include security spending in all IT project requests. "The myth that software has to have flaws is only true if you use flawed software," he said. Mogull's list of security technologies that companies will need includes quarantine/containment, security audit capabilities and automated password management. Security technologies that would probably not be needed include personal digital signatures, quantum key exchange, and 500-page security policies.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2004-08-30 **information technology IT spending survey increase**

DHS IAIP Daily;
http://news.com.com/Survey%3A+IT+spending+to+grow+modestly+n
ext+year/2100−1022_3−5330227.html

August 30, CNET News.com — Survey: IT spending to grow modestly next year.

IT spending on goods, services and staff is expected to grow 6.4 percent in the United States next year, according to Forrester Research's quarterly survey of chief information officers. That expectation reflects modest growth and an improvement from the past two quarterly polls of CIOs. "Despite the negative perception from oil prices and software vendors putting out quarterly warnings, CIOs are generally expecting a modest growth cycle," said Tom Pohlmann, Forrester research director.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2004-10-22 **predictions robots UN Colin Angle iRobot**

NewsScan; http://apnews.excite.com/article/20041022/D85S6N380.html

NUMBER OF DOMESTIC ROBOTS TO INCREASE SEVEN-FOLD

The U.N.'s annual World Robotics Survey predicts that the use of robots for such domestic chores as mowing lawns and vacuuming floors will surge sevenfold by 2007, as the result of steadily dropping prices. Sales of window-washing and pool-cleaning robots are also set to take off. Colin Angle of iRobot says, "We are just at a point where robots are becoming affordable... and some of them can actually do real work." The World Robotics Survey predicts that by the end of this decade robots will "also assist old and handicapped people with sophisticated interactive equipment, carry out surgery, inspect pipes and sites that are hazardous to people, fight fire and bombs." (AP 22 Oct 2004)

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2004-11-01 **social engineering information security risk prediction ten years Garner research**

DHS IAIP Daily; http://software.silicon.com/malware/0,3800003100,39125457,00
.htm

November 01, Silicon.com — Social engineering becoming greatest risk.

The greatest security risk facing large companies and individual Internet users over the next 10 years will be the increasingly sophisticated use of social engineering to bypass IT security defenses, according to analyst firm Gartner. Gartner defines social engineering as "the manipulation of people, rather than machines, to successfully breach the security systems of an enterprise or a consumer." This involves criminals persuading a user to click on a link or open an attachment that they probably know they shouldn't. "Criminals are using social engineering to take the identity of someone either for profit, or to gather further information on an enterprise," said Rich Mogull, research director for information security and risk at Gartner.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2004-11-19 **research development R&D needed information security President committee US PITAC report**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/27979−1.html

November 19, Government Computer News — More funding needed for security R&D, IT committee says.

The government has shortchanged basic research into cybersecurity and should at least quadruple the money available for civilian research, a subcommitee of the President's IT Advisory Committee (PITAC) said in a draft report presented Friday, November 19. The government plays a key role in supplying the intellectual capital to improve the security of IT systems, said F. Thomas Leighton, chairman of the PITAC subcommittee on cybersecurity. "The government has largely failed in this regard," he said. In addition to being underfunded, government research efforts are becoming increasingly classified and focused on short-term results, the committee found. The subcommittee identified ten critical areas for future research including securing fundamental networking protocols, end-to-end system security, and cyberforensics tools. The subcommittee expects to present a final draft report at the next PITAC meeting on December 5.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2004-12-03 **information technology IT spending six percent growth 2005 prediction**

DHS IAIP Daily;
http://www.computerworld.com/managementtopics/management/its
pending/story/0,10801,98040,00.html

December 03, InfoWorld — IT spending to grow six percent in 2005.

In making its annual predictions for the upcoming year, IDC said it expects worldwide IT spending to grow 6.1% for 2005, a year that will be marked by "enormous turbulence" and significant consolidation and realignment in several key sectors. The 6.1% growth, a slight improvement over the 5% growth rate expected for 2004, means the IT market will exceed $1 trillion in overall spending. What will spur some of this higher growth will be the migration by larger IT shops toward more dynamic IT environments, those that innately offer greater efficiency and better business responsiveness. IDC predicted that there would be a concerted quest for "business value" that will force an increasing number of infrastructure players to partner and acquire technologies and companies that can help them zoom to the upper stack of dynamic IT environments. IDC also predicted the continued rise of open-source software, including the Linux operating system and compatible middleware applications.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-01-03 **information technology IT spending fall 2005 poll security spending increase**

DHS IAIP Daily; http://www.internetnews.com/stats/article.php/3453831\

POLL: IT SPENDING EXPECTED TO FALL

IT spending in 2005 is expected to fall somewhat according to a new poll from CIO magazine. However, there are certain sectors, including security and storage, that are reportedly expected to rise. The magazine conducted the poll during a one-week period in December that garnered 243 responses from a cross section of industries. Only 6.7 percent of poll respondents indicated that they expected IT spending to increase in 2005, which was a decline of 1.7 percent from the poll's November results (8.4 percent). IT security spending is on the upswing with 60.9 percent of poll respondents indicating that they were planning on increasing spending over the next 12 months. The expected growth in security spending represents a 7.7 percent increase over November expectations (53.2 percent). A number of different studies in 2004 painted a very vivid picture of enterprises' attitudes toward IT security spending. A September Ernst & Young report noted that only 17 percent said spending would increase significantly, and 52 percent thought it would increase only slightly. In July, research firm IDC reported that 59 percent of its survey base indicated that IT security spending would increase.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-01-12 **computer information physical security merge 2005 Forrester Research report**

DHS IAIP Daily;
http://news.com.com/Computer%2C+physical+security+expected+t
o+merge/2100−7348_3−5534312.html

COMPUTER, PHYSICAL SECURITY EXPECTED TO MERGE

Companies will increasingly integrate physical and computer security systems in 2005, spending over $1 billion in the United States and Europe, according to a report released this week from Forrester Research. Companies have generally treated physical security as part of the facilities department and computer security as part of the information-technology group. But employee information has increasingly become integrated, allowing businesses to link the two systems, Steve Hunt, an analyst with Forrester Research, said in the report. "Locks, cameras, entry systems, and even guard desks will be upgraded to work with the same computing systems that control computer and network sign-on, identity management and security incident management," he said in the report. Government projects to integrate physical and network security will make up the lion's share of the money being spent, Forrester predicted. Report: http://www.forrester.com/Research/Document/Excerpt/0,7211,36 137,00.html

---

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-02-10 **International Business Machines IBM security report mobile satellite car communications attack 2005 e-mail worm virus PDA**

DHS IAIP Daily; http://sys−con.com/story/?storyid=48190&DE=1

IBM SECURITY REPORT PREDICTS MOBILE/SATELLITE ATTACKS IN 2005

According to IBM, results from its 2004 Global Business Security Index Report show mobile devices becoming targets of viruses and worms. IBM, looking at potential security threats in 2005, said this may be the year for the aggressive spread of viruses and worms to handheld devices, cell phones, wireless networks, and embedded computers, which include car and satellite communication systems. The report, written by IBM's Global Security Intelligence Services team, said e-mail-based worms and viruses wreaked havoc on corporate networks in 2004. E-mail worms such as Bagle, Netsky and Mydoom led the pack in the number of variants and overall impact. During the latter part of 2004, a growing number of viruses aimed at PDAs and other mobile devices, such as the Cabir worm, were released. Such worms will likely be used by copycats and may start an epidemic of viruses aimed at mobile devices.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-03-02 **information technology IT executives survey cybersecurity highest priority 2005 IPIC conference**

DHS IAIP Daily; http://www.govexec.com/dailyfed/0305/030205p1.htm

IT EXECUTIVES SAY CYBERSECURITY IS TOP CONCERN

Leading federal information technology executives say that cybersecurity is their chief concern, according to an information technology vendor's survey. Forty-three percent of federal executives surveyed at a conference this week in Orlando, FL, said information technology security was their highest priority for 2005. More than two-thirds listed it is one of their top three concerns. The survey, released Wednesday, March 2, by CDW Government Inc., was conducted at the 2005 IPIC conference, and included 79 government technology executives attending the conference. The Federal IT Executive Survey results are similar to those in a recent survey by the Information Technology Association of America, which concluded that cybersecurity is the top priority of federal chief information officers. The IPIC conference is a forum for Government and Industry Information Technology (IT) executives to meet and share experiences of mutual interest. Survey: http://www.govexec.com/pdfs/IPIC.ppt

---

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-03-09 **US high-tech companies Microsoft Cisco HP warn investment lose competitive advantage**

DHS IAIP Daily; http://www.washingtonpost.com/ac2/wp−dyn/A17721−2005Mar8?lan guage=printer

U.S. TECHNOLOGY LEADERS WARN OF LOSING COMPETITIVE ADVANTAGE.

Leaders of high-tech companies said Tuesday, March 8, the United States risks losing its competitive edge without significant new investments in education, research and development and the spread of broadband technology. TechNet, which represents about 200 high-tech leaders, including Microsoft, Intel Corp., Cisco Systems, and Hewlett Packard, made its annual lobbying trip to Capitol Hill on Tuesday. TechNet officials cited some troubling indications that the U.S. is falling behind in high-tech development: the percentage of U.S. households with broadband access lags behind other highly-developed countries; U.S. investment in research and development has stayed flat for the last three decades, while it has grown significantly in competitor countries; and students in the U.S. are behind their counterparts in other countries in math and science. Among other recommendations, the group called on Congress to increase basic research funding, make permanent a research and development tax credit, and promote cybersecurity initiatives.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-03-15 **antivirus management stress survey**

http://news.bbc.co.uk/1/hi/technology/4349065.stm

ANTIVIRUS EFFORTS WORSE THAN DIVORCE

"Keeping computer viruses at bay is more stressful than divorce, warns a survey. The research revealed how European technology bosses were coping with the growing number of hi-tech threats...About 20% of those questioned said the stress of protecting their employer was worse than getting married, moving house or separating from a partner."

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-03-23 **study user blame encouraging spam bad e-mail behavior**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4375601.stm

STUDY BLAMES USERS FOR ENCOURAGING SPAM

A new report lays much of the blame for the ongoing problem of spam at the feet of computer users who open spam messages and even buy products or services advertised in spam. According to the survey, conducted by Mirapoint and the Radicati Group, nearly one-third of users have opened such messages, and one in ten has made a purchase. The report calls such actions "bad e-mail behavior" and said it encourages not just marketers but con artists to continue sending vast amounts of spam. Many adult-themed e-mail messages lure computer users into visiting Web sites that then install spyware or other malicious code. Graham Cluley, senior technology consultant for security firm Sophos, agreed that users bear much of the responsibility for spam's continued presence.
"If no one responded to junk e-mail and didn't buy products sold in this way," he said, "then spam would be as extinct as the dinosaurs." BBC, 23 March 2005

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-06-16 **us government report software future projection issues security risk management costs**

RISKS; http://www.cnsoftware.org/nss2report/NSS2FinalReport04-29-05PDF.pdf 23 91

SOFTWARE 2015 REPORT FROM CNSS

Jim Horning noted:

>There's a recent report by the Center for National Software Studies that does not seem to have been adequately publicized, and hence has not received the attention it deserves: "SOFTWARE 2015: A National Software Strategy to Ensure U.S. Security and Competitiveness"

Risks loom large in the discussion, including
* Risk of critical infrastructure failures
* Risk of sudden and severe economic loss
* Risk of loss of life and limb
* Risk of loss of public confidence
* Risk of loss of our technological edge and leadership

I've posted excerpts from the Executive Summary at both
http://bayosphere.com/node/554
and
http://horning.blogspot.com/2005/06/software-2015.html

<

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-06-21 **security study Gartner research malicious software impact mobile devices 2007**

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml?artic leID=164901703

MALICIOUS SOFTWARE NOT LIKELY TO HAVE LARGE IMPACT ON MOBILE DEVICES UNTIL 2007

Mobile phone and PDA users have more than two years to get ready for a quick-spreading worm, John Pescatore and John Girard, analysts at Gartner research. Client-side anti-virus software meant for cell phones and PDAs "certainly work", but vendors aren't selling them said Pescatore. In part that's because the threat of a fast-spreading malicious worm or virus has been overblown by security vendors. In fact, the conditions for a real threat-one that has the ability to infect more than 30 percent of mobile devices used in the enterprise-simply don't exist. The three factors that must exist before a Slammer- or MSBlast-style attack hits mobile devices, said Pescatore, are the large-scale adoption of smart phones, ubiquitous uses of wireless messaging to exchange executable files, and the convergence of operating systems to the point where one enjoys a majority share of the market. According to Pescatore and Girard, those three conditions won't co-exist until around the end of 2007. Furthermore, they believe that end-point security solutions for smart phones, cell phones, and PDAs are a waste of time because they often fail to block the most damaging viruses.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-06-22 **port sniffing attack warning TCP 445 SMB protocol Windows XP SP2 Gartner research**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/holes/s tory/0,10801,102687,00.html

INCREASED PORT 'SNIFFING' COULD HERALD ATTACK, RESEARCHER WARNS

An increase in "sniffing" activity on TCP Port 445 associated with a recently patched Microsoft vulnerability may be the signal of an impending attack attempting to exploit the flaw, according to an alert from analyst firm Gartner. The flaw in question is a remote code execution vulnerability associated with the Microsoft Windows Server Message Block (SMB) Protocol. Attackers who exploit this vulnerability could take complete control of affected systems. An increase in activity on TCP Port 445, which is associated with the SMB protocol, may be a signal that attackers are attempting to exploit the hole, Gartner analyst John Pescatore said in an alert posted Tuesday, June 21. Officials at Symantec also spotted increased activity on Port 445, but they downplayed any immediate threat. Alfred Huger, senior director of engineering at Symantec, said his company noted a " significant spike" in activity last Friday, June 17. Since then, activity levels have gone back to normal. "Activity targeting Port 455 is very common. It's almost like background noise," Huger said. Companies that have installed Microsoft's Windows XP SP2 should also be protected against the flaw because it closes off access to Port 445 by default, Huger said.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-06-28 **US-CERT warning scanning activity port 445 TCP Server Message Block SMB**

DHS IAIP Daily; http://www.us−cert.gov/current/current_activity.html#smb

SCANNING ACTIVITY ON PORT 445/TCP

US-CERT has seen reports indicating an increase in scanning activity of port 445/tcp. This port is used by Server Message Block (SMB) to share files, printers, serial ports and communicate between computers in a Microsoft Windows environment. Scanning for port 445/tcp has been active for a number of years. In 2004, Microsoft released a bulletin (MS04-011) describing a vulnerability in the Local Security Authority Subsystem Service (LSASS). Since this time a number of exploits have been published that take advantage of this vulnerability. More recently, Microsoft published two security bulletins (MS05-011 and MS05-027) that describe vulnerabilities in the Server Message Block (SMB). The LSASS and SMB services utilize RPC for communications. Ports configured to support RPC (i.e., port 445/tcp) may be scanned to locate vulnerable hosts. Scanning for port 445/tcp could be a result of attempts to exploit any of the vulnerabilities referenced above or attempts to authenticate to Microsoft Windows systems through brute force password attacks. More recently, an exploit was released that attempts to take advantage of the vulnerability described in MS05-011. While reports of successful system compromises using this vulnerability have not been confirmed, US-CERT strongly recommends that users patch their systems as soon as possible.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-08-03 **warning SANS Internet servers attack risk DNS cache poisoning**

DHS IAIP Daily; http://news.com.com/DNS+servers−−
an+Internet+Achilles+heel/2 100−7349_3−5816061.html?tag=nefd.lede

INTERNET SERVERS AT RISK OF ATTACK

In a scan of 2.5 million so-called Domain Name System machines, which act as the White Pages of the Internet, security researcher Dan Kaminsky found that about 230,000 are potentially vulnerable to a threat known as DNS cache poisoning. "That is almost 10 percent of the scanned DNS servers," Kaminsky said in a presentation last week at the Black Hat security event in Las Vegas, NV. The motivation for a potential attack is money, according to the SANS Internet Storm Center, which tracks network threats. Attackers typically get paid for each spyware or adware program they manage to get installed on a person's PC. Information lifted from victims, such as social security numbers and credit card data, can also be sold. Additionally, malicious software could be installed on a PC to hijack it and use it to relay spam. The DNS servers in question are run by companies and Internet service providers to translate text-based Internet addresses into numeric IP addresses. The cache on each machine is used as a local store of data for Web addresses.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-11-29 **cyber crime attack threat risk prediction security expert warning DHS Scott Borg**

DHS IAIP Daily;
http://www.infoworld.com/article/05/11/29/HNmoreattacks_1.html

SECURITY EXPERT: MORE SOPHISTICATED ATTACKS LIKELY

The cyber attacks of recent years have been relatively unsophisticated and inexpensive compared to the potential of organized attacks, a cybersecurity expert said Tuesday, November 29. Organized attacks by teams of hackers that have members with expertise in business functions and processes -- as well the rudimentary access and coding expertise that many current attackers have -- could have a huge impact on a nation's economy, said Scott Borg, director of the U.S. Cyber Consequences Unit, an agency supported by the U.S. Department of Homeland Security. "We will probably see terrorist groups, criminal organizations putting together combinations of talent," Borg said at the E-Gov Institute's Security Conference in Washington, DC. While past cyber attacks have done relatively small amounts of damage, coordinated attacks on important targets such as the U.S. electrical grid, the banking and finance industry, or the telecommunications and Internet industries could potentially cause many billions of dollars in damage, he said. Most viruses and worms knock out company networks for two or three days at most, but costs would multiply quickly for any coordinated attack on a critical U.S. industry that knocked out service for more than three days, said Borg, an economist.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-11-29 **RSS Really Simple Syndication security threat risk prediction Trend Micro expert Microsoft Internet Explorer IE**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1894232,00.asp

TREND MICRO: REALLY SIMPLE SYNDICATION IS WORM BOT'S NEXT TARGET

Security researchers at Trend Micro Inc. have pinpointed Really Simple Syndication (RSS) technology as a lucrative target for future bot worm attacks. David Sancho, senior anti-virus research engineer at Trend Micro, warned that RSS feed hijacking will become commonplace when Microsoft Corp. ships Internet Explorer 7 (IE7), a browser refresh that will feature built-in RSS support. In a white paper titled "The Future of Bot Worms," Sancho said the IE7 release "will open some interesting possibilities to worm creators." "The easy way of taking advantage of the popularity [of RSS] is to hijack the existing configured feed clients to automatically download new copies of worms and other threats to the infected computers. This is accomplished by pointing the already-configured client to different and malicious Web content," Sancho wrote. "The way this would work is checking if the system has any automatic feed download configured. If it does, it would just add or change an existing one to point to the malicious Website," he added. Sancho predicts that RSS feed hijacking attacks will serve as a passive download point that could easily bypass personal firewalls and other security barriers. David Sancho's white paper: http://www.trendmicro.com.au/global/products/collaterals/whi te_papers/BotsWP.pdf

---

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-12-07 **FBI report terror groups lack denial-of-service Internet attack capability**

DHS IAIP Daily; http://abcnews.go.com/Politics/wireStory?id=1383901

FEDERAL BUREAU OF INVESTIGATION: TERROR GROUPS LACK ABILITY TO MOUNT CRIPPLING INTERNET-BASED ATTACKS

Al Qaeda and other terror groups are more sophisticated in their use of computers but still are unable to mount crippling Internet-based attacks against U.S. power grids, airports and other targets, the Federal Bureau of Investigation's (FBI) top cyber crime official said Wednesday, December 7. Investigators keep a close watch on terror groups' use of computers but have not detected any plans to launch cyber attacks against major public institutions in the United States, FBI assistant director Louis M. Reigel said. The government has conducted simulated terrorist attacks on computer, banking, and utility systems, and Reigel said his division of around 1,100 agents treats seriously the prospect of such a strike. FBI cyber experts have noticed progress in the technical mastery suspected terrorists have shown online, he said. Terrorists also have made only infrequent use of stenography, the practice of hiding a text message in another kind of file, typically a picture, Reigel said.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-12-12 **Sober worm attack prediction January 2005 effect mitigation strip infections**

DHS IAIP Daily;
http://news.zdnet.co.uk/internet/security/0,39020375,39241437,00.htm

PREPARATION SYSTEMS ADMINISTRATORS CAN MITIGATE THE EFFECTS OF THE UPCOMING SOBER WORM ATTACK, SAY EXPERTS

Security administrators need not worry about the effects of the predicted Sober attack on January 5, as long as they take precautions and strip infections from their systems, security experts said on Friday, December 9. The impact of the upcoming attack can be mitigated by rooting out the problem at source, according to McAfee. Because a machine needs to be already infected with a variant of the virus for the update to take effect, machines can be prevented from downloading the updated virus by having the current version removed before January 5. "The effects can be mitigated by updating antivirus software, and scanning for normal versions of the variant," said Greg Day, security analyst at McAfee. McAfee said that administrators had a relatively large time frame in which to scan machines. However, McAfee warned that systems professionals should not underestimate the scale of the problem, and should be aware of the potential strain on their mail servers when the virus update is released.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-12-14 **AT&T security chief opinion Internet carrier predict prevent cyber attacks**

DHS IAIP Daily; http://www.techweb.com/article/showArticle.jhtml?articleId=1
75002779&pgno=1

AT&T SECURITY CHIEF SAYS CARRIERS SHOULD PREDICT, PREVENT ATTACKS

A centralized military presence would be more effective in warning a neighborhood of incoming attacks than if each family sent grandpa up to their roof with field glasses. AT&T Chief Security Officer Ed Amoroso used that analogy to explain his company's strategy for fighting cyber attacks. "Every one of you is fighting the same cyber war," said Amoroso, a keynote speaker Wednesday, December 14, at Interop in New York City. Carriers have the power to detect problems by observing activity with a broad view. That, he said, puts them in a position to detect and prevent attacks of all kinds, rather than requiring each subscriber to individually erect firewalls and take redundant precautions against attacks. Though software creators need to improve their methods and reach for higher security standards, carriers must also take responsibility in providing much-needed improvements, he said. Amoroso said that evolving applications need to be better integrated and better protected, especially with broadband leaving computers more vulnerable.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-12-21 **McAfee Avert Labs warning mobile cell phone user alert 2006 threat predictions**

DHS IAIP Daily;
http://www.techworld.com/security/news/index.cfm?NewsID=5051
&Page=1&pagePos=9&inkc=0

SECURITY COMPANY WARNS MOBILE USERS TO BE ALERT IN 2006

Rising threat levels for mobile users should come as no surprise, but McAfee's Avert Labs division has marked 2006 down as a potential turning point in the spread of malware to these platforms. Keylogging Trojans, adware, bots and backdoor programs will all hit users with greater frequency in 2006, with smartphone and "converged" users witnessing damage much greater than that seen on PCs because few currently bother to protect themselves. "Consumers are less likely to install mobile security versus PC security because the perceived risk from mobile threats is much less," a company release said. According to McAfee, mobile malware has grown ten times more rapidly than PC threats over any period of one year, and that in general "potentially unwanted programs" (PUPs) have grown by 40 percent in 2005 alone. The problem appears to be the increasing usefulness of Smartphones and PDAs. Having spent years as technological curiosities, they are now being sold to perform a variety of useful but risky operations such as mobile banking.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2005-12-28 **Instant messaging threats MessageLabs malicious target infect enterprises spam Trojan attacks report phishing emails**

DHS IAIP Daily; http://www.scmagazine.com/uk/news/article/533780/firm−im−
thr
eats−increase−next−year/

INSTANT MESSAGING THREATS TO INCREASE NEXT YEAR

MessageLabs warned that malicious users will increasingly target instant messaging (IM) in the next year, calling it a "widening backdoor" to infect enterprises with spam and trojan attacks. In a year-end report, the company said, "Spammers will diversify further into the IM ecosystems, as business adoption of IM increases and as the 'big three' IM protocols begin to standardize in 2006 and onwards." The report also noted a considerable increase in phishing emails sent this year, representing 13 percent of malicious emails intercepted during 2005, with a high of 27 percent in January. In total, more than 62.5 million phishing emails were intercepted by MessageLabs since Saturday, January 1, an increase of 238 percent from the 18 million caught the year before. The company also predicted more attacks on mobile devices: "Criminals will continue to attempt to gain access to users' mobile devices as the proliferation of wireless technologies like Wi-Fi spreads to airplanes, trains, and other public locations." Analysts found targeted attacks on specific industries became more common in 2005. Over all, MessageLabs reported one in every 36.15 emails sent this year contained a virus or Trojan. The report noted that cybercriminals chose more specific targets during 2005.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2006-01-04 **estimate prediction Sober worm time bomb under control**

DHS IAIP Daily; 23
http://news.com.com/Experts+Sober+time+bombs+under+control/2 100−7349_3−6018012.html?tag=cd.top

EXPERTS: SOBER TIME BOMB'S UNDER CONTROL

The Sober attack expected later this week is unlikely to have much effect on company systems, antivirus experts predicted. As reported last month, machines that were infected by Sober in November have the potential to download malicious code from certain Websites and then launch a new wave of viruses on Thursday, January 5, or Friday, January 6. But experts from antivirus companies F-Secure, Websense and MessageLabs all agreed on Wednesday, January 4, that this Sober attack is unlikely to cause many problems, because systems administrators and antivirus companies have had time to prepare for it. F-Secure raised the possibility that there might not even be an attack, as Internet service providers could block access to the malicious Websites. Websense agreed that the Sober attack likely won't have a major effect. The worm time bomb is contained in a variant of Sober that hit systems in November, clogging e-mail servers and stalling messages sent to Microsoft's Hotmail and MSN e-mail services.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2006-01-19 **cybercrime price FBI estimate $67 billion**

EDUPAGE; http://news.com.com/2100-7349_3-6028946.html 23

PUTTING A PRICE ON CYBERCRIME

A study by the FBI estimates that yearly losses to computer crimes exceed $67 billion. The study is based on the results of a survey of more than 2,000 organizations, of which 90 percent reported having suffered some form of computer attack in the previous 12 months, and 64 percent said they suffered a financial loss due to those attacks. The average financial loss was $24,000 per company. In estimating total losses, the FBI multiplied the average loss by just 20 percent of U.S. organizations because survey results are often skewed when reporting problems. Even with the significant reduction in the number of affected businesses, the total estimate was an enormous amount of money, far exceeding the $1 billion in losses each year to telecommunications fraud. Because of the relatively large sample size, Bruce Verduyn of the FBI said he believes the estimate is more accurate than other studies that have attempted to quantify losses to cybercrime.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2006-01-24 **spammer innovation ISP prediction Internet Service Providers**

DHS IAIP Daily; http://www.pcworld.com/news/article/0,aid,124408,00.asp 23

SPAMMERS WILL INNOVATE, MORPH, AND ADAPT IN 2006.

Representatives at several ISPs say they are gearing up for new challenges in 2006, when they expect spammers to grow more sinister. AOL spam fighters say that 2006 will be the year of the zombie networks. Zombie PCs are computers that have been infected by malicious code that allows spammers to use them to send e-mail. AOL also says that in 2006 there will be more "special-order" spam, in which phishers play off of your security concerns, especially the fear that your identity has already been stolen. Viruses and worms that take advantage of security holes in Microsoft's Outlook and Internet Explorer are a given for 2006, say experts. Richi Jennings, analyst at Ferris Research, says the recent Windows Metafile Format flaw is a perfect example. Also experts predict a new spam theme this year. In 2005 spam pitches ranged from cable descramblers to "free" iPods. But in 2006 spammers will be promoting things like investment opportunities and pumping penny stocks instead of pushing products. This is likely because it's extremely hard to differentiate a real stock tip from your broker as opposed to a fake one from a spammer, AOL says.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2006-02-15 **Homeland Security DHS online threat prediction 2006**

DHS IAIP Daily; http://www.informationweek.com/news/showArticle.jhtml?articleID=180202429 23

HOMELAND SECURITY SPELLS OUT COMING ONLINE THREATS.

The top Internet threats for 2006 will include more attacks through instant messages and cell phones, as well as a boost in identity hacks against online brokerage accounts, the Department of Homeland Security (DHS) and the National Cyber Security Alliance (NCSA) predicted Wednesday, February 15. By joining forces, DHS and NCSA hope to give consumers time to put additional protection in place on their PCs. Calling instant messaging networks "extremely vulnerable" and noting that cell phone malware is on the rise, the federal agency and the non-profit also predicted more "spear phishing," or targeted phishing attacks. Other threats to expect, include an increase in brokerage account break-ins.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2006-02-16 **DHS NCSA cyber threat predictions 2006 IM virus worms phishing cell-phone PDA viruses**

EDUPAGE; http://news.yahoo.com/s/nf/20060216/tc_nf/41677 23

PREDICTIONS OFFERED ON CYBERTHREATS

The Department of Homeland Security (DHS) and the National Cyber Security Alliance (NCSA) have issued a set of warnings about the kinds of cyberthreats the two organizations anticipate will be on the rise in 2006. Officials involved said the list of predictions is intended to raise awareness of computer threats in the hope that users will better protect themselves. "Arming consumers with a list of emerging threats is just the first step to educating consumers about the ever-evolving online security environment," said Ron Teixeira, executive director of the NCSA. The four areas identified in the list are instant-messaging viruses and worms, phishing, cell-phone and PDA viruses, and attacks on online brokerage accounts. Included with the warnings was acknowledgment that many computer crimes are not reported, complicating the task of tracking them. The agencies provided a number of strategies consumers can use to minimize their risks of being victimized.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2006-04-07 **estimate security risk Web services ignored Ajax Xquery**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/story/0,10801,110321,00.html 23

RESEARCHER: SECURITY RISKS IN WEB SERVICES LARGELY IGNORED.

In their rush to implement Web services, some companies may be exposing themselves to new security risks that they may not fully understand, a security researcher said on Thursday, April 6. During a presentation at the CanSecWest/Core06 Conference, researcher Alex Stamos outlined how a number of Web services technologies, including AJAX and the XQuery query language, could be exploited by hackers to attack systems. Stamos described an attack whereby a user could enter malicious code into a Web form and then get that code to run by calling up the company's customer service number and tricking a representative into inadvertently executing it. Stamos also showed how Web services requests could be used to conduct denial-of-service attacks.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2006-04-13 **Mac Windows XP dual boot security risk hype estimate Gartner**

DHS IAIP Daily; http://www.zdnet.com.au/news/software/soa/Boot_Camp_security_risk_is_just_hype_Gartner/0,2000061733,39251707,00.htm 23

BOOT CAMP SECURITY RISK IS JUST HYPE: GARTNER.

Any talk of Apple's Boot Camp software exposing the company's operating system to security risks is just hype and should be ignored, according to analyst firm Gartner. In a Garner advisory, research vice-president Michael Silver said: "The Mac software will be located on another partition within a different file system; thus, running Windows on a Mac will not expose the Mac software to more malware." However, if Boot Camp helps to increase the penetration of Apple's platform then OS X could attract the attention of cyber-criminals, he said.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2006-04-20 **Linux desktop malware activity prediction estimate warning**

DHS IAIP Daily; 23
http://www.computerworld.com/softwaretopics/os/linux/story/0
,10801,110710,00.html

LINUX DESKTOP GROWTH COULD SPUR NEW MALWARE ACTIVITY.

Besides Linux's low cost, its relative immunity from viruses, spyware, worms and other malware has long been one of the open-source operating system's key attractions to potential desktop users. But experts warn that could change if Linux begins to win a mass audience on the desktop, bringing in millions of users who are less proficient technically and less security-conscious than today's typical Linux user. The number of viruses that has so far targeted Linux remains small compared with the thousands of viruses and billions of dollars in estimated damage and lost productivity caused by Windows viruses. Some experts argue that because Linux, with its Unix heritage, was created from the ground up as a multi-user system with built-in access controls and privileges, it is fundamentally more secure than Windows. The relatively small number of Linux users spread among different versions of Linux has long hindered the growth of new software by creating a lower reward/effort ratio. That has also driven away virus creators, said Ed Metcalf, product marketing manager at McAfee Inc. Regardless, some Linux users, while reluctant to install antivirus software on client computers, are starting to take more safety measures.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2006-04-25 **insider infiltration threat business security concern UK crime agency**

DHS IAIP Daily; 23
http://news.com.com/Mafia+insiders+infiltrating+firms%2C+U.K
.+cops+warn/2100−7348_3−6064954.html?tag=cd.top

INSIDERS INFILTRATING FIRMS, UK CRIME AGENCY WARNS.

Employees are still one of the greatest threats to corporate security. Speaking Tuesday, April 25, at the Infosecurity 2006 conference in London, Tony Neate, e-crime liaison for the Serious Organized Crime Agency, said insider "plants" are causing significant damage to companies. "[Organized crime] has changed. You still have traditional organized crime, but now they have learned to compromise employees and contractors. [They are] new-age, maybe have computer degrees and are enterprising themselves," he added.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2006-04-26 **Federal Computer Week checklist new cyberthreat outline US government industry Cybersecurity Checklist Cyber Consequences Unit**

DHS IAIP Daily; http://www.fcw.com/article94201−04−26−06−Web 23

CHECKLIST OUTLINES NEW CYBERTHREATS.

The U.S. government and industry face many cyberthreats that, until now, have not received adequate attention, according to a new checklist outlining the threats. "We're talking about vulnerabilities where we can calculate the effects, and the effects are considerable," said Scott Borg, director and chief economist at the U.S. Cyber Consequences Unit. The unit's Cybersecurity Checklist looks at potential avenues for real-world cyberattacks and recommends ways to thwart them. The unit analyzed each of the 16 critical infrastructure sectors, Borg said. Many sectors say they follow international security standards but still have gaping security vulnerabilities, he said. Borg presented a draft version of the list at the GovSec conference in Washington, DC. The Department of Homeland Security has not yet approved the draft.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2006-05-01 **smarter spam techniques mimic e-mail friends real companies social engineering**

DHS IAIP Daily; 23
http://www.techweb.com/headlines_week/showArticle.jhtml?arti cleId=187002202

SMARTER SPAM COULD MIMIC FRIENDS' MAIL.

The next generation of spam and phishing e-mails could fool both software filters and the most cautious people, Canadian researchers said Sunday, April 30, by mimicking the way friends and real companies write messages. John Aycock, an assistant professor of computer science at the University of Calgary, and his student, Nathan Friess, explained that tomorrow's criminals could plant malicious programs on compromised computers. Those programs would scan the e-mail in the zombie's inbox, mine it for information and writing patterns, then crank out realistic-looking replies to real messages.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2006-05-05 **file sharing peer-to-peer P2P music piracy copyright intellectual property rights RIAA US Supreme Court**

EDUPAGE; http://online.wsj.com/article/SB114678807401044401.html 23

FILE-SHARING LANDSCAPE EVOLVES

The fallout continues from a U.S. Supreme Court ruling in June that found that the file-sharing service Grokster could be sued for copyright infringements taking place with its application. After that ruling, the Recording Industry Association of America (RIAA) pressed a number of file-sharing companies to modify their operations or face legal action. Grokster settled with the RIAA in November, and, in the latest announcement, BearShare has settled with the RIAA for $30 million and committed to stop facilitating illegal file sharing. Another file-sharing company, iMesh, which settled with the RIAA in 2004 for $4.1 million, announced it will acquire the assets of Free Peers Inc., which owns BearShare. Robert Summer, CEO of iMesh, said his company is "committed to transitioning the compelling experience of [peer-to-peer file sharing] to an authorized marketplace." Streamcast Inc., which owns the Morpheus file trading application, is pressing on with its defense against the RIAA.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2006-05-08 **Microsoft Vista security interference annoying prediction**

DHS IAIP Daily; 23
http://www.techweb.com/wire/security/187201321;jsessionid=FO
DGNYAZCAXS2QSNDBGCKH0CJUMEKJVN

MICROSOFT VISTA'S SECURITY WILL BE HIGHLY ANNOYING: YANKEE GROUP ANALYST.

Windows Vista's new security features will so annoy users that Microsoft won't meet its goal of 400 million copies in two years, Yankee Group's Andrew Jaquith said Monday, May Although Microsoft touts Vista as its most secure operating system ever, Jaquith sees it as somewhat of an albatross. "Anytime you put in a new security system, you're asking users to make changes," he said. But the shift in Vista, which Jaquith characterized as the first major security modifications since Windows NT, will require a huge alteration in how people interact with Windows. "In the Windows world, there are few limits on what a user can do," says Jaquith. That's part of the problem, says Microsoft, which has instituted a feature in Vista dubbed "User Account Control" (UAC) which takes a least-privilege approach to changes made to the OS and will require a user password for many common chores, including software installation.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2006-05-09 **Virginia cybercrime discussion test computer crime laws anti-spam**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1959790,00.asp 23

VIRGINIA OFFICIAL DISCUSSES THE FIGHT AGAINST CYBERCRIME.

Gene Fishel, assistant attorney general in the state of Virginia's Attorney General's office, delivered the keynote address during Ziff Davis' Tuesday, May 9, "Enterprise Applications Virtual Tradeshow," where he provided some prime examples of computer crime, and what IT shops can do about it. Because two of the United States' Internet powerhouses are headquartered in Virginia -- AOL and MCI -- Fishel said that about 80 percent of the traffic on the Internet passes through Virginia at some point. This little-known fact is actually what provides the Virginia Attorney General's office with jurisdiction over many criminal computer crimes. "It allows us as a state to test computer crime laws before they go federal," said Fishel. "Spam is a good example of that." The Virginia Attorney General's office was the first in the nation to criminalize spam with its anti-spam law; there's now a federal law in place modeled on Virginia's efforts.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2006-05-12 **search engines spread malware McAfee report**

DHS IAIP Daily; 23
http://www.betanews.com/article/Report_Search_Engines_Spread
_Malware/1147449437

REPORT: SEARCH ENGINES SPREAD MALWARE.

Security software company, McAfee said Friday, May 12 that the epidemic of spyware and viruses could be linked to search engines. According to research from the company, even seemingly benign search terms could bring up sites loaded with nasty payloads. The study, "The Safety of Internet Search Engines," looked at the five major search engines -- Google, Yahoo, MSN, AOL, and Ask -- and covered a period from January through April. Researchers found that in every search engine, popular keywords returned sites that could be potentially dangerous.

Category 31.2 *Estimates, guesses, predictions, forecasts concerning security*

2006-05-14 **US computer network attack cyber threat business dangerous Cyber Consequences Unit**

DHS IAIP Daily; http://www.networkingpipeline.com/showArticle.jhtml?articleID=187202905 23

CYBER THREATS TO U.S. BUSINESS GROW MORE DANGEROUS.

Attacks on U.S. computer networks could escalate from mere inconveniences to disasters that ruin companies or even kill people, according to the head of a cyber-security unit working with the U.S. government. Scott Borg, director of the Cyber Consequences Unit, or CCU, a Department of Homeland Security advisory group, said increasing intelligence "chatter" was pointing to possible criminal or terrorist schemes to destroy physical infrastructure such as power grids. The CCU is considering how to prevent attacks beyond ubiquitous e-mail hoaxes or computer viruses, with concerns rising about plots to cause power blackouts, tamper with pharmaceutical products or reprogram machinery to build dangerously defective products. Borg's CCU, a small independent unit funded by Homeland Security, spends its time trying to imagine how technology could be used to cripple the United States. It also holds cyber-security exercises for U.S. corporations and investigates reports of attacks on computer systems. A major crisis could be triggered, for instance, by shutting down critical computer systems for as little as four days.

31.3 New technology with security implications

Category 31.3 *New technology with security implications*

2002-07-01 **service bureau metered computing remote network**

NewsScan

IBM PUTS A METER ON SOFTWARE USE
IBM is introducing a new service called Linux Virtual Services that enables customers to run a wide variety of software applications on IBM mainframes located in company data centers, and pay rates based largely on the amount of computing power they use. This metered payment system marks a major shift from the more conventional outsourcing and Web hosting arrangements typical today. IBM executive James Corgel touted the new service, saying "we see a huge opportunity going forward. Our best estimate is that in five years, 10% to 15% of the $1 trillion IT market will be in the form of on-demand computing," with utility computing a significant part. Industry analysts remain a little more cautious about the prospects for metered computing. "We know customers are interested in doing this, but we don't know how many will," says one market researcher. Another added that "the pricing is still very complicated. It's not like electricity or even phone service." (Wall Street Journal 1 Jul 2002)
http://online.wsj.com/article/0,,SB1025472035492706880.... (sub req'd)

Category 31.3 *New technology with security implications*

2002-07-02 **nanotechnology supercomputing data storage density**

NewsScan

SPINTRONICS SHRINKS DATA STORAGE TO NANOSCALE
Researchers at the University at Buffalo in New York have developed a nickel-based, magnetic sensor, measuring only a few atoms in diameter, that could increase data storage capacity 1,000 times through the use of spintronics -- a field that takes advantage of electron spin as well as charge. Current technology used in data-reading sensors is based on giant magnetoresistance (GMR), where sensor resistance changes in a magnetic field. The new sensor developed at UB creates an effect called ballistic magnetoresistance (BMR), which uses an electrical conductor only a few atoms in size. Researchers say the technology could ultimately make it possible to store 50 or more DVDs on a hard drive the size of a credit card, or enable military personnel to carry supercomputers the size of a wristwatch into the field. (NewsFactor 1 Jul 2002)
http://www.newsfactor.com/perl/story/18446.html

Category 31.3 *New technology with security implications*

2002-07-08 **quantum computing nanotechnology brute force decryption encryption factoring public key cryptography PKC PKI**

NewsScan

RACE IS ON BETWEEN QUANTUM ENCRYPTION AND COMPUTING
Dozens of labs around the world are working to develop the first viable quantum computer, but scientists note that the tremendous boost in computing power that these tiny machines will deliver could lead to chaos, as the majority of encryption schemes now used on banking, e-commerce and government Web sites would become instantly obsolete. Conventional encryption codes rely on the premise that the amount of time it would take for a computer to factor a multi-bit key makes them an unattractive target. "Now we have the challenge of turning quantum computation into an engineering reality," says MIT professor Isaac Chuang. "If we could perform this calculation at much larger scales -- say the thousands of qubits required to factor very large numbers -- fundamental changes would be needed in cryptography implementations." Quantum encryption is already being deployed on a limited basis in some military and intelligence applications, and in response, companies like MagiQ Technologies are working to develop quantum encryption products for commercial release. "Between the intrinsic weaknesses of classic cryptography and the advanced research and development -- both commercial and academic -- that is being conducted around the globe, quantum encryption will be a widespread security tool sooner than you may think," says MagiQ Technologies spokesman Andy Hammond, who predicts his company will have a "commercially available solution" in 2003. (Newsfactor Network 8 Jul 2002)
http://www.ecommercetimes.com/perl/story/18490.html

Category 31.3 *New technology with security implications*

2002-07-15 **wireless technology broadband high speed download**

NewsScan

NEW TECHNOLOGY REVS UP WIRELESS TRANSMISSIONS
The latest technology aimed at souping up wireless transmissions is Orthogonal Frequency Division Multiplexing (OFDM). Flarion Technologies, which is adapting OFDM for use on wireless networks, claims that in theory, at least, OFDM could enable a consumer to download an MP3 music album in eight minutes, compared with an hour and a half or more using today's technology. The OFDM technology faces an uphill battle to commercial adoption, however, because industry heavyweights have already invested billions of dollars in other standards such as GSM and CDMA. "It's not necessarily the best technology that wins," says a Yankee Group analyst. Meanwhile, OFDM will get its first trial run on a small section of Nextel's network, and Verizon, which tested Flarion gear in its labs last year, says it is monitoring the development as a possible way to improve the high-speed services it launched in January. Verizon said it was also keeping an eye on other OFDM developers, including BeamReach Networks, Malibu Networks and Broadstorm Telecom. (Reuters 14 Jul 2002)

Category 31.3 *New technology with security implications*

2002-07-29 **satellite plane wireless telephone networks**

NewsScan

SATELLITE PLANES IN OUR FUTURE?
A company called SkyTower hopes that within two or three years it will have satellite solar-powered planes flying over metropolitan areas to demonstrate the ability of such aircraft to serve as a low-cost platform for delivering a host of next-generation wireless services. An executive of AeroVironment, SkyTower's parent company, says: "We expect that within 10 years we can have thousands of airplanes in the sky over the major cities of the world. Development of the plane is basically finished." SkyTower got its name because the high-altitude aircraft can be though of as essentially a 12-mile tall tower that provides better coverage than satellites and terrestrial towers, since it would be both closer to earth than satellites and yet high enough to avoid ground interference from buildings and trees. (AP/San Jose Mercury News 29 Jul 2002)

Category 31.3 *New technology with security implications*

2002-08-13 **nanotechnology transistors microprocessors**

NewsScan

INTEL AIMS FOR LARGE-SCALE PRODUCTION OF NANOSCALE CHIPS
Intel is taking the wraps off a new technology that it says will enable it to produce the world's smallest transistors in large-scale production. This latest innovation is the result of Intel's $12.5-billion spending spree over the last two years to improve manufacturing technologies and signals its intention to get a jump on rivals to be better positioned when the economy improves. The company's 90-nanometer production process entails a proprietary system for creating transistors whose key features are just 50 nanometers, or 1/2,000th of the width of a human hair. In addition, Intel is implementing a technology that effectively stretches the atoms apart in a silicon wafer to allow electrical current to flow faster, boosting performance, and is moving forward with plans to shift over to the 12-inch (300-milimeter) silicon wafer standard, up from the current eight inches. (Wall Street Journal 13 Aug 2002)

Category 31.3 *New technology with security implications*

2002-08-19 **laptop computers fuel cells portable digital divide international development**

NewsScan

THE EVER-EVOLVING LAPTOP
Laptop computers are making significant inroads in the computer market, with notebook growth pegged at 6% in the second quarter, despite a decline in overall sales. And while desktop machines are not likely to change much in style over the next few years, the laptop of the future will be smaller, lighter, and may even run on methane. PolyFuel, a spinoff of SRI International, is developing fuel cells that break down methane molecules into protons, electrons and carbon dioxide. While the protons pass through a special membrane, the electrons are maneuvered into a wire that powers the laptop. The replacement fuel cartridges initially will last two to three times longer than conventional batteries but eventually will last 10 times longer. Other companies are seeking to expand battery life by supplementing them with supercapacitators, which store energy at the chip level. "Supercapacitators hold more electricity than capacitators and transfer and recharge faster than batteries," says Anthony Kongats, CEO of supercapacitator startup Cap-XX. Batteries can be completely removed and the notebook will continue to run for about five minutes. Supercapacitator-enhanced notebooks could begin hitting the shelves in 2004 and notebooks powered by fuel cells could be available by late 2004 to 2005. Other likely laptop improvements include wireless capability that can switch effortlessly between WiFi and cellular networks, as well as low-power screens and new types of heat-dissipation techniques. (CNet News.com 19 Aug 2002)
http://news.com.com/2100-1001-951449.html?tag=fd_lede

Category 31.3 *New technology with security implications*

2002-09-03 **large-capacity disk recorder download copyright infringement piracy movies TV television**

NewsScan

SONY TAKES THE WRAPS OFF 'COCOON'
Sony unveiled the first of its "Cocoon" line of products that aim to replace the PC for downloading Internet content. The new video recorder sports a 160-gigabyte hard-disk, capable of recording up to 15 hours of HDTV or up to 100 hours of standard quality programming. It features an always-on broadband Internet connection that enables to access programming information online and records TV programs that match preferences selected by the owner. It can also "infer" preferences from previously recorded content and automatically record programs that fit that profile. The device even offers an apology if the owner rejects its selections. The new system will roll out in Japan on Nov. 1, but Sony has not yet said when it will be available for sale overseas. Cocoon is based on the Linux platform and will be priced at about $1,100. (Reuters 4 Sep 2002)

Category 31.3 *New technology with security implications*

2002-09-09 **nanotechnology memory chip logic**

NewsScan

HP DESIGNS NANOSCALE MEMORY CHIPS
Hewlett-Packard has created a new computer memory chip using nanotechnology to fit a 64-bit memory unit inside a single square micron (a micron is one-millionth of a meter). Although the new chip's capacity is too small to be useful, the development signals a key advance in the prevailing trend toward miniaturization. In addition, the chip combines for the first time both memory and logic by manipulating molecules caught in a grid of superthin platinum wires. "This is the first demonstration that molecular logic and memory can work together on the same nanoscale circuits," says an HP spokesman. (CNN.com 9 Sep 2002)

Category 31.3 *New technology with security implications*

2002-09-11 **nanotechnology transistors microprocessors**

NewsScan

AMD UNVEILS TINY DOUBLE-GATE TRANSISTORS
Advanced Micro Devices reports that it has succeeded in manufacturing the smallest double-gate transistors to date using industry-standard technology. The gate of the transistor, across which electrical current flows to turn the switch on, measures 10 nanometers, or 10 billionths of a meter. AMD says this latest development means that a chip now capable of holding 100 million transistors could conceivably pack about a billion of the nanoscale transistors. (Reuters/Los Angeles Times 11 Sep 2002)

Category 31.3 *New technology with security implications*

2002-09-18 **transistor nanotechnology computer performance speed**

NewsScan

INTEL DEVELOPS 'TRI-GATE' TRANSISTOR
Intel has developed a 'tri-gate' transistor, planned for large-scale production after 2005, which uses three rather than the current single logic gate, in order to increase computer performance The company says the new technology amounts to a three-dimensional extension of the terahertz transistor architecture it has already presented at research conferences. (Reuters/San Jose Mercury News 17 Sep 2002)

Category 31.3 *New technology with security implications*

2002-10-07 **palm pocket handheld computer low cost available**

NewsScan

PALM WILL OFFER A HANDHELD FOR $99
Staking out a position in the low end of the handheld computer market, Palm is offering an entry-level device for $99. Called the Palm Zire, it's made in China for less than $80. Industry analyst Tim Bajarin of the Creative Strategies consulting firm says Palm's low-end strategy has a pretty good chance of succeeding: "Palm should have this part of the market to themselves for actually quite a while. It's pretty much a win-win for Palm, for Palm software partners, for Palm after-market partners." Sony and Handspring, the No. 2 and No. 3 handheld manufacturers, also use the Palm operating system, are focused on the higher end of the market, and the companies that license Microsoft Pocket PC software usually charge $300 or more for their products. (San Jose Mercury News 6 Oct 2002)

Category 31.3 *New technology with security implications*

2002-10-17 **location surveillance wireless beacon**

NewsScan

NOAA EXPANDS 'PERSONAL LOCATOR BEACON' PROGRAM
Beginning July 1, the National Oceanic and Atmospheric Administration will extend to hikers, hunters and other land-bound recreational enthusiasts the same emergency locator service now available to pilots and boaters. The "personal locator beacons" — handheld devices equipped with GPS technology — work in zones not covered by cell phone networks and will cost $300 or more. "It takes the search out of search and rescue," says Randy Crosby, who heads up rescue teams in northern Alaska, where the devices have been tested for the past six years. In its 20 years of operation, the satellite rescue system has helped save some 14,000 people worldwide, including about 4,300 in the U.S. There is no penalty for accidental false alarms, but deliberate misuse can cost perpetrators up to $250,000 in fines, a six-year prison term and reimbursement of rescue costs. NOAA spokesman Daniel Karlson says the government works to educate beacon owners so "someone doesn't go out there and stub their toe and trip this thing off. We want this as a last resort. (AP 16 Oct 2002)
http://apnews.excite.com/article/20021016/D7MMLK0O0.htm

Category 31.3 *New technology with security implications*

2002-10-22 **Wi-Fi wireless communication mobile computing strategies plans predictions**

NewsScan

INTEL BETS BIG ON WI-FI
Intel is investing $150 million in companies involved in developing Wi-Fi technology, in the chipmaker's latest strategy to stimulate markets that could boost demand for its chips. Intel plans next year to introduce a chip technology for mobile computing — code-named Banias — that offers built-in Wi-Fi capability. The top three areas targeted for investment by Intel will be: companies helping to expand the number of Wi-Fi-equipped locations or otherwise helping to improve wireless infrastructure; companies working to solve some fundamental problems associated with the technology; and companies that improve the basic capabilities of the technology. The company plans to allocate the money for wireless investments from an existing $500 million communications fund. (Wall Street Journal 22 Oct 2002)

MOBILE PC SALES Another note on Intel's interest in Wi-Fi:
Melissa McVicker, the company's Asia Pacific regional manager, says that sales of mobile PCs are set to grow at a compounded rate of 15% to more than 50 million units by 2006 (compared to 30 million in 2002), and nine out of ten of them will make use of Wi-Fi or other wireless network technology. She says that "countries like Japan and Korea have about 50% of their PC purchases in mobile PCs, and there are a few others in Asia that are moving up quickly." Global demand for mobile PCs such as laptops and notebooks will soon outpace demand for desktop systems. (Reuters/San Jose Mercury News 22 Oct 2002)

Category 31.3 *New technology with security implications*

2002-10-28 **fast computing devices nanotechnology**

NewsScan

LIGHT-EMITTING SILICON BREAKTHROUGH
STMicroelectronics, the world's largest chip maker after Intel and AMD, has made a breakthrough in light-emitting silicon that could lead a new generation of more-powerful computing devices and higher-speed optical data-transmission systems. The efficiency of light-emitting silicon has been increased 100-fold, according to the researchers who achieved the breakthrough. Technology consultant Richard Doherty of Envisioneering says, "As we move toward placing entire computing systems on a single chip, the need to optically clock microelectronic circuits will become crucial." (New York Times 28 Oct 2002)

Category 31.3 *New technology with security implications*

2002-11-18 **children video games violence ethics crime education pornography theft**

NewsScan

CRIME PAYS
The new videogame "Grand Theft Auto: Vice City" sold more than 1.4 million copies the first two days it was available, at an average of $48 a copy. Chock full of violence, prostitutes and porn stars, it is probably the fastest-selling game in the 20-year history of the videogame industry. (USA Today 18 Nov 2002)

Category 31.3 *New technology with security implications*

2002-12-02 **virtual move characters child pornography**

NewsScan

MOTION-CAPTURE TECHNOLOGY REWRITES THE SCRIPT
Robert Zemeckis's new film project, "The Polar Express," is pushing the envelope in film-making technology, creating a live-action movie without filming any true "live" action. All of the scenes will be shot with a digital camera in front of a blank screen, with the sets to be filled in later by computers. The actors will be wired with motion-capture sensors that will store each movement digitally, to be used later as a guide for the animators who will create the actual film footage. Unlike other digitally animated movies like "Shrek," "The Polar Express" animators are striving to create images that actually look like the actors who will "star" in the film. The film will also combine characters based on real and virtual people — for instance, the child version of Tom Hanks' character will be backward engineered using photos of Hanks as a youth and 3D digital representations of his current facial and muscle structure. "This is an ambitious, exciting project for us. We've seen the early tests, and it's like nothing I've ever seen," says Martin Shafer, chairman and CEO of Castle Rock Entertainment, which is making the movie. (Los Angeles Times 2 Dec 2002)

Category 31.3 *New technology with security implications*

2002-12-04 **e-commerce intellectual property distribution subscriptions**

NewsScan

MOVIE SUBSCRIPTIONS OVER THE NET
RealNetworks, the software company specializing in the digital distribution of music and video over the Internet, and StarZ, the cable company, have teamed up to offer movie subscriptions over the Internet. Customers will pay about $10 a month, and will receive movie downloads suitable for viewing on computer displays; customers wanting to view the movies on a TV screen would need additional equipment. (AP/San Jose Mercury News 4 Dec 2002)
http://www.siliconvalley.com/mld/siliconvalley/4661968.htm

Category 31.3 *New technology with security implications*

2002-12-05 **digital divide broadband ISP Internet service provider dialup modem**

NewsScan

BROADBAND: FAST BUT PRICEY — APPARENTLY TOO PRICEY
Although 70% of U.S. households now have the technical option of subscribing to broadband services, only15% actually do, because many people are intimidated by the high cost of broadband: typically $40-50 a month, whether it is acquired through cable company or phone company. The problem is an upscale corollary of basic theorem of the digital divide, and is illustrated by the fact that whereas 28% of households with income above $100K a year have broadband access, a mere 4% of families with household incomes under $35K a year have such access. The industry is trying to reconcile itself to the basic facts of economic life; analyst Daryl Schoolar of the InStat/MDR research firm says: "We're working with a model of broadband adoption that is long and steady, rather than a big revolutionary pop." Which means that most network users will still be using dial-up connections a long, long time from now. Professor Andrew Odlyhzko of the University of Minnesota says all this is not too surprising: "There is hardly anything more ludicrous than the fax machine, but it is still around." (New York Times 5 Dec 2002)
http://partners.nytimes.com/2002/12/05/technology/05BROA.html

---

Category 31.3 *New technology with security implications*

2002-12-07 **wireless networks Internet access growth Wi-Fi**

NewsScan

AT&T, IBM AND INTEL FORM WI-FI VENTURE
AT&T, IBM and Intel are teaming up to back a new venture, called Cometa Networks, which plans to deploy a nationwide Wi-Fi wireless data network in coffee shops, hotels and other public venues. Cometa CEO Larry Brilliant says his company's goal is to install a wireless antenna within five minutes of anyone located in the top 50 U.S. metropolitan areas. A company spokeswoman says Cometa's advantage over the current informal hodgepodge of Wi-Fi hot spots is that it will offer "consistent, uniform service at a variety of locations. We think this is an important marketplace." Yankee Group analyst Roberta Wiggins says the involvement of the three industry heavyweights "obviously gives credibility to this whole arena." (Wall Street Journal 6 Dec 2002)
http://online.wsj.com/article/0,,SB103910982849940039 3.djm,00.html (sub req'd)

Category 31.3 *New technology with security implications*

2003-01-09 **smart wireless watch download**

NewsScan

MICROSOFT'S 'SMART' WRISTWATCH
Microsoft took the wraps off its new "smart" wristwatch that delivers custom-tailored data, such as sports scores, weather reports or traffic updates, via a new wireless network that Microsoft is cobbling together by leasing existing FM spectrum. Initially, the watches will work in 100 cities covered by the network. In order to access information, the wearer just checks the different "channels" on the watch to determine the best route home or how warmly to dress in the morning. The souped-up watches, made by Fossil, Citizen Watch and the Finnish firm Suunto, are expected to be available late this year, priced in the $100 to $250 range. The wristwatches are part of Microsoft's "Smart Personal Objects Technology" or SPOT initiative, which eventually will also include "smart" alarm clocks and refrigerator magnets. (Wall Street Journal 9 Jan 2003)

Category 31.3 *New technology with security implications*

2003-01-15 **surveillance privacy camera telephone**

NewsScan

CAMERA/CELL PHONES RAISE NEW PRIVACY ISSUES
Citing its customers' need for privacy, a chain of Hong Kong health clubs has banned the use of mobile phones in its locker rooms. At issue is the new generation of phones that can record and transmit video and still photos. Analysts say the new policy at Physical is one of the first cases they've heard of connected with the new cell phone capabilities. Fitness First, another Hong Kong chain that competes with Physical, is also considering a ban on cell phone use in some areas, and in nearby Macau, the use of the new camera-equipped cell phones has become an issue for the territory's 11 casinos. A spokeswoman for the casino company says traditional cameras are now prohibited in the establishments but that cell phones, which are extremely popular in Hong Kong, have yet to be forbidden. "This is something new that's come up. We have inspectors watching. Should they find anyone using these phones, because it's just like a camera, they will delete whatever photos were taken." (Reuters/CNet 14 Jan 2003)
http://news.com.com/2100-1033-980530.html

Category 31.3 *New technology with security implications*

2003-01-28 **location surveillance tracking objects people children wireless radio GPS**

NewsScan

FORGETFUL BOOMERS SPAWN MARKET FOR MEMORY AIDS
A stream of new products is hitting the shelves, aimed at solving one of life's daily annoyances: locating everyday objects such as keys or glasses that always seem to go missing just when you're in a hurry to leave. The products range from a FINDIT keychain that beeps after the user claps three times to the Sharper Image's "Now You Can Find It!" — a collection of plastic tags that can be attached to potentially elusive items, and then beep when users hit a button on the central device (of course, for it to work, users must make sure not to misplace the central device). The device and tags communicate with each other via radio frequency waves, and require that the user be within several meters of the hidden object's location. A handful of companies are also marketing GPS-enabled "kid finder" watches and pagers, and plans are underway to put homing devices on everything from luggage to pacifiers. Most ambitious of all, perhaps is the DIPO device, made by a French company of the same name, that not only finds an object but notifies the owner if it is about to be left behind. The central device — the size of a small cell phone — checks every few seconds to ensure that all tagged objects are within a certain radius — say, five meters. If it notices that the tag on the Palm Pilot, for instance, has moved outside the radius, it will beep or vibrate to remind the user to take it along. DIPO started out as the brainchild of the company's absent-minded CEO, Bruno Enea, who says, "I kept losing my credit card. I always forgot my passport. I realized I had to do something about this problem." (Wall Street Journal 15 Oct 2002)

RADIO FREQUENCY IDENTIFICATION (RFID) TAGS READY TO GO
A number of new consumer products from companies such as Gillette, Procter & Gamble, and Prada will come with embedded RFID (radio frequency identification) "tags" (actually, tiny computer chips), that will contain scannable information such as the product's serial number. The goal is to dramatically improve inventory processes, and other big companies poised to join the RFID movement are Johnson & Johnson, Coca-Cola, Pepsi, Home Depot and Target. Within a year or two RFID tags will be included in all kinds of products, including Michelin and Goodyear tires (to tell where a tire was made). Privacy groups are expressing fears that thieves will buy or make chip scanners that can crack security controls to scan shoppers' bags and know what they bought. (USA Today 28 Jan 2003)

Category 31.3 *New technology with security implications*

2003-02-10 **electrical power lines broadband communications network**

NewsScan

POWER COMPANIES TEST BROADBAND TECHNOLOGY
Energy utility Ameren Corp. and other power companies are testing technology that would deliver high-speed Internet access over their power lines, making every home electrical outlet an always-on Web connection. The FCC has applauded the energy companies' efforts, with chairman Michael Powell saying the technology "could simply blow the doors off the provision of broadband." But existing broadband providers and others are skeptical, saying that while they consider the technology intriguing, talk about it has been around for years, with nothing to show for it. "I think they're a long way from proving it, let's leave it there," says Larry Carmichael, a project manager with the Electric Power Research Institute. "The tests to date have been so small as far as looking at the financial and technical viability. It's still at the very early stage of development." (AP 10 Feb 2003)
http://apnews.excite.com/article/20030210/D7P3R6801.htm

Category 31.3 *New technology with security implications*

2003-02-13 **pen handwriting capture replay biometrics**

NewsScan

IT'S ALL IN THE SCRAWL: PENS THAT READ
Two companies, Logitech and Seiko, have developed pens that can be used to translate your handwriting into a computer. Here's how the $170 Logitech Io pen works: A pinhole camera next to the tip of the pen records your movements as you write on paper, and a microprocessor then turns this information into handwritten notes and diagrams (as many 40 pages worth). Later, you can insert the pen into a small desktop stand which communicates to a Windows personal computer through a USB connector. The handwriting is stored as a dumb graphic, but you can make simple editing changes and can e-mail the notes to someone else. (New York Times 13 Feb 2003)

Category 31.3 *New technology with security implications*

2003-03-07 **autonomic computing self-repair artificial intelligence**

NewsScan

IBM ZEROES IN ON AUTONOMIC COMPUTING IBM has established a new Autonomic Computing group, which will focus on R&D and product development in self-diagnosing computers that can take steps to fix themselves. The goal is to free up users from routine maintenance and repair tasks so that they can concentrate on other things. "The end game is to deliver a computing environment that is online all the time as a utility," says Nick Donofrio, senior VP of technology and manufacturing at IBM. "It sounds far-fetched right now, only because it's a lot of hard work." But ultimately, says Donofrio, "for consumers it means incredibly available data and a much richer (online) environment." IBM has been working on autonomic computing for more than a year, and has already incorporated the technology in several products, such as its newest DB2 Version 8 database software. The Autonomic Computing group hopes to expand use of the technology in IBM's products and create open standards for an autonomic computing architecture that would apply across computing platforms and manufacturers. (CNet News.com 20 Oct 2002)
http://news.com.com/2100-1001-962623.html?tag=fd_top_1

AUTONOMIC COMPUTING
IBM says it has developed software that allows networked computer systems to automatically adjust to unexpected demand surges by turning on additional computers on the network. This kind of capability is known as autonomic computing, which IBM also calls "on-demand" computing. As an example of on-demand computing, IBM says that if an airline is hit by a flood of customer responses to a special fare sale, it would take the system only a minute to note the changing load requirements and add another computer to handle the new demand. (Reuters/San Jose Mercury News 7 Mar 2003)

Category 31.3 *New technology with security implications*

2003-03-27 **e-mail traffic monitoring terrorist criminal activity logs**

NewsScan

E-MAIL TRAFFIC PATTERNS SIGNAL WHO'S IN CHARGE
A new technique developed at Hewlett-Packard's research labs in Palo Alto can quickly identify online communities and the key people in them. "If the CIA or another intelligence agency has a lot of intercepted e-mail from people suspected of being part of a criminal network, they could use the technique to figure out who the leaders of the network might be," says researcher Joshua Tyler. Tyler and his colleagues analyzed communications patterns using the lab's log of nearly 200,000 internal e-mails sent by 485 employees over a couple of months. They plotted lines between people who had exchanged at least 30 e-mails with each other, and found the grid included 1,110 links between 367 people. The researchers then used a computer algorithm that looks for critical links that form bridges between separate groups, which revealed 66 communities within the lab. To identify the leader in each community, they plotted the same network of e-mails using a standard algorithm that tries to arrange the connections in the least tangled way. This step identified the managers, who tended to cluster in the middle. "This approach puts in the middle the people who have the most diverse range of contacts in the organization — and these tend to be the leaders," says Tyler, who adds that the technique could be used to identify the ringleaders in criminal or terrorist gangs. (New Scientist 27 Mar 2003)

Category 31.3 *New technology with security implications*

2003-04-18 **Cisco WiFi telephone**

NewsScan

CISCO'S WIFI PHONE DUE OUT IN JUNE
Cisco plans a June rollout for its 7920 portable phone, which will use a WiFi network to connect. A future update will combine conventional cellular and WiFi capabilities in one handset. Meanwhile, the competition is heating up as similar phones are planned by Motorola, Avaya and WiFi equipment maker SpectraLink. However, the short battery life of these "multimodal" devices likely will prove a technological hurdle for companies planning to tackle the market, says an Aberdeen Group analyst, who based his criticism on his own experience with a Toshiba WiFi-enabled handset that needed recharging after only 75 minutes of use. (CNet News.com 18 Apr 2003)

Category 31.3 *New technology with security implications*

2003-04-21 **new tool counterterrorism search find pattern recognition database**

NIPC/DHS

April 17, Government Computer News — Data management system gets new analysis tool.

An automated data analysis tool will power a new FBI counterterrorism database, letting bureau analysts easily pore through more than 1 billion documents. The tools, ClearTags and ClearResearch, will draw patterns from terrorism-related intelligence collected from several sources into a centralized data mart that's part of the agency's modernized Trilogy network. The applications are intended to ease information sharing between the FBI and organizations at the CIA and Department of Homeland Security. The tools will also give intelligence officers a quicker method for scanning various databases at the Bureau of Alcohol, Tobacco and Firearms, Defense Department, Drug Enforcement Agency, State Department, and state and local agencies.

Category 31.3 *New technology with security implications*

2003-04-29 **Microsoft digital newspapters intellectual property rights**

NewsScan

MICROSOFT TARGETS DIGITAL NEWSPAPERS
Microsoft is developing software geared toward delivering digital newspapers, said chairman Bill Gates at the Newspaper Association of America's annual convention Tuesday. The new software will enable newspapers also to provide services like video messaging and bill-payment to readers across a variety of devices. Publishers who continue to view their Web sites as an add-on feature of their print operations are ignoring the next generation of readers, said Gates. "We see the online newspaper as one where it takes all the strengths [of current newspapers] and then adds in new capabilities." Readers not only will be able to read about an upcoming concert, but also will have the ability to hear audio clips and purchase tickets, added Gregg Brown of Microsoft's e-periodicals team. (AP/Wall Street Journal 29 Apr 2003)

Category 31.3 *New technology with security implications*

2003-05-06 **bill gates microsoft security system hard-wired technology protect medical records**

NewsScan

GATES ON MICROSOFT'S NEW SECURITY SYSTEM: USE IT OR DON'T IT
Microsoft's Bill Gates thinks people should have no fears about the company's new hard-wired security technology — but reminds them that they don't have to use it unless they want to: "This is a mechanism that if people want to use, for example, to protect medical records, they can use it. It's a lot of work to do this stuff, and we think consumers will want those privacy guarantees. If they don't want them, then fine, ask me about our other work." Chipmakers Intel and AMD are working on the hardware aspects of the technology, which will provide the creators or owners of digital content a very high level of control over that content, allowing it to be viewed only by trusted employees or paying customers, and locking out snoops and vandals. Microsoft is calling its technology "Next Generation Secure Computing Base." (AP/San Jose Mercury News 6 May 2003)

Category 31.3 *New technology with security implications*

2003-05-10 **Verizon Wi-Fi wireless payphone urban areas terminals Bell Canada Lawrence Babbo**

NewsScan

VERIZON TO TRANSFORM PAYPHONES TO WIFI TERMINALS
Verizon Communications, following the lead of Bell Canada, is planning to install WiFi terminals in payphones located in busy urban areas, according president Lawrence Babbo. "All of our payphone people have already told us (that the phones would make good wireless access points.) That will probably be the vehicle we use, probably in Manhattan." Verizon already offers WiFi equipment to its DSL customers, and last November began offering WiFi connectivity to small and medium-sized businesses. Bell Canada has been testing the concept at payphones in Toronto and Montreal, and several independent phone companies are interested in following suit. (AP 10 May 2003)

Category 31.3 *New technology with security implications*

2003-05-28 **hacker university michingan rollback techonology track transactions administrators system authorized ReVirt backup restore intruders**

NIPC/DHS

May 28, SC Infosecurity News — Hacker damage reversal technology revealed.

The University of Michigan is developing a rollback technology that allows administrators to track all transactions on a system, whether authorized or not, and reverse those transactions when required. The ReVirt technology is still way off completion but, according to Peter Chen, associate professor of electrical engineering with university, several commercial products can record all changes made to a hard drive, allowing users to restore their systems to a previous backup point. But, he said, none of these products allow system administrators to replay an intruder's actions on a step-by-step basis.

Category 31.3 *New technology with security implications*

2003-05-29 **pornography tiny storage device videos photos law enforcement**

NewsScan

TINY DEVICES OFFER LAW ENFORCEMENT CHALLENGE
Portable storage drives continue to gain popularity among child pornography collectors. The typical drive is as small as a cigarette lighter yet holds 128 megabytes of data and costs only $100 or less; it device plugs directly into most PCs, and can store entire movies or hundreds of digital photos. Sgt. Art Martinez of the San Mateo County Sheriff's Department in California explains that the devices offer a completely new challenge to law enforcement officers: "A lot of officers will look at them and don't know what they are. It's just another thing that we need to be looking for." (San Jose Mercury News 29 May 2003)

Category 31.3 *New technology with security implications*

2003-06-12 **privacy problems 3rd generation image capable cell phones**

NewsScan

3RD-GENERATION PRIVACY PROBLEMS
In Australia, that country's Royal Life Saving Society (a lifesaving and lifeguarding organization) intends to ban 3rd-generation image-capable cell phones from swimming pool changing rooms: "We, as operators and as providers of guidelines to the industry in this particular case, we just want to make sure that people are aware. We make every reasonable step to make sure that the privacy of individuals and, as I say, the private parts of individuals are not exposed where they don't want them to be exposed," says a spokesman for the Society. The potential for mischief with the new technology is apparent from the remarks of a student who reported: "One of my mates who's got one actually, as a joke, said that you could stand on the elevators and take photos up girls' skirts, which I thought was a bit much. He was only joking, he wasn't being serious, but, sure enough, the potential is there." Australia's privacy commissioner, Malcolm Crompton, says: "We need the social debate to make sure we use these technologies the way we want them to be used, we need to demand that technologies are developed the right way, we need laws in place, as appropriate, to back up those social norms." (ABC News Australia 12 Jun 2003)

Category 31.3 *New technology with security implications*

2003-06-16 **RECONFIGURABLE chip designs laptops**

NewsScan

RECONFIGURABLE CHIP DESIGN
A coming trend in chip design will be the use of software that can, in an instant, reconfigure a microchip's circuitry. Paul Master of QuickSilver, which has created a prototype the chip, says: "Until now, the hardware had to match the problem. Now we can change that." Possible uses of reconfigurable chips will include: cell phones that can work anywhere in the world; portable computers that can wirelessly and automatically connect to the Internet using the most suitable radio frequency; and consumer electronics devices that can easily adjust to every new technical standard in digital sights and sounds. (New York Times 16 Jun 2003)

Category 31.3 *New technology with security implications*

2003-06-18 **united airlines E-Mail domestic flights attachments**

NewsScan

UNITED TO OFFER E-MAIL ON DOMESTIC FLIGHTS
By the end of the year, United Airlines will become the first domestic airline to offer e-mail on all of its domestic flights. Industry analyst Jonathan Gaw of IDC says the service will be a good attraction for business users, who both need their e-mail and who can expense it." For $15.98 a flight, a passenger will be able to send and receive e-mail and attachments, by connecting a laptop computer to a jack on the Verizon Airfone handset available throughout the plane. (Baltimore Sun 18 Jun 2003)

Category 31.3 *New technology with security implications*

2003-06-23 **cell phone commerce buy stuff bookings paying**

NewsScan

EUROPEAN PAY-BY-CELL-PHONE PLANS

Four of Europe's top wireless carriers have created a new clearinghouse for taking payments for small purchases directly from mobile phone customers. Using the slogan "Pay for stuff with your mobile," the promoters are saying: "Our aim is for you to see it on music Web sites, when making a flight booking, or even when paying a bus fare." The carriers are Britain's Orange SA and Vodafone, Spain's Telefonica Moviles, and Germany's T-Mobile. (AP/San Jose Mercury News 23 Jun 2003)

Category 31.3 *New technology with security implications*

2003-09-10 **internet control VoIP voice phone PC household equipment 802.11 wireless**

NewsScan

VINT CERF ON THE FUTURE OF VOIP
Vint Cerf, senior VP of Internet Architecture and Technology for MCI, talks about the next-generation phone services based on VoIP (voice over Internet protocol) that are now being rolled out: "You can show up at a hotel and register your normal telephone number — as long as you can plug in your PC to an Internet service. What that means is your visibility in the communications world is now portable. Wherever you are, your communications are (there also). You can control where things go. If someone's trying to send a fax, you can vector that to your e-mail as an attachment or vector it to a different fax machine. There's an incredible amount of interaction over what had been completely separate services." Looking to the future, Cerf says the most important next-generation service is the ability to use the Internet as a household control system. "If you're like me, you have consumer equipment with remotes around the house. I can't figure out which one's which. And once I get the right one, the batteries are dead. Why not Internet-enable everything? Then it's possible to just have a single radio-based device, maybe 802.11-enabled, that lets you interact with all those appliances. You don't even have to be home. Obviously there are some security issues involved. You need strong authentication to make sure some 15-year-old next door won't reprogram your house." (CNet News.com 10 Sep 2003)

Category 31.3 *New technology with security implications*

2003-09-18 **Intel wireless future radio peer-to-peer mesh network access technology WiMax 802.16**

NewsScan

INTEL BETS ON WIRELESS FUTURE
Intel chief technology officer Patrick Gelsinger says the chip giant is focusing on a wireless future and is contributing to a "renaissance of the radio" through research in antennas, networks and other technology. At this week's Intel Developer Forum, Gelsinger demonstrated Intel's MIMO (multiple input, multiple output) antenna technology, which adds multiple antennas to both transmitters and receivers to improve performance significantly. He told participants that the company is also exploring the concept of a "mesh" network, which enables devices on a wireless network to communicate more easily using the same idea behind peer-to-peer networks. "We want to make wireless 'the' access technology. Simply put, no more copper," said Gelsinger. Future plans also call for new chips based on the 802.16 WiMax standard. WiMax, or Worldwide Interoperability for Microwave Access, is being touted as a broadband wireless access alternative to cable, DSL and other last-mile technologies. (CNet News.com 18 Sep 2003)

Category 31.3 *New technology with security implications*

2003-10-02 **security risk overlook telephone VoIP voice over IP**

NewsScan

OVERLOOKED SECURITY RISK: THE TELEPHONE
As corporate phone systems become increasingly complex and computerized, criminals are finding new ways to infiltrate company networks, and the problem becomes magnified as businesses turn to IP-based phone systems. "This is the first time that a computer virus can stop your telephones from working," says PricewaterhouseCoopers senior manager Mark Lobel. "There is a whole new class of attacks that can occur. The essence of the problem is that everyone is looking at this as a new technology for voice — the way we're sending voice communications is absolutely new. But the data is still riding on the same infrastructure that was pounded by recent problems like SoBig." To counteract the threats, phone system administrators need to be much more vigilant about password management and may even consider locking out certain country codes. "In fact, you should probably consider the risk associated with VoIP systems to be as high as the threats to your organization's most sensitive data. If someone in your IT department gets paged when your firewall goes down, they should also be paged when 40 new voicemail boxes mysteriously appear on your IP system," says Lobel. (E-Commerce Times 2 Oct 2003)

Category 31.3 *New technology with security implications*

2003-10-19 **self-destructing e-mail Microsoft Office 2003**

NewsScan

MICROSOFT TOUTS SELF-DESTRUCTING E-MAIL
Microsoft's new Office 2003 software, set to debut on Tuesday, will include an e-mail feature that can be used to time-stamp messages, directing them to delete themselves on a certain date. In addition, senders will be able to restrict forwarding and printing of messages by the recipient. The new Information Rights Management software could run into opposition from U.S. regulators, who view destroying e-mail as on a par with shredding documents. Earlier this year, Morgan Stanley was fined $1.65 million for failing to keep e-mail records, despite the company's claim that it due to oversight rather than a deliberate attempt to evade financial investigation. (BBC News 19 Oct 2003)

Category 31.3 *New technology with security implications*

2003-10-21 **stereo Japan download online music copyright intellectual property**

NewsScan

NEW STEREO LINKS DIRECTLY TO ONLINE STORE

Four major Japanese electronic makers have unveiled a prototype of a next-generation audiovisual system that downloads music directly from the Internet without a PC and is expected to hit the shelves in Japan early next year. Officials from Sony, Sharp, Pioneer and Kenwood said there are no plans to distribute the Linux-based device outside Japan. The test models from Any Music Planning sport Ethernet ports and LCDs automatically set to access a Web site run by LabelGate, a Japanese online music store. Users can browse, download, store and play songs, which can also be recorded on mini-disc or transferred to other devices. "Ultimately, our dream is to make the service a worldwide standard," says Any Music CEO Fujio Noguchi. (AP 21 Oct 2003)

Category 31.3 *New technology with security implications*

2003-10-30 **USB flash drives data leakage security policies precautions**

Network World Fusion Security Newsletter
http://www.nwfusion.com/newsletters/sec/2003/1027sec1.html &
http://www.nwfusion.com/newsletters/sec/2003/1027sec2.html

Gone in a Flash

by John Bumgarner, MA, CISSP, GCIH, IAM, SSCP
& M. E. Kabay, PhD, CISSP

In the movie "The Recruit," (Touchstone Pictures, 2003) an agent for the Central Intelligence Agency (played by Bridget Moynahan) downloads sensitive information onto a tiny USB flash drive. She then smuggles the drive out in the false bottom of a travel mug. Could this security breach (technically described as "data leakage") happen in your organization?

Yep, it probably could, because most organizations do not control such devices entering the building or how they are used within the network. These drives pose a serious threat to security. With capacities currently ranging up to 2 GB (and increasing steadily), these little devices can bypass all traditional security mechanisms such as firewalls and intrusion detection systems. Unless administrators and users have configured their antivirus applications to scan every file at the time of file-opening, it's even easy to infect the network using such drives.

Disgruntled employees can move huge amounts of proprietary data to a flash drive in seconds before they are fired. Corporate spies can use these devices to steal competitive information such as entire customer lists, sets of blueprints, and development versions of new software. Attackers no longer have to lug laptops loaded with hacking tools into your buildings. USB drives can store password crackers, port scanners, key-stroke loggers, and remote-access Trojans. An attacker can even use a USB drive to boot a system into Linux or other operating system and then crack the local administrator password by bypassing the usual operating system and accessing files directly.

On the positive side, USB flash drives are a welcome addition to a security tester's tool kit. As a legitimate penetration tester, one of us (Bumgarner) carries a limited security tool set on one and still has room to upload testing data. For rigorous (and authorized) tests of perimeter security, he has even camouflaged the device to look like a car remote and has successfully gotten through several security checkpoints where the officers were looking for a computer. So far, he has never been asked what the device was by any physical security guard.

This threat is increasing in seriousness. USB Flash drives are replacing traditional floppy drives. Many computers vendors now ship desktop computers without floppy drives, but provide users with a USB flash drive. Several vendors have enabled USB flash drive support on their motherboard, which allows booting to these devices. A quick check on the Internet shows prices dropping rapidly; Kabay was recently given a free 128 MB flash drive as a registration gift at a security conference. The 2 GB drive mentioned above can be bought for $849 as this article is being written; 1GB for $239; 512 MB for $179; 256 MB for $79; and 128 MB for $39.

In the next part of this two-part series, John and I will look at preventive measures for safe use of these devices.

* * *

In the last column, security expert John Bumgarner and I looked at the potential for data leakage introduced through the use of small portable USB flash drives.

To counter the threats presented by USB Flash drives organizations need to act now. Organizations need to establish a policy which outlines acceptable use of these devices within their enterprises.

* Organizations should provide awareness training to their employees to point out the security risk posed by these USB Flash drives.

* The policy should require prior approval for the right to use such a device on the corporate network.

* Encrypting sensitive data on these highly portable drives should be mandatory because they are so easy to lose.

* The policy should also require that the devices contain a plaintext file with a contact name, address, phone number, e-mail address and acquisition number to aid an honest person in returning a found device to its owner. On the other hand, such identification on unencrypted drives will give a dishonest person information that increases the value of the lost information – a bit like labeling a key ring with one's name and address.

* Physical security personnel should be trained to identify these devices when conducting security inspections of inbound and outbound equipment and briefcases.

Unfortunately, the last measure is doomed to failure in the face of any concerted effort to deceive the guards because the devices can easily be secreted in purses or pockets, kept on a string around the neck, or otherwise concealed in places where security guards are unlikely to look (unless security is so high that strip-searches are allowed). That doesn't mean that the guards shouldn't be trained, just that one should be clear on the limitations of the mechanisms that ordinary organizations are likely to be able to put into place.

Administrators for high security systems may have to disable USB ports altogether. However, if such ports are necessary for normal functioning (as is increasingly true), perhaps administrators will have to put physical protection on those ports to prevent unauthorized disconnection of connected devices and unauthorized connection of flash drives.

Because without appropriate security, these days your control over stored data may be gone in a flash.

* * *

John Bumgarner < mailto:john.bumgarner@cyberwatchinc.com > is President of Cyber Watch, Inc. < http://www.cyberwatchinc.com >, a security consulting firm based in Charlotte, NC. John has a rich background in national security and international intelligence and security work.

Category 31.3 *New technology with security implications*

2003-10-30 **superfast new processor Israeli company Enlight electron computation**

NewsScan

COMPUTING AT THE SPEED OF LIGHT
Israeli tech firm Lenslet has developed a superfast processor called EnLight that uses light rather than electrons to perform calculations at 8 trillion arithmetic operations per second. EnLight's optical circuits use a process called vector matrix-multiplication, which allows calculations to be performed on 256 optical inputs. The beams from these lasers are then added or multiplied together when shone on a device called a spatial light modulator, and the output is read by an array of light detectors. Lenslet founder Aviram Sariel notes that EnLight "is not a general purpose processor like a Pentium," but his company plans to custom-build the processors to perform a specific set of tasks for each client. Prices could range in the tens of thousands of dollars for each EnLight processor. (New Scientist 30 Oct 2003)

Category 31.3 *New technology with security implications*

2003-10-30 **DRM copy management BMG sales boos Anthony Hamilton music CD**

NewsScan

COPY-MANAGED CD BOOSTS SALES FIGURES
BMG Entertainment is cautiously optimistic about its latest experiment in discouraging music copying. The new Anthony Hamilton album, "Comin' From Where I'm From," hit the shelves in late September on a CD with built-in "copy management" technology. Buyers were limited to making three copies of the CD, and BMG says so far, the Hamilton album has experienced a slower-than-average sales drop-off — 23% vs. the typical 40-60% after the first week. "I know my science well enough to know that correlation does not mean causation," says Jordan Katz, senior VP of sales at BMG's Arista label. "I would not go out on a limb and say this was the only reason [sales] were down only 23%. However, I would say it was a contributing factor." The CD also allows users to e-mail songs to friends, who can download and play them on their computers for 10 days before they expire. A lack of buyer backlash against the technology has prompted Katz to put the copy management software on at least two more upcoming releases. (Washington Post 30 Oct 2003)

Category 31.3 *New technology with security implications*

2003-11-12 **ibm linux desktop operating system simplified computing scott handy**

NewsScan

IBM'S LINUX STRATEGY
IBM vice president Scott Handy says, "There is a lot of interest in Linux on the desktop from customers; this is definitely a trend with traction." IBM is now using Linux as the desktop operating system in a simplified computing environment that delivers, updates and maintains desktop applications over high-speed corporate networks. "The discussion with customers usually starts with Linux. But the huge gains come from using this server-based architecture, which is made possible by these Internet technologies. And Linux is one of them." Handy says IBM's Linux solutions could be easily adopted by bank branch offices, sales people, insurance agents, auto dealers and others. (New York Times 12 Nov 2003)

Category 31.3 *New technology with security implications*

2003-11-18 **cell phone secure conversation freedom phone XDA microsoft**

NewsScan

NEW CELL PHONE OFFERS SECURE CONVERSATION
German-based Cryptophone has developed a mobile handset that guarantees your conversation won't be tapped into by unscrupulous competitors or your local law enforcement officials. And while some observers say such phones could promote nefarious activities by the criminal crowd, privacy lobbyists say the new device is more of a "freedom phone" than a "terror phone." "It's a tremendous step forward, because the level of surveillance by authorities is breathtaking," says Simon Davies, director of the U.K.'s Privacy International. The Microsoft-based XDA handheld computer phone sells for about €3,499 (about $4,121) for two handsets, a price point that ensures the gadgets will be targeted at the corporate market. "Not many average consumers will pay that kind of money. The people who will be using it are in business," says Ian Brown, director of the Foundation for Information Policy Research in Britain. (Reuters 18 Nov 2003)

Category 31.3 *New technology with security implications*

2003-12-09 **Internet Protocol Voice VoIP Time Warner digital data plug regular phones**

NewsScan

TIME WARNER TO OFFER VOIP
The cable unit of Time Warner has developed a plan to send telephone calls using Internet protocol (VoIP) technology. VoIP sends phone calls as digital data over the Internet and lets customers plug regular phones into modems connected to the cable wire in their homes. Still, the chief executive of Time Warner Cable is not ready to declare victory over traditional phone companies, because those companies have the overwhelming share of the local telephone market, and "they're going to be around for a long time." (New York Times 9 Dec 2003)

Category 31.3 *New technology with security implications*

2003-12-16 **ipass T-mobile wi-fi wireless internet Ken Denman HotSpot mobile**

NewsScan

T-MOBILE TEAMS WITH IPASS ON WI-FI ROAMING
T-Mobile USA and iPass, two of the top U.S. wireless Internet access providers, have inked a Wi-Fi roaming agreement that will enable mobile workers to access the T-Mobile HotSpot network through the iPass virtual network. The move could spark broader adoption of Wi-Fi technology by corporations, which have lagged behind consumers in Wi-Fi use. Part of the reluctance on businesses' part has stemmed from security concerns, but they also have been waiting for the emergence of a nationwide service with broad coverage and enhanced reliability before jumping on the Wi-Fi bandwagon. "The Wi-Fi vision of both iPass and T-Mobile are in synch," says iPass chairman and CEO Ken Denman. "Both companies believe the addition of the T-Mobile HotSpot network to the iPass global Wi-Fi network of business-oriented venues represents a major step closer to the tipping point of Wi-Fi by the enterprise." (Financial Times 16 Dec 2003)

Category 31.3 *New technology with security implications*

2004-02-09 **Google hacking hobbyist technology uncover sensitive documents information Internet**

NewsScan

GOOGLE-HACKING TAKES OFF

Google is increasingly becoming a hacking tool for techno-hobbyists who seek out sensitive documents using Google's powerful search capabilities. "There's a whole subculture that's doing this," says Chris O'Ferrell, chief technology officer of security consultancy Netsec, who notes that Google is the search tool of choice for these folks because of its effectiveness. "The reason Google's good is that they give you more information and they give you more tools to search." Companies, organizations and government agencies could block Google from accessing documents by setting up a digital gatekeeper in the form of a robots.txt file that dictates which pages are accessible to Google, but many don't bother, leaving such sensitive information as medical records, bank account numbers, students' grades and the docking locations of 804 U.S. Navy ships, submarines and destroyers open to viewing. Search strings with "xls," or "cc" or "ssn" often bring up spread sheets, credit card and social security numbers linked to a customer list. "It's the easiest point-and-click hacking — it's fun, it's new, quirky and yet you can achieve powerful results," says security consultant Edward Skoudis. "This concept of using a search engine for hacking has been around for awhile, but it's taken off in the last few months." Companies are urged to be more careful about what they put on the Web in the first place, because thanks to caching technology, "Once it is placed online, it's very hard to get the digital horse back in the electronic barn," says Marc Rotenberg, executive director of the Electronic Privacy Information Center. (Washington Post 9 Feb 2004)

Category 31.3 *New technology with security implications*

2004-02-10 **VPN virtual private network Georgia state deployment**

DHS IAIP Daily; http://www.fcw.com/geb/articles/2004/0209/web−georgia−02 −10− 04.asp

February 10, Federal Computer Week — Georgia to build state VPN.

The Georgia Technology Authority this week released a request for proposals for a new statewide virtual private network (VPN). The new Multiprotocol Label Switching (MPLS) VPN would replace the existing frame relay network used by state, county and municipal government organizations. That includes schools, libraries and law enforcement agencies. It is expected to be cost at least $10 million). The MPLS VPN will allow administrators to ration and prioritize bandwidth for mission-critical applications. New security and privacy requirements - including federal mandates and common business needs - are also taking agencies beyond the existing network's capabilities. Initially, the network will provide data and video, including videoconferencing for distance learning and telemedicine. The architecture must, however, support the inclusion of voice over IP a year after the initial deployment. One of the biggest advantages to the new network will be the support for mobile workers, allowing users to connect via Digital Subscriber Line, cable modem or dial-up. In addition to standard telework environments, the mobile access will be key for public safety, family and children services site visits, and staff working in state parks.

Category 31.3 *New technology with security implications*

2004-03-01 **cell phone security telephone network attack RSA conference**

NIPC/DHS

February 27, Knight Ridder Newswire — Cell phone security.

Computer-security experts say cell phones could be the next carriers for computer-network attacks. Computer-security experts in San Francisco this week at the annual RSA Conference swapped stories about attacks and discussed the possible next big threat. Experts generally agree that 2004 will bring more worms and viruses that can spread among computers with increasing speed. But as computer users grow more savvy about protecting their machines from attack, hackers could turn their focus to the growing number of cell phones and other handheld devices. With more memory and faster processing power than before, these devices are mini-computers, connecting to the Internet and running many of the same programs as desktop machines. But they don't have anywhere near the same levels of protection from cyberattacks. "They are in growing numbers susceptible to the same types of attacks that we've seen on traditional wired machines," said Carey Nachenberg, chief architect with the research labs of the antivirus company Symantec. "The reason why we probably haven't seen any real worms for these platforms is they are not nearly as pervasive as the other platforms. That will change."

Category 31.3 *New technology with security implications*

2004-03-04 **hard disk drive HD heat monitor sensor health lifespan**

NewsScan

NEW SENSOR MONITORS HARD DRIVE HEALTH

Researchers at Carnegie Mellon University have developed a new heat-sensitive sensor that can alert computer users to imminent hard drive failure. "Essentially what we are trying to do is save the life of the computer hard drive. Hard drives get hot and the sensor is designed to pick up the slightest temperature variation," says CMU scientist Michael Bigrigg. The researchers predict that by using the dime-sized sensor they may be able to extend the lifespan of a computer hard drive beyond its 3.1 year average by tracking how much daily heat a hard drive endures. (Science Daily 4 Mar 2004)

Category 31.3 *New technology with security implications*

2004-04-30 **bar codes people tracking surveillance school Long Island**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/25816−1.html

April 30, Government Computer News — Long Island school tests bar codes for emergencies.

An elementary school on Long Island is trying out bar codes as a way to keep track of students during emergency evacuations. Bretton Woods Elementary School in Hauppauge, NY, held a drill on the morning of April 23. Overseen by Hauppauge Schools security director Edward Spear, the faculty evacuated about 800 children onto 16 school buses, which took them to a nearby high school. Stickers with bar codes were placed on the backs of the children's shirts as they left classrooms. When the students stepped off the buses, their bar codes were read by four people holding bar code readers and transmitted to a notebook computer for comparison against an attendance list. Each sticker held a Portable Data File 417 two-dimensional bar code. Although most of the tags were readable without problems, a few proved difficult to scan because they were wrinkled during transit, Spear said. The tags could be placed on identification cards or book bags as an alternative to placing them on clothing.

Category 31.3 *New technology with security implications*

2004-05-17 **remote control transportation trains reliance on technology**

DHS IAIP Daily; http://jacksonville.com/tu−online/stories/051504/bus_1561500 2.shtml

May 17, The Times-Union (Jacksonville, FL) — Remote-control locomotives safer, federal report shows.

Switching railcars using remote-control locomotives instead of engineers results in improved safety, according to a preliminary report issued Thursday, May 13, by the Federal Railroad Administration. Such locomotives are increasingly popular with railroads, including CSX Transportation and Florida East Coast Railway, but their use is criticized by the main engineers union, which says they result in increased accidents and injuries. The injury rate of railroad workers in rail yards across the country dropped 57.1 percent with remote-control locomotives, according to the study, which reviewed 2003 data from May 1 through November 30. When the locomotives are equipped with remote control, the engineer's job is eliminated, leaving the train to be run by a two-person team including a conductor equipped with a belt pack. Having fewer employees reduces railroads' labor costs. The Brotherhood of Locomotive Engineers and Trainmen fired back at the positive numbers with a statement saying they were derived solely from data provided by the railroads. It referred to a March AFL-CIO resolution calling for an end to the use of remote-control locomotives. The resolution said that without proper safeguards, it "places all rail workers at risk of injury and death."

Category 31.3 *New technology with security implications*

2004-07-23 **China national technology standards DVD Centrino Windows**

NewsScan

CHINA GOES IT ALONE ON HIGH-TECH STANDARDS

DVD? China's trying to do it one better -- with a technology called EVD. CDMA? The digital cell phone standard is so 2003, the Chinese say. Give TD-SCDMA a try instead. Intel's Centrino and Microsoft's Windows? If you're doing business with Beijing, better bone up on WAPI and Red Flag Linux, too. These days, China's dominant message is this: We'll embrace the world -- but on our terms. And nowhere is this more evident than in the realm of high technology, where behind the acronyms is a battle of standards that could have global repercussions. Pushed by their government, Chinese firms are shunning technological protocols invented abroad and developing their own.
They want Chinese-made video discs to run on Chinese-invented players, and they want Chinese consumers linking up with China-developed mobile gadgets. (The Age 23 Jul 2004) Rec'd from John Lamp.

Category 31.3 *New technology with security implications*

2004-08-16 **new technology PC masses illeterate uneducated developing countries affordable entertainment information**

NewsScan

A PC FOR THE MASSES

Carnegie Mellon University professor Raj Reddy is working with researchers at the Indian Institute of Science, the Indian Institute of Information Technology and the University of California Berkeley to develop a low-cost wireless PC designed for users in developing countries, particularly those with large populations who cannot read. The $250 PCtvt is controlled by a simple TV remote control and can function as a television, DVD player, telephone and videophone. Reddy sees his project not only as a philanthropic effort, but one that may even produce profits. "I kept asking myself, 'what would the device have to do for someone on the other side of the digital divide to be desirable?'" The result is a simple device that offers a seductive combination of connectivity and
entertainment. "Entertainment is the killer app, and that will smuggle something that is a lot more sophisticated into the home," says Tom Kalil, special assistant to the chancellor for science and technology at Berkeley. (New York Times 16 Aug 2004)

Category 31.3 *New technology with security implications*

2004-11-29 **surveillance software SAME see anywhere map anywhere Vincent Tao Canadian inventor**

DHS IAIP Daily; http://www.reuters.com/audi/newsArticle.jhtml?type=technology News&storyID=6946893

November 29, Reuters — Canadian inventor lets everyone be an armchair spy.

New Internet-based technology could soon turn regular computer users into armchair spies, a Canadian inventor said on Monday, November 29. Vincent Tao, an engineer at Toronto's York University said he has invented a mapping and surveillance tool called SAME (see anywhere, map anywhere), that produces images so sharp that geographic co-ordinates typed into a Website can reveal the make of a car parked on the street -- the resolution is two feet. Tao said the potential applications are broad, including defense, emergency response and environmental monitoring. He added that the technology could become widely available as early as next year.

Category 31.3 *New technology with security implications*

2005-01-04 **blogs Pew Internet and American Life Project RSS aggregators compile news sources told election**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4145191.stm

2004 A GREAT YEAR FOR BLOGS

According to a new survey by the Pew Internet and American Life Project, readership of blogs jumped significantly in 2004, as did the use of RSS aggregators. The survey indicated that blog readership rose 58 percent last year, with 32 million Americans now reading blogs. Eight million Americans have created a blog, according to the survey. RSS aggregators, which compile information from blogs and other online news sources based on user preferences, also saw significant increases, with six million Americans now using those tools. The increased use of such immediate tools as blogs and RSS in 2004 is attributed in part to close following of the U.S. presidential election. Those who have created blogs were found--on average--to be young, male, college-educated, and Web-savvy. Although many blog readers fall into similar demographic categories, much of the rise last year was among women and minorities. Despite the higher profile of blogs and increased use, more than 60 percent of those surveyed said they had not heard of blogs.

Category 31.3 *New technology with security implications*

2005-01-24 **machine learning cognitive science artificial intelligence pattern recognition intrusion detection logic programming**

DHS IAIP Daily; http://www.newscientist.com/article.ns?id=dn6914

MACHINE LEARNS GAMES "LIKE A HUMAN;" COULD POTENTIALLY DETECT INTRUDERS.

A computer that learns to play a 'scissors, paper, stone' by observing and mimicking human players could lead to machines that automatically learn how to spot an intruder or perform vital maintenance work, say UK researchers. CogVis, developed by scientists at the University of Leeds in Yorkshire, UK, teaches itself how to play the children's game by searching for patterns in video and audio of human players and then building its own "hypotheses" about the game's rules. In contrast to older artificial intelligence (AI) programs that mimic human behavior using hard-coded rules, CogVis takes a more human approach, learning through observation and mimicry. Chris Needham, a member of the CogVis team, says the system's visual processor analyzes the action by separating periods of movement and inactivity and then extracting features based on color and texture. Combining this with audio input, the system develops hypotheses about the game's rules using an approach known as inductive logic programming.

Category 31.3 *New technology with security implications*

2005-03-30 **grid computing network security threats large scale deployment confidentiality**

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1780849,00.asp

GRID COMPUTING CAN ALLOW SECURITY THREATS

Security experts on Wednesday, March 30, recommended that IT administrators clearly identify and understand the security risks associated with large-scale grid computing deployments. During Ziff Davis Media's Enterprise Solutions Virtual Tradeshow, the pros and cons of grid computing and safe data storage took center stage, with panelists stressing the importance of using best practices to protect the confidentiality of information passed over corporate grid systems. Lenny Mansell, senior security consultant at Triad Information Security Services LLC, warned that greater sharing of information and resources across traditional trust boundaries will result in increased risks that must be addressed as a matter of urgency. Mansell recommends that businesses deploying grid systems identify critical assets and the threats to those assets. Mark Teter, chief technical officer of Advanced Systems Group LLC, said the highly automated manner in which resources are allocated on a grid can be used by a malicious attacker to steal sensitive corporate data. Grid computing is the concept of using computers in the way that utilities use power grids to tap the unused capacity of a vast array of linked systems. Users can then share computing power, databases and services online.

Category 31.3 *New technology with security implications*

2005-06-07 **quantum computer cryptography security guarantee wireless link Massachusetts Harvard Boston University DARPA**

DHS IAIP Daily; http://www.newscientist.com/article.ns?id=dn7484

QUANTUM CRYPTOGRAPHY NETWORK GETS WIRELESS LINK

The world's first quantum encryption computer network has been expanded to include a wireless link that uses quantum communications codes. The wireless connection was added to the Defense Advanced Research Projects Agency (DARPA) Quantum Network, a quantum fiber-optic network buried beneath the ground in Massachusetts. The network was built by BBN Technologies with funding from DARPA. It now links ten different sites, including BBN's offices, Harvard University and Boston University. Most modern cryptography rests upon the difficulty of solving very complex mathematical problems used to encrypt data. This makes it theoretically vulnerable to being hacked using dramatic mathematical or computing breakthroughs. By contrast, quantum cryptography near guarantees communications security, using quirks of quantum physics to thwart eavesdropping attempts. Quantum cryptography guarantees security by encoding information as polarized photons which can be sent down a fiber optic cable or through the air. Intercepting these photons disturbs their quantum state, alerting both sides to an eavesdropper's presence.

Category 31.3 *New technology with security implications*

2005-08-01 **car computer systems MP3 Bluetooth protocol risk viruses**

DHS IAIP Daily;
http://www.cnn.com/2005/TECH/08/01/viruses.cars.reut/index.html

CAR COMPUTER SYSTEMS AT RISK TO VIRUSES

Car industry officials and analysts say hackers' growing interest in writing viruses for wireless devices puts auto computer systems at risk of infection. As carmakers adjust on-board computers to allow consumers to transfer information with MP3 players and mobile phones, they also make their vehicles vulnerable to mobile viruses that jump between devices via the Bluetooth technology that connects them. The worst that could happen is that the computer's control of engine performance and emissions, navigation and entertainment systems cease to function. That would probably mean an annoying trip to the repair shop or having to reboot the system. Companies so far have seen no reports of viruses in auto systems, and studies have shown it is not easy to transplant a virus into a car, but carmakers say they are taking the risk seriously. The first mobile phone virus, Cabir, has spread to over 20 countries, ranging from the United States to Japan and from Finland to South Africa, using only Bluetooth. Bluetooth is used in car electronics interfaces for monitoring and service. Carmakers say they use the most sophisticated protection for safety equipment such as airbags or motor controls, whereas infotainment systems so far have less stringent safeguards.

Category 31.3 *New technology with security implications*

2005-08-24 **study federal spending IT increase 2005 third quarters**

EDUPAGE; http://www.fcw.com/article90331-08-24-05-Web

FEDERAL SPENDING ON IT SURGES IN THIRD QUARTER

Market research firm Input reported a surge in U.S. federal spending on information technology in the fiscal third quarter, with the U.S. Navy as the main source of the spike. The Navy generated almost $57 billion of the $67 billion in government awards, a 190 percent increase over fiscal 2004 third quarter data. Federal Computer Week, 24 August 2005

Category 31.3 *New technology with security implications*

2005-09-14 **new technology password cracking keylogger keylogging**

EDUPAGE; http://news.zdnet.com/2100-1009_22-5865318.html

SOUND OF KEYBOARD CLICKS REVEALS WHAT IS TYPED

Researchers at the University of California at Berkeley have demonstrated that an audio recording of someone typing on a computer keyboard can reveal with surprising accuracy exactly what they have typed. Using commercially available recording equipment, the researchers captured audio of typing and analyzed the sounds using an algorithm they developed. Because keys make different sounds, the system is able to make educated guesses about what key was pressed in what order. The application then applies some linguistic logic, including spelling and grammar checks, to refine the results. After three rounds of revisions, the application was able to identify 96 percent of the individual characters typed and 88 percent of the words. The application was effective even with background noise, such as music or cell phones ringing. Doug Tygar, UC Berkeley professor of computer science and information management and a principal investigator of the study, said the project should raise concerns about the security risks of such a technology. "If we were able to figure this out," he said, "it's likely that people with less honorable intentions can--or have--as well." ZDNet, 14 September 2005

Category 31.3 *New technology with security implications*

2005-10-10 **nanotechnology research NSF funding ethical privacy questions security biomedicine**

EDUPAGE; http://chronicle.com/daily/2005/10/2005101005n.htm

NSF FUNDS NANOTECHNOLOGY RESEARCH

Researchers at several universities have received grants from the National Science Foundation (NSF) to study the social implications of nanotechnology. Until now, most funds for nanotechnology projects have supported efforts to develop the technology itself rather than to study its potential effects. Over the next five years, Arizona State University at Tempe and the University of California at Santa Barbara will receive $6.2 million and $5 million, respectively, to study the possible societal side effects of manipulating matter at the atomic level to create new substances and extremely small devices. The University of South Carolina and Harvard University will receive smaller grants to support existing projects. Among the speculative uses of nanotechnology is an idea to create tiny sensors that could reside within a human body and monitor its health. Such sensors would presumably spawn a host of ethical and privacy questions. Moreover, the prospect of creating new types of compounds at the atomic level raises concern about possible risks to the environment. Research at Arizona will focus on security, privacy, and biomedicine; at Santa Barbara, research will address social perceptions of the risk inherent in nanotechnology. Chronicle of Higher Education, 10 October 2005 (sub. req'd)

Category 31.3 *New technology with security implications*

2005-11-16 **MIT $100 laptop production One Laptop per Child OLPC Nicholas Negroponte Tunisia conference**

EDUPAGE; http://chronicle.com/free/2005/11/2005111602t.htm

MIT DEBUTS $100 LAPTOP

At the World Summit on the Information Society in Tunisia, Nicholas Negroponte, director of MIT's Media Lab, will show an early version of a $100 laptop that he announced in January. Negroponte has said that such a device would bring the fruits of technology to millions of schoolchildren in developing nations, spanning the digital divide and spurring economic development. According to those involved with the project, a number of countries have expressed interest, including Brazil, China, Egypt, Nigeria, Thailand, and South Africa, though development remains before orders can be placed. In addition, the governor of Massachusetts has called on his state to provide the new laptops to every middle and high school student. Critics of the program argue that people in developing nations often need more basic supplies, such as food and clean water, and some also note that the educational value of laptops for every student has not been proven. The devices use the Linux operating system and flash memory; they do not include cameras or DVD-ROM drives, as originally planned. They run on C batteries that can be recharged using a hand crank attached to the device. Chronicle of Higher Education, 16 November 2005

Category 31.3 *New technology with security implications*

2005-12-14 **information security new channel alerts AT&T**

DHS IAIP Daily; http://www.networkworld.com/news/2005/121405−att−security.html

AT&T LAUNCHES 24-HOUR SECURITY NEWS SERVICE

AT&T Wednesday, December 14, turned on a 24-hour security news service that streams to customers of the carrier's Internet Protect service. The always-on Webcast includes regular programming that is interrupted by security alerts that AT&T deems important enough to let customers know about right away. "We're building a security geek channel," said AT&T CSO Ed Amoroso during his keynote address at Interop New York, during which he announced the service. Programming includes lectures on technologies, interviews with corporate CIOs as well as twice-daily news updates. The alerts will call attention to worms and viruses and suggest ways to deal with them, Amoroso says. These supplement the existing alerts that AT&T would send along as part of Internet Connect. Amoroso acknowledged that most threats come from inside corporate networks, and he characterized badly written software as the biggest threat to network security, but he said AT&T's service could help deal with threats coming from outside.

Category 31.3 *New technology with security implications*

2005-12-14 **MIT $100 laptop production Quanta Taiwan manufacturer One Laptop per Child OLPC Nicholas Negroponte**

EDUPAGE; http://hardware.silicon.com/desktops/0,39024645,39155040,00.htm

QUANTA TO PRODUCE MIT'S $100 LAPTOPS

Computer maker Quanta has been chosen to manufacture the $100 laptops that are the brainchild of MIT's Nicholas Negroponte and supported by the One Laptop per Child (OLPC) organization. Based in Taiwan, Quanta is the world's largest maker of laptops, building the devices for companies including Dell and HP. Some believe that supplying the developing world with inexpensive computer technology will be a boon for educational and economic development of those nations, and the notion of an inexpensive laptop is part of that vision. Previous attempts to build and deploy similar technology have failed, and detractors argue that the $100 laptop program doesn't stand much of a chance. Nevertheless, recruiting a major hardware manufacturer signals the level of support that the project enjoys. Of the announcement, Negroponte said, "Any previous doubt that a very-low-cost laptop could be made for education in the developing world has just gone away." Silicon.com, 14 December 2005

Category 31.3 *New technology with security implications*

2006-02-06 **machine learning algorithms software self-improving security applications**

DHS IAIP Daily; http://www.computerworld.com/developmenttopics/development/story/0,10801,108320,00.html 23

MACHINE-LEARNING TECHNIQUES TO CREATE SELF-IMPROVING SOFTWARE ARE HITTING THE MAINSTREAM.

Attempts to create self-improving software date to the 1960s. But "machine learning," as it's often called, has remained mostly the province of academic researchers, with only a few niche applications in the commercial world, such as speech recognition and credit card fraud detection. Now, researchers say, better algorithms, more powerful computers and a few clever tricks will move it further into the mainstream. Computer scientist Tom Mitchell, director of the Center for Automated Learning and Discovery at Carnegie Mellon University, says machine learning is useful for the kinds of tasks that humans do easily, but that they have trouble explaining explicitly in software rules. In machine-learning applications, software is "trained" on test cases devised and labeled by humans, scored so it knows what it got right and wrong, and then sent out to solve real-world cases. Mitchell is testing the concept of having two classes of learning algorithms in essence train each other, so that together they can do better than either would alone. Mitchell's experiments have shown that such "co-training" can reduce errors by more than a factor of two. The breakthrough, he says, is software that learns from training cases labeled not by humans, but by other software.

Category 31.3 *New technology with security implications*

2006-04-27 **USB memory stick warning new technology security risk business data leakage theft**

DHS IAIP Daily; http://news.bbc.co.uk/2/hi/technology/4946512.stm 23

WARNINGS OVER USB MEMORY STICKS.

Smart phones, iPods and USB memory sticks are posing a real risk for businesses, warn security experts. Just over half of companies take no steps to secure data held on these devices, found a UK government-backed security survey. Figures from the Information Security Breaches Survey, which is backed by the Department of Trade and Industry, reveals how firms are struggling to control the growing use of USB flash memory sticks. Matt Fisher, spokesperson for Centennial Software, said USB sticks could also become an attack vector for viruses and other malicious programs largely because they are swapped between many different computers. Both the executive summary and the full results of the Information Security Breaches Survey, April 2006, can be found at: http://www.pwc.com/Extweb/pwcpublications.nsf/docid/F9843CD3 C8E0FB828025715A0058C63B

31.4 Outsourcing

Category 31.4 Outsourcing

2003-11-07 **security consumer profiling private personal sensitive information outsourcing**

RISKS; 23 1
http://sfgate.com/article.cgi?file=/c/a/2003/11/07/MNG4Q2SEAM1.DTL

Credit agencies sending our files abroad (via Dave Farber's IP)

David Lazarus writes in the San Francisco Chronicle that, "[T]wo of the three major credit-reporting agencies" are "outsourcing sensitive operations abroad, and a third may follow suit shortly." The information being sent overseas includes Social Security Numbers and full credit histories, so there are fears that identity theft will rise. Credit agencies justify their moves as "necessary cost-cutting". Senator Dianne Feinstein recognizes the threat to US citizens' privacy from this development. She said "she would ensure that the matter was raised as senators and House members completed changes to the Fair Credit Reporting Act." She hopes to protect Americans from "...such outrageous
invasions of privacy."

Category 31.4 Outsourcing

2004-02-09 **privacy database disclosure outsourcing security**

RISKS 23 18

THREE DEGREES OF OUTSOURCING LEADS TO DATA DISCLOSURE

Contributor Ed Ravin writes about a case of disclosure of private information from outsourcing. A programmer ("Dennis") working for a community college posted a full database with confidential information on the Internet in asking for technical help. In a different posting, an anonymous programer warned Dennis about the consequences of posting private informatin. Despite this mild warning, the Dennis posted

---

Category 31.4 Outsourcing

2004-05-10 **outsourcing identity theft risk**

DHS IAIP Daily;
http://www.canada.com/vancouver/vancouversun/news/business/s
tory.html?id=b3d19fb5−4675−4fad−af8d−a118b3cf4fc6

May 10, Canadian Press — Bank of America plans to hire hundreds in India in outsourcing expansion.

Bank of America Corp. may hire 1,500 people at its subsidiary after it opens in southern India this month, 50 percent more than previously disclosed, and the bank has reserved land that would allow for even more expansion. Late last year, the bank said it eventually expected to have 1,000 people at its Continuum Solutions subsidiary in Hyderabad, but wouldn't give specifics about work intended for the center. Executives with the Charlotte, NC-based financial giant said that Continuum employees will initially work with corporate accounts drawn from London operations and later from the bank's offices worldwide. In the future, Indian workers are likely to work with consumer information. The Indian startup is Bank of America's latest step in moving work abroad, part of a cost-cutting trend called offshoring or foreign outsourcing.

Category 31.4 Outsourcing

2004-06-08 **Australia outsource Optus India call center**

NewsScan

OPTUS OPTS FOR INDIAN CALL CENTERS

Optus, an Australian telecom company controlled by the Singapore government, has joined the ranks of other companies using cheap labor in India for some of its call center operations. However, the company's corporate affairs manager has promised Australians: "Optus will always maintain a call center presence in Australia" Optus has about 4000 call center staff in Australia, and it's unclear how many Australian jobs may be affected by the company's new reliance on Indian call center operators. (The Australian 8 Jun 2004) Rec'd from John Lamp, Deakin U.

Category 31.4 *Outsourcing*

2004-06-16 **Microsoft intention offshore outsourcing high-skilled low-cost foreign vendors**

NewsScan

UNION VERSUS MICROSOFT ON OFFSHORING

The Washington Alliance of Technology Workers claims to have identified documents that expose Microsoft's intention to hire low-cost foreign vendors to write its software: "These documents clearly show that as a major software vendor they're looking at the highest skilled, highest trained workers to try to move their work abroad." A Microsoft spokeswoman says the company has long hired outside vendors in India and around the world, but that the company's core technology work will continue to be done in-house: "We're in a cyclical business, so that's part of it. In the work we do,
there are areas of expertise. It makes sense to go to the experts because it's not intellectual property, core technology. We'll continue to do that." The documents in question show that Microsoft paid its U.S. workers $60 an hour for software developers, $72 for senior software developers, and $90 for software architects, whereas for workers in India it paid hourly rates of $23, $31 and $36. (Seattle Times 16 Jun 2004)

Category 31.4 *Outsourcing*

2004-07-14 **outsourcing fear clamor fading management policy cost cutting India computer software**

NewsScan

OUTSOURCING OUTRAGE GOING OUT OF STYLE

The clamor against the outsourcing to India of computer software and back-office services appears to have faded substantially. Infosys chief executive Nandan M. Nilekani says: "The backlash against outsourcing has abated, customer spending is on the rise, and we have redesigned ourselves internally to take advantage of the vast opportunities." According to Sunil Mehta of India's leading software industry trade body: "The debate about outsourcing appears to have moved from an emotional, anecdotal, job-losses plane to a more sober, balanced one about the advantages of globalization of services." Ironically, the anti-outsourcing clamor in the U.S. has actually turned out to be good for the outsourcing business. Partha Iyengar, research director for Gartner explains: "The backlash proved a gold mine of freepublicity for Indian outsourcing companies," and the U.S.-based CEO of iGate Global Solutions (operates in Bangalore, India) says: "The backlash issue made outsourcing so mainstream that even my barber was speaking knowledgeably about outsourcing." (New York Times 14 Jul 2004)

Category 31.4 *Outsourcing*

2005-03-07 **terrorist India outsourcing industry suicide attack disaster recovery plans IBM Intel Texas Instruments Accenture Wipro Infosys**

DHS IAIP Daily;
http://www.infoworld.com/article/05/03/07/HNterroristsindia_ 1.html

TERRORISTS TARGET INDIA'S OUTSOURCING INDUSTRY.

India's software and services outsourcing industry is a likely target for a terrorist group operating in the country, local police warned on Sunday, March 6. But Indian outsourcing and software companies said they are prepared to cope with the threat. Documents seized from three members of the Lashkar-e-Toiba (LeT) terrorist group killed in an encounter with the police on Saturday, March 5, revealed that they planned to carry out suicide attacks on software companies in Bangalore, Karnal Singh, joint commissioner of police in Delhi, told reporters. LeT is demanding independence for the Indian state of Jammu and Kashmir. "The terrorists planned to hit these companies in an effort to hinder the economic development of the country," Singh said. IBM, Intel, Texas Instruments, Accenture, Wipro, and Infosys Technologies are among those with operations in Bangalore. Most of the technology companies in the city have already set up disaster recovery plans and special disaster recovery sites that could be used in the event of a terrorist attack, according to Kiran Karnik, president of the National Association of Software and Service Companies in Delhi.

---

32 Censorship, indecency laws, 1st amendment (law)

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-01-16 **censorship china C**

EDUPAGE

China marginally relaxed its restrictions on Internet access, but it continues to block sites that report news from Hong Kong and Taiwan.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-01-16 **Internet regulation availability**

Reuters

Experts argue that the Internet is unstoppable and that governments will try, but fail, to control its use. Neil Winton, writing for the Reuter news agency, reported in January on his interviews with leading thinkers about government control over cyberspace. Some of the key findings:
* "Governments which seek to restrain the freedom of speech and tax the vast electronic commerce spawned by the Internet will almost certainly be wasting their time, experts say."
* "Dr Bob Glass of the U.S. technology leader Sun Microsystems Inc said any attempt by governments to curtail any of this would be a waste of time. Not even the most powerful computers will be able to effectively patrol the world's telephone lines. Individual computer experts will always be one step ahead."
* Attempts to force Internet users to pass through proxy servers to limit their access to the Net fail when users use the public switched telephone network to access uncontrolled ISPs.
* Even if governments attempt to monitor all telephonic communications through their land lines, low-orbit satellite telephony will defeat their interference.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-01-17 **censorship hate**

Reuters

The German government filed charges against Angela Marquardt, the 25-year-old, blue-and-purple-haired deputy leader of the communist Party of Democratic Socialism, for linking from her Web page to a banned issue magazine called _Radikal_. The issue of _Radikal_ was banned because it included detailed instructions on how to sabotage railway lines. According to the public prosecutor, "It has nothing to do with censorship. Criminally relevant materials are subject to classification by the district attorney or criminal prosecutors." In early June, the court hearing opened and adjourned after an hour so the magistrates could arrange for expert testimony to explain the Net and the Web when the case reconvened toward the end of June. On June 30, the court ruled that maintaining a hyperlink to objectionable material is not tantamount to publication of that material.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-01-19 **censorship NY**

EDUPAGE

New York's recently-passed online-decency law barring computer-based distribution of indecent materials harmful to minors was challenged by the ACLU and 14 other organizations. EDUPAGE summarized their case: >The ACLU argues that New York's law "does not define the relevant 'community' for purposes of determining what is 'patently offensive' in the global medium of cyberspace," nor does it distinguish between what might be harmful to young children and vs. what might be harmful to teenagers. Finally, the lawsuit says the statute violates the Commerce Clause because it attempts to regulate communications that take place outside New York, poses an unreasonable burden on interstate and foreign commerce, and subjects interstate use of the Internet to inconsistent regulations. (BNA Daily Report for Executives 15 Jan 97 A13)<

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-01-21 **CDA censorship law**

UPI

US Department of Justice prepared to support the Communications Decency Act by claiming that because families and children use the Internet, therefore the CDA is not an infringement of the First Amendment to the US Constitution (guaranteeing free speech).

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-01-25 **Net censorship**

Reuters

The United Arab Emirate's government-controlled ISP has set up a proxy server to censor the Net. The country's 9,669 Etisalat users are required by law to configure their Web browsers to use the official proxy server that filters out offensive materials.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-02-02 **infowar censorship culture**

EDUPAGE

EDUPAGE reported: >An editorial in the Iraqi government newspaper Al-Jumhuriya says that the Internet — which is not accessible in Iraq — is "the end of civilizations, cultures, interests, and ethics," and "one of the American means to enter every house in the world. They want to become the only source for controlling human beings in the new electronic village." (AP 17 Feb 97)<

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-02-03 **Law**

RISKS 18 81

A Maryland bill that would make it illegal to send "annoying" or "embarrassing" e-mail was introduced in early February by Democratic General Assembly member Samuel Rosenberg. Critics describe the proposed legislation as using impossibly vague terms and being unconstitutional.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-02-04 **censorship culture**

EDUPAGE

Not everyone supports calls for freedom of speech and absence of government controls on the Net. At the World Economic Forum in Switzerland, representatives from such countries as Iran called the pressure for unfettered communications an ideology and explicitly rejected liberalism.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-02-19 **censorship racism**

PA News

The British government announced that it may introduce legislation to interfere with neo-Nazi use of the Internet.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-03-12 **censorship Vietnam C**

RISKS 18 89

Vietnam joined the growing roster of authoritarian regimes scared into needing laxatives by the prospect of allowing their citizens to read whatever they want.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-03-25 **Sweden free speech internet**

RISKS 18 94

A new law proposed in Sweden would guarantee free speech rights to people publishing non-modifiable texts on the Internet provided that a named person be the "responsible editor" who would have legal responsibility for the texts being posted.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-04-17 **censorship porn libraries filter**

EDUPAGE

The ACLU threatened to launch court actions against the Ohio Public Library Information Network because state librarians decided to install Net filters to stop kids from surfing through pornographic and other undesirable sites. Undesirable by others than the children, that is. The fuss began when six boys in a county library were discovered to be gawking at pornographic pictures from the Internet. A month after the ACLU's intervention, a parents' group, Citizens for the Protection of Children, vigorously supported the proposed filters.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-04-17 **porn**

EDUPAGE, Reuters

The Bavarian state prosecutor's office laid criminal charges in April against Felix Somm, head of CompuServe Germany. The indictment cites the online availability of "images of child pornography, violent sex and sex with animals" through CompuServe's making the USENET available to its users. CompuServe vowed to support its employee in the case. An interesting development occurred in June, when the federal parliament began consideration of the Information and Communications Services Law, which would exempt carriers and ISPs from prosecution for the content of their traffic.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-05-11 **censorship**

EDUPAGE

In Virginia, state employees such as professors at state-funded universities and colleges are forbidden to view sexually explicit online materials. Six Virginia university professors and the ACLU filed a challenge to the legislation, which interferes with online access to materials that are available on paper without question. Currently, it is ""a crime for state employees using state-owned computers to `access, download, print or store any information . . . having sexually explicit content."" The law also seems to apply to non-pornographic but sexually-explicit information such as the classic English poetry of Swinburne or the historically important works of Sigmund Freud. The federal lawsuit demands that this state law be overturned. The plaintiffs say this is insulting and a breach of academic freedom.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-05-20 **censorship slander law ISP CDA**

Wired via PointCast

Two self-described worshippers of Satan launched a lawsuit against ElectriCiti Inc., a San Diego ISP, for failing to shut down one of their persistent anonymous public critics. The ISP's lawyers countered that the short-lived Communications Decency Act precluded suing ISPs for the content of messages posted on the Net. In addition, the defendants claimed that the lawsuit by Michael and Lilith Aquino is a "SLAPP" — "strategic lawsuit against public participation" and should be dismissed out of hand.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-06-14 **Internet pornography ISP law**

AP

In a Federal Circuit court in Florida, Judge James Carlisle ruled in June that AOL is not liable for the content of cyberchat. The case concerned a civil lawsuit by the parents of a 14-year-old boy who was raped by Richard Lee Russell in 1994 after the two met in an AOL chat room. The parents said they would appeal the ruling.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-06-17 **censorship CDA**

EDUPAGE

The White House backpedaled on its support for the notorious Communications Decency Act, apparently anticipating the Supreme Court's rejection of this law's constitutionality. Observers chuckled over the abrupt reversal from the Department of Justice's position in March, when the administration vigorously asserted the value of this law.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-06-21 **Internet law pornography pseudonyms**

AP

In a case brought by the ACLU, U.S. District Judge Loretta Preska issed a temporary injunction in June preventing prosecutions under New York State's new law making it a criminal offense for pedophiles to use the Net to entrap children. The Judge wrote, "The protection of children from pedophilia is an entirely valid and laudable goal of state legislation. The New York act's attempts to effectuate that goal, however, fall afoul of the (federal) Commerce Clause." In a similar case in Georgia, Senior U.S. District Judge Marvin Shoob of the Atlanta federal court ruled that the Georgia law making it illegal to use pseudonyms on the Net was subject to challenge by the ACLU and others and suspended enforcement pending resolution of the lawsuit.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-06-22 **censorship law CDA New York Georgia NY GA**

EDUPAGE

In New York, a judge voided that state's version of the Communications Decency Act without waiting for the Supreme Court of the United States; the law was invalid, said the judge, because it attempted to regulate interstate activities in violation of the US Constitution. In Georgia, a federal judge imposed a preliminary injunction against enforcement of a state law making it illegal to use pseudonyms on e-mail.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-06-25 **censorship law China ISP C**

RISKS 19 23

China passed even more draconian laws restricting access to the Internet by its citizens. The regulations force all Net access to go through the government's proxy servers to permit extensive censorship.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-06-26 **CDA censorship law**

RISKS, AP 19 23

In a stinging rebuke to censorship buffs in the US, the Supreme Court issued its ruling on the Communications Decency Act, finding that it violated First Amendment protection of free speech. The unanimous opinion stated that the effort to protect children from sexually explicit material goes too far because it also would keep such material from adults who have a right to see it. Justice John Paul Stevens wrote for the court, "The (Communications Decency Act) is a content-based regulation of speech. The vagueness of such a regulation raises special First Amendment concerns because of its obvious chilling effect on free speech. . . . As a matter of constitutional tradition . . . we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it."

See <http://www.cdt.org> or <http://www.epic.org> for the full text of the ruling, which was noteworthy for the clarity of its prose and spirited defense of free speech on the Net.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-06-29 **censorship law international Europe CDA**

EDUPAGE

In the wake of the CDA decision by the Supreme Court of the U.S., European Internet experts warned that no country should try to "change the Internet we know and love into a kindergarten." Regulating the Internet would in any case require extensive international cooperation because of the international nature of the Net.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-07-01 **Internet filtering SCOTUS libraries freedom of speech**

American Library Association

The American Library Association's Intellectual Freedom Committee issued a statement on the problems faced by libraries in using Internet-filtering software. The report pointed to the Supreme Court ruling of 1997.06.29 on the Communications Decency Act affirming the protected status of speech on the Internet. In addition, said the ALA statement's authors, libraries must serve a wide range of users; filtering software is generally designed for families or corporations where centralized controls can successfully be dictated for children or employees. Filtering software imposes unreasonable restrictions on everyone to protect a minority of users; "can impose the producer's viewpoint on the community;" does not "generally reveal what is being blocked, or provide methods for users to reach sites that were inadvertently blocked;" and use "vaguely defined and subjectively applied" criteria for blocking sites.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-07-06 **censorship Internet Germany**

EDUPAGE

The German federal legislature passed a law to prosecute Internet Service Providers that make illegal materials available on-line; e.g., child pornography or Nazi publications. Commentators scoffed that the law was too vague for enforcement and could not be made to apply to international networks. In other developments, government representatives from Canada, Europe, Japan, Russia and the U.S. met in Bonn with officials from ISPs to sort out the issue of regulation and prevent hobbling the new mode of communication.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-07-16 **Net filters censorship**

RISKS 19 24

Another farcical situation was revealed when three counties in New Jersey discovered that their sites are blocked by the notorious AOL "Scunthorpe" filter. All the sites included the three letters "sex" in their names.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-07-16 **pornography law Australia police filtering censorship**

Newsbytes

The Australian government proposed new laws under the Broadcasting Services Act to make ISPs liable for criminal breaches of the regulations of the Office of Film and Literature Classification and other laws. The Australian Industry Association hailed the proposals as "a sensible balance between community concerns over Internet content and business concerns on over-regulation." Communications Minister Richard Alston stated that the government realizes that it cannot regulate the global Internet, but said the government will help control access by minors so that parents and guardians can prevent abuse.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-08-24 **censorship advertising Net Web law**

EDUPAGE

According to the Investor's Business Daily, the recent deal between tobacco companies and many states would prohibit tobacco advertising on the Internet. Commentators worry that this precedent could cripple online speech from international companies by enforcing the most restrictive laws found anywhere around the world.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-08-26 **cellular phones censorship repression Yemen infowar**

Reuters

The Yemeni government suspended cellular phone services to 9,000 residents because of security concerns. The authoritarian government has been fighting a resurgance of terrorism in the country and unfettered communication is clearly seen as a threat to its power.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-09-05 **Internet censorship government law**

AAP

Communications Minister Richard Alston announced that the Australian Broadcasting Authority would begin discussions with ISPs to establish new codes of practice to prevent distribution of offensive materials through the Internet.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-09-10 **Internet censorship government regulation law content**

Newsbytes

The Office of the Ontario Attorney General suggested that it might make ISPs legally responsible for content made available to Canadians through their facilities. Canada has much stricter regulations on hate-speech, for example, than the US, and such regulations are theoretically possible but difficult to impose in practice because of the international nature of the Internet.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-09-29 **censorship government law**

AP

In the United Arab Emirates, hackers are more interested in evading clumsy government attempts to limit access to the Internet than in invading other people's computer systems. Savvy users have been sidestepping government restrictions to access pornography and — even worse — to talk to Israelis. In Saudi Arabia, fear of the Net has prevented any local ISP from being set up, but rich users simply place international long-distance calls to external ISPs.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-10-06 **child pornography rape law**

AP

The Pennsylvania legislature unanimously passed a law criminalizing the use of the Internet to lure children or teens into sex acts.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-10-09 **child pornography rape censorship law**

New York Times (Cybertimes)

New York Penal Law 235.22 criminalizes the distribution of indecent material online to minors that is for the specific purpose of inducing them to engage in sexual acts. This law, to take effect 1 Nov 96, has gained the support of free speech advocates and opponents of child pornography alike. It was successfully upheld in the case of People v. Barrows, Justice Alan Marrus of the New York State Supreme Court presiding. He ruled for the first time to uphold an indictment under the luring statute. The case involved a 56-year-old man who is alleged to have tried to lure a 13-year old virtual girl into a meeting — and arrived equipped with a rope, lubricants and paper towels. He was arrested by a female police officer posing as the child. His attorney protested the grand jury indictment on free speech grounds but lost because, ruled the judge, the element of luring overshadowed speech issues.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-10-14 **censorship Web site**

Globe & Mail, EDUPAGE

In October, the Canadian Human Rights Tribunal began an interesting hearing into the possibility of limiting the publication of the writings of notorious Holocaust-denier Ernst Zundel on a Web page physically located in California. EFF Canada President, David Jones of McMaster University warned that the law in question was written to handle hate-messages on phone-answering machines and suggests that extending it to deal with the Internet ought to be subject to wide public debate. In an editorial, the Globe & Mail came down, as usual, strongly in favor of free speech. Marginal and delusional cases like Zundel don't deserve the publicity they garner through legal prosecution.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-10-23 **library Internet filtering censorship free speech**

UPI

Members of the Library Board in Loudon County, VA voted 6-2 in July 1997 to install filtering software on their Internet terminals and to ask adults to request inactivation of the filters when desired. Children aged 16 and younger will have unfettered access to the Internet from Library terminals only when their parents are with them. In October 1997 they voted 5-4 to extend the filtering to adult patrons despite indications from the American Civil Liberties Union that the filtering, when applied to adults, clearly violates First Amendment rights. In February 1998 the ACLU and seven other plaintiffs filed suit on First-Amendment grounds. EDUPAGE noted, "The X-Stop software, which is intended to screen out obscene material or sexually explicit language, is blocking sites that include some mainstream newspapers, a Methodist church, a university women's association, and a safe-sex page for teenagers."

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1997-11-07 **extortion publication Web Internet censorship**

The Guardian (London)

The power of national governments and legal systems to control publication of what they don't like is being eroded by access to the World Wide Web and the rest of the Internet. Ian Katz of _The Guardian_ wrote that Richard Tomlinson, a former M16 agent charged in November with breaking the Official Secrets Act, had allegedly placed a manuscript of his revealing memoirs on the Internet. Unless they computers received a signal from him once a week the book would be automatically published on the Internet. In another case of opposition to legal constraints, McDonald's Corporation has proved powerless to prevent availability of critical comments about its food and employment practices on the McSpotlight sites, run by volunteers in 22 countries.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1998-01-08 **censorship government Internet filter proxy**

EDUPAGE

CHINA IMPOSES NEW CONTROLS ON INTERNET ACCESS

New rules against "defaming government agencies," spreading pornography and violence, and revealing state secrets have been imposed by the Chinese government. The rules, which are said particularly to target Internet users, call for criminal punishment and fines of up to $1,800 for Internet providers and users who are found to have spread "harmful" information or leak state secrets via the Internet. In announcing the rules, China's assistant minister for public security noted that Internet links had increased China's cultural and scientific exchanges around the world, but that "the connection has also brought about some security problems, including manufacturing and publicizing harmful information, as well as leaking state secrets." (Chronicle of Higher Education 9 Jan 98)

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1998-01-18 **censorship free speech student high school academic hacker**

RISKS 19 56

Greenfield High School (Milwaukee, WI) expelled senior Justin Boucher for writing an article entitled, "So you want to be a hacker" in an underground student newspaper.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1998-02-19 **censorship schools library ISPs law states pornography**

EDUPAGE

The ACLU complained that state legislatures are ignoring the U.S. Supreme Court's ruling on the unconstitutionality of the Communications Decency Act. According to EDUPAGE editors John Gehl and Suzanne Douglas, "New laws are being considered by Tennessee, Rhode Island, Illinois and New Mexico. The Tennessee law, which is the most sweeping, would create a special domain code for adult-oriented sites; require schools and libraries to use filtering software, with criminal liability for teachers and librarians who fail to comply; and make Internet service providers liable for distribution by their customers of harmful material."

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1998-05-07 **censorship Internet monitoring filtering government**

RISKS 19 72

The government of the Ukraine issued a presidential edict requiring monitoring all inbound and outbound TCP/IP traffic for all Ukrainian Internet users. [Sales and piracy of cryptographic software should shoot up in Ukraine, followed soon by attempts to outlaw strong cryptography.]

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1998-05-28 **censorship ISP privacy pornography laws Germany decency**

EDUPAGE, RISKS

In April 1997, Bavarian state prosecutors charged Felix Somm, head of CompuServe Germany, with tolerating child pornography and other indecent materials to be accessed — from the World Wide Web and other parts of the Internet — through the CompuServe ISP. The prosecutors eventually reversed themselves and actually petitioned the Munich district court to acquit Somm. Nevertheless, the court condemned Somm, by now the ex-head of CompuServe Germany, to two years probation. Supporters of civil liberties around the world protested the verdict.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1998-06-14 **child pornography pedophiles Internet Web law**

EDUPAGE

The House of Representatives sent the Senate a unanimously-approved bill making it a felony to transmit obscene materials to a minor via the Internet. Other prohibited activities include contacting a minor for sexual purposes and engaging in sexual activity with a minor using a computer. Sentences start at three years in prison.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1998-06-28 **children pornography indecency bills filtering censorship**

EDUPAGE

Two bills began moving through the US chambers in June to impose filtering software on Internet access points so that children could not see pornography. Rep. E. Istook (R-OK)'s bill would apply to public schools and libraries; Sen.J. McCain (R-AZ) would apply only to federally-assisted institutions. The ACLU is fighting both bills. The McCain measure passed in July, as did a bill sponsored by Sen. D. Coats (R-IN) that severely penalizes (fines of up to $50,000) Web site operators that make pornography available to minors.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1998-07-28 **privacy ISPs subscriber Web libel tort**

EDUPAGE

Privacy advocates expressed concern over the trend for ISPs to yield to court orders demanding they divulge the identity of their subscribers. The problem is not the ISPs compliance with lawful orders, say the activists. The danger, says one activist, is that "It's an attempt to chill speech. They're hoping people will self-censor out of fear."

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1998-07-29 **China repression censorship punishment Internet law legal**

INDEPENDENT ON SUNDAY

Lin Hai, a 30-year-old software developer, was thrown in jail by Chinese authorities on March 25 for having sent 30,000 Chinese e-mail addresses to a U.S. organization that publishes Da Can Kao, or Big Reference, a Chinese-language pro-democracy Internet magazine. Mr Lin was charged with thereby inciting the overthrow of the state but the official prosecutor threw the case out of court in September, insisting on further investigations (Mr Lin remained in jail). The prosecutors further delayed the trial in November but decided to hold it in secret.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1998-09-27 **censorship online pornography children minors adult identity**

EDUPAGE

The US House Commerce Committee unanimously approved the Child Online Protection Act, which among other things requires commercial Web sites to demand some form of adult identification such as a credit card number.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1998-09-27 **censorship filtering library public institution pornography**

EDUPAGE

The long-running dispute over Loudoun County Library's decision to install Net-filters on their Internet access points reached a judge in late September.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1998-10-04 **library censsorhip filtering feminist hostile work**

EDUPAGE

The National Organization of Women filed an amicus curiae brief in defense of net filtering in public libraries. The organization argued that "explicitly or constructively forcing librarians to deal with displays of pornography could result in the development of a hostile or abusive workplace." The ACLU disagreed, claiming that "libraries have always had adequate policies for addressing misbehavior by patrons, and that the use of filtering to censor cyberspace is not the way to protect librarians."

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1999-01-01 **children parents pornography Internet Web monitoring warning**

PA News

Peter Luff of the Conservative Party of Great Britain proposed a bill obliging computers to be sold with warning labels. Noxious emissions? Danger of shock? In a way: he wanted to be sure that parents were aware of the ease with which their children would be able to access pornography on the Net.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1999-01-29 **censorship Internet chat government fear persecution freedom**

AP, Washington Post

In yet another demonstration of the potential power of the Net, the Chinese dictatorship set up a 24-hour monitoring group to catch anyone making anti-government remarks. [Anything contradicting the Party line is defined as anti-government in China.]

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1999-01-30 **child pornography digital editing law judgement court case**

AP, Washington Post

In Maine, a federal appeals court denied a defense against a child pornography conviction that was based on digital modification of innocent pictures of kids.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1999-02-11 **pornography First Amendment censorship university professors**

Washington Post

Six professors at Virginia universities protested the state law forbidding state employees from using employer-supplied computers to download pornography. They argued in court that their work on human sexuality and on sexually-explicit poetry was being hampered. The U.S. federal 4th Circuit Court of Appeals rejected their petition.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1999-02-14 **censorship China law repression Internet Web police ISP**

Australian AP

China's dictators established a taskforce in February to monitor Internet usage and to interfere with human-rights and pro-democracy groups' ability to use the network for anti-government activity. The ostensible reason for the draconian crackdown was the protection of state secrets; however, as Owen Brown of the Australian Associated Press reported, "in China even tomorrow's weather forecast is considered a national secret until its publication and release to the tightly controlled state-run media is approved by the relevant government authority."

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1999-02-15 **Internet Web free speech censorship incitement violence law**

TIME Magazine

In Portland, OR in February, a jury handed down a $107M penalty against the anti-abortionists who, the plaintiffs argued, incited violence against purveyors of abortions. The "Nuremberg Files" Web site, complete with dripping-blood images, presented personal details about reproductive-center workers, including home address, the particular way they traveled to work, and even the names of their children. When "baby butchers" on the list were wounded, their names were changed to gray; when they were killed, their names were boldly crossed out.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1999-02-19 **child pornography Web Internet crime vigilante volunteer**

AsiaWeek

Toko's Metropolitan Police asked the Japanese chapter of the Guardian Angels to monitor the Japanese Internet for child pornography and other criminal activity.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1999-03-19 **pornography censorship government regulation ISPs Web**

Reuters

An Australian government bill would ban pornography and other objectionable materials on Web sites physically located in Australia and would also impose requirements on Australian ISPs to filter such materials. The international Internet Industry Association protested that such restrictions would be impracticable and argued for self-regulation and better tools parental supervision of Internet use by children.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1999-04-08 **information warfare hacking tools censorship culture subvert**

BORNEO BULLETIN

An article in the Borneo Bulletin reported on the growth of hacking in Brunei, where "officials, armed with red and black marker pens, painstakingly black out thousands of copies of undesirable pictures everyday, while undesirable computer software continue to flood the market."

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1999-04-19 **free speech censorship Communications Decency Act lawsuit**

TechWeb, Reuters

In April, the SCOTUS upheld the part of the Communications Decency Act of 1996 which outlaws "the sending of any comment or image which is obscene, lewd, lascivious, filthy, or indecent, with intent to annoy, abuse, threaten or harass another person." This decision greatly offended the operators of <annoy.com>, a Web site that encourages anonymous e-mail to public officials. Lawyers for ApolloMedia argued unsuccessfully that some valid protected speech may offend some people but that constitutional rights to free speech should nonetheless apply.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1999-04-20 **library free speech censorship censorware evidence**

New York Times

David Butt, Librarian in Lake Oswego, OR launched a Freedom-of-Information campaign to collect factual information from libraries throughout the USA about the frequency of complaints about inappropriate use of library Internet-access computers. Butt, supported by the Center for Law and Policy at the American Family Association, a Christian group that backs censorship in Internet terminals in public libraries, is opposed to the position of the mainstream American Library Association, which argues that the problem is minor and that filtering software is inappropriate for institutions devoted to the dissemination of knowledge.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1999-04-23 **censorship legislation bill proposal**

http://www.it.fairfax.com.au/breaking/924857680.html

The Internet Industry Association of Australia rejected its government's proposals for Internet censorship. The Minister for Communications, Information Technology and the Arts had described legislation to force ISPs to conform to government instructions on blocking access to specific sites on the Web. ISPs protested that there are no foolproof steps to block such access and that the demand placed unreasonable demands on the entire industry.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1999-05-11 **censorship Internet Web content rating classification porn**

AAP

In Australia, a Senate committee approved The Broadcasting Services Amendment (Online Services) Bill 1999, which would extend the existing system of film classification to the Internet, outlawing RC and X rated material and making R material available only to people over 18 years. The bill remained to be approved by the entire Senate.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1999-05-17 **Canada Internet Web regulation content censorship law rules**

Wired

The Canadian Radio-television and Telecommunications Commission (CRTC) announced in May that it would not try to enforce requirements for Canadian content on the Net, arguing that most of the material is textual and therefore not covered by the Broadcast Act.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1999-06-17 **bill proposal law filtering obscenity child pornography library school constitution free speech censorware**

C|Net

In June, the House of Representatives passed an amendment to the Juvenile Justice Bill (Bob Franks, R-NJ & Chip Pickering, R-MS) that would require schools and libraries receiving federal subsidies to impose filters on Net access to keep kids from viewing harmful materials.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1999-09-01 **government censorship law COPA Child Online Protection Act**

Wired via PointCast; EDUPAGE

The ACLU and other lobbyists for freedom of speech on the Net won an injunction against the Child Online Protection Act (COPA) passed in the closing days of 1998. US District Judge Lowell A. Reed Jr. ruled on 1 Feb 1999 that the law was too broad and must not be enforced. He also wrote in his memorandum that he considered the Act an unconstitutional violation of First Amendment rights of free speech: "Despite the Court's personal regret that this preliminary injunction will delay once again the careful protection of our children, I without hesitation acknowledge the duty imposed on the Court and the great good such duty serves. Indeed, perhaps we do the minors of this country harm if First Amendment protections, which they will with age inherit fully, are chipped away in the name of their protection." In September, COPA opponents including publishers, Internet
companies, and trade associations filed an amicus brief in the Third Circuit Court of Appeals supporting the view that COPA was unconstitutional.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1999-10-27 **pornography censorship filtering academic universities state employees sexual content college ACLU**

Washington Post

Half a dozen die-hard civil libertarians challenged the State of Virginia once again over its ban on state employees' accessing sexually-oriented materials from the Internet on computers in their places of work. The six professors, supported by the ACLU, argued that this law (ruled unconstitutional in early 1998 but reinstated in early 1999) violates the First Amendment. The State argues that because there is an exception for research approved by a professor's dean, the law is permissible.

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1999-10-29 **Internet Web broadcasting authority government regulation control censorship pornography harm filtering**

Australian Broadcasting Authority
http://www.aba.gov.au/about/public_relations/newrel_99/101nr99.htm

The Deputy Chairman of the Australian Broadcasting Authority delivered a stirring call to government action on Internet regulation in the 1999 Spry Memorial Lecture in Vancouver, Canada. He called for national governments to exercise strict controls on Internet just as they control the airwaves for broadcasting. Oddly, he described the Net as "a means of mass communication of a particularly intrusive nature." He warned, "They [i.e., broadcast media and the Internet] enter our homes and workplaces, [and] exercise important influences on public life and national cultures. Their content has been and remains. . . of considerable concern to the public who wish to see national cultures preserved and enriched and to see young people protected from inappropriate material." He added later in his speech, "Whereas in the United States the US Constitution First Amendment allows the free speech lobby to dominate discussion about self-regulation, other countries with healthy democratic systems and vibrant processes of open expression are able to seek a more appropriate balance between the right to free expression and the right of communities to nurture national and local cultures and to protect children from harmful content."

Category 32 *Censorship, indecency laws, 1st amendment (law)*

1999-11-30 **censorship FBI police intimidation fraud lies**

http://www.freedomforum.org/speech/1999/11/29closing.asp

In mid-November, the president of an ISP in Michigan, BECamation, removed a satirical video from a user's Web site after FBI agents allegedly intimidated him by threatening legal action if he failed to act. In fact, the agents had no legal basis whatsoever for their demands. The video by New York artist Mike Zieper pretended to show an FBI training film discussing possible violence in Times Square because of putative Y2K problems. The FBI denied that any intimidation was involved.

32.1 Censorship in the USA

Category 32.1 Censorship in the USA

2000-01-26 **pornography filtering censorship university free speech law**

Edupage, Wired

Republican Representative Jean McGrath (AZ) introduced new proposals for interfering with the viewing of pornography at state universities by restricting Internet access to "educational purposes" and by forcing universities to install censorware. Free-speech advocates and First-Amendment legal specialists protested that such legislation would be unconstitutional in the US.

Category 32.1 Censorship in the USA

2000-02-23 **filtering software censorship Internet library public filter shield**

AP

Voters in the Republican primary in Michigan on 2000-02-23 voted 4,379 to 3,626 against forcing the local public library to install censorware on their free public-access Internet terminals. The battle began when a child typed in "chocolate chip cookies" and the search returned pornographic pictures. Advocates of the filtering software were outraged that pornography was so easily accessible in a public institution; opponents said that filters are only 85% effective whereas the current strict policies of supervision ensure 99.9% compliance with the rules precluding visits to inappropriate sites. Library board members said they would rather shut down the library than install filters. Proponents of filtering worked closely with evangelical Christian organizations such as the Mississippi-based American Family Association, which contributed $35,000 to the campaign.

Category 32.1 Censorship in the USA

2000-02-23 **content filtering law library censorship**

NewsScan, San Jose Mercury News

The city of Holland, a conservative 30,000-population town in the western part of Michigan, has defeated (with about a 55% margin) a proposal that would require the local public library to install filtering software on library computers so that children would be unable to access pornographic, violent, and hate sites on the Web. Apparently Holland is the first city to put this issue on the ballot, though it's been debated in many other places. One supporter of the defeated proposal said: "I just think that children really don't know what's for their own good. It may not be a really big problem at the library right now or in the future, but why take a chance?" An opponent of software filtering explained its defeat by saying: "I think free speech brought out a number of voters." (AP/San Jose Mercury News 23 Feb 2000)

Category 32.1 Censorship in the USA

2000-06-23 **children pornography free speech court case lawsuit judgement injunction COPA**

NewsScan, New York Times
http://partners.nytimes.com/library/tech/00/06/biztech/articles/23privacy.html

A federal appellate court . . . upheld a lower court injunction against enforcement of the 1998 Child Online Protection Act, a law intended to protect children from commercial Web sites trafficking in pornography. The three-judge panel ruled that the law, which required such sites to forbid access to Internet users who could not provide proof of their age, fell far short of meeting First Amendment standards of free speech. Though praising the efforts of Congress to protect children, the judges rejected the law's reliance on "community standards" to define pornography and asserted that it is impossible to simultaneously meet the moral standards of communities such as Chicago, Amsterdam, and Tehran. (New York Times 23 Jun 2000)

Category 32.1 Censorship in the USA

2000-08-09 **free speech censorship law judgement lawsuit ruling constitution**

NewsScan, San Jose Mercury News
http://www.sjmercury.com/svtech/news/breaking/ap/docs/293190l.htm

U.S. District Judge J. Harry Michael Jr. . . . declared unconstitutional a Virginia law making it a crime to use the Internet to send children sexually explicit images or other materials that could harm them. The judge agreed with the civil liberties groups and Internet companies that had challenged the law as abridgment of the First Amendment right to free speech, on the grounds that there is no practical way to prevent children from accessing such material without also denying it to adults. (AP/San Jose Mercury News 9 Aug 2000)

Category 32.1 *Censorship in the USA*

2000-09-11 **survey study government infrastructure protection vulnerabilities weaknesses**

NewsScan, Los Angeles Times
http://www.latimes.com/business/20000911/t000085464.html

A . . . study released [in September] by the General Accounting Office has exposed widespread deficiencies in computer security in government agencies ranging from the Department of Interior to the U.S. Treasury. The report comes nine months after the President Clinton called on federal agencies to beef up security in his "National Plan for Information System Protection." That plan proposed that Congress boost federal spending for computer security and research by $280 million to $2.3 billion in 2001, but agencies say they need the money now. Government computer managers point to the tight labor market for computer security experts and say it's difficult to retain good personnel. The GAO report found that some agencies have failed to take even the most rudimentary steps to increase security, such as encrypting password files and limiting physical access to sensitive computers. In addition, agencies have been less than diligent about blocking access for independent contractors and former employees after they've left the government. In one agency, 7,500 of 30,000 users were not deleted after 160 days of inactivity. "The federal government, outside the defense area, is worse than the private industry because good computer security is about regular maintenance and housekeeping — and that's not one of the government's strong points," says Stewart Baker, a Washington, D.C. technology lawyer. (Los Angeles Times 11 Sep 2000)

Category 32.1 *Censorship in the USA*

2000-10-30 **censorship filtering censorware pornography violence lawmakers legislation school children**

NewsScan, New York Times
http://www.nytimes.com/2000/10/20/technology/20NET.html

Although a commission appointed by Congress has decided that parental involvement rather than software filtering is the right way to shield children from pornography on the Internet, senators John McCain and Rick Santorum and congressman Ernest Istook are introducing legislation to require schools and libraries to install software to protect children from encountering pornography and violence as they use the Web. Presidential candidates Al Gore and George W. Bush are both in favor of such filters. (New York Times 20 Oct 2000)

Category 32.1 *Censorship in the USA*

2001-01-23 **child pornography computer-generated images law jurisprudence**

NewsScan

SUPREME COURT TO HEAR CASE ON COMPUTER-GENERATED CHILD PORN
The U.S. Supreme Court has agreed to hear a case that challenges the 1996 federal "Child Pornography Prevention Act," which makes engaging in child pornography a crime even when the images depicting minors engaging in sexually explicit acts are generated entirely by computer, without the participation of real children. A lower court overturned the law, ruling that it "criminalizes the use of fictional images that involve no human being" and are "entirely the product of the mind." However, both Congress and the U.S. Justice Department have taken the position that the law protects real children by reining in a pornography industry that desensitizes viewers and thus puts children at risk of exploitation. (New York Times 23 Jan 2001)
http://partners.nytimes.com/2001/01/23/national/23SCOT.html

COURT TO REVIEW "VIRTUAL PORNOGRAPHY" CASE [29 Oct 2001]
Tomorrow the U.S. Supreme Court will begin reviewing arguments in a case about "virtual" pornography, and will be required to answer the question whether child pornography is child pornography even when the "minors" shown engaging in sex are not real children but rather computer-generated images that only appear to be children. The Free Speech Coalition, backed by the American Civil Liberties Union, considers the case a "no-brainer," and FSC lawyer Louis Sirkin insists that "when "you don't have a child, you don't have a crime. It'd be like charging someone for murder by turning on a computer and making something that looked like murder." The government, however, maintains that the law restricting virtual child pornography is needed to protect real children from pedophiles and others seeking to harm them. Robert Flores, an attorney in favor the law, says: "If the Supreme Court does not uphold the statute, it will negatively impact on all child pornography investigations. It's just not the case that the First Amendment protects all fantasy." (San Jose Mercury News 29 Oct 2001)
http://www.siliconvalley.com/docs/news/svfront/pornlw102901.htm

COURT HEARS ARGUMENTS ON "VIRTUAL" CHILD PORNOGRAPHY [31 Oct 2001]
The U.S. Supreme Court heard arguments yesterday to decide whether "virtual" child pornography could be outlawed because it "conveys the impression" that it depicts real children engaged in sex acts, even though the images of sex acts are created entirely through computer video graphics. Government lawyers took the position that virtual child pornography was as effective as actual child pornographer in putting children at danger from predators. Lawyers defending computer-generated pornographer as an exercise of Constitution-protected free speech said the Child Pornography Prevention Act would have "radical and tragic consequences," in that "visual messages of adolescent sexuality will be barred regardless of their artistic or scientific merit." Justice Scalia asked: "What great works of art would be taken away from us if we couldn't see minors copulating?" When the attorney offered the movie "Lolita" as an example, Scalia said, "With all due respect, this is not the Mona Lisa or the Venus de Milo." (New York Times 31 Oct 2001)
http://partners.nytimes.com/2001/10/31/national/31SCOT.html

Category 32.1 *Censorship in the USA*

2001-01-26 **legislation censorship video game violence children**

NewsScan

SENATORS CRITICAL OF VIDEOGAME VIOLENCE
U.S. Senators Joseph Lieberman, Herb Kohl, and Sam Brownback plan to introduce legislation that will punish companies that market excessively violent video games to children. Kohl, a Wisconsin Democrat, said: "Practically everybody in the industry still markets inappropriate games to kids, practically every retailer regularly sells these games to kids, and practically all parents need to know more about the rating system." But Doug Lowenstein, president of the Interactive Digital Software Association, which represents video game makers, argues that such legislation could violate the First Amendment guarantees of freedom of speech and might simply make it more complicated for the video game industry to police itself. (AP/USA Today 25 Jan 2001)
http://www.usatoday.com/life/cyber/tech/review/games/2001-01-25-violence.htm

---

Category 32.1 *Censorship in the USA*

2001-03-13 **censorship censorware filtering library lawsuit CIPA**

NewsScan

NEW EFFORT TO END INTERNET FILTERING PROGRAM IN LIBRARIES
The American Civil Liberties, the American Library Association, and other plaintiffs are filing federal lawsuits this [week] to overturn a new law called the Children's Internet Protection Act, which requires schools and libraries receiving federal money for technology to shield school children from pornography and violence transmitted over the Internet. The dispute splits political parties. One Republican, Ernest Istook of Oklahoma, says that civil libertarians falsely label the law censorship "if they're not permitted to expose our children to the very worst things on the Internet, using federal tax dollars to do so," whereas Republican Jeffrey Pollock (whose own political site was once blocked by filtering software) says: "To mandate the federal government to legislate morality, I find abhorrent." (New York Times 19 Mar 2001)
http://partners.nytimes.com/2001/03/19/technology/19FILT.html

---

Category 32.1 *Censorship in the USA*

2001-03-19 **censorship library lawsuit law CIPA filtering**

NewsScan

LIBRARIANS SUE OVER NET CENSORSHIP
The American Library Association says it plans to sue the U.S. over the legality of the Children's Internet Protection Act, which was signed into law December 21, 2000. The ALA says the law, which requires schools and libraries to install content filters on computers as a condition for U.S. government funding, infringes on First Amendment free-speech rights. Specifically, the ALA is alleging that the new filtering rules would serve to widen the so-called digital divide, which separates those with the means to access the Internet through their own household PCs from those who must rely on public-access machines. Even with the filter options turned on, says the ALA, there is no filtering software that "differentiates constitutionally protected speech from illegal speech on the Internet." That argument was successfully upheld in 1998 in a similar court case in Loudon County, Virginia. "The filters blocked so much constitutionally protected material that had absolutely nothing to do with pornography or anything like that," says Larry Ottinger, senior staff attorney at People for the American Way, the civil rights group that fought the Loudon restrictions. Among the sites blocked in that instance were the Yale University graduate school of biology, a Quaker Web site, Have an Affair Catering, and a beanie babies Web site. (NewsFactor Network 19 Jan 2001)
http://www.newsfactor.com/perl/story/6838.html

NEW EFFORT TO END INTERNET FILTERING PROGRAM IN LIBRARIES
The American Civil Liberties, the American Library Association, and other plaintiffs are filing federal lawsuits this [week] to overturn a new law called the Children's Internet Protection Act, which requires schools and libraries receiving federal money for technology to shield school children from pornography and violence transmitted over the Internet. The dispute splits political parties. One Republican, Ernest Istook of Oklahoma, says that civil libertarians falsely label the law censorship "if they're not permitted to expose our children to the very worst things on the Internet, using federal tax dollars to do so," whereas Republican Jeffrey Pollock (whose own political site was once blocked by filtering software) says: "To mandate the federal government to legislate morality, I find abhorrent." (New York Times 19 Mar 2001)
http://partners.nytimes.com/2001/03/19/technology/19FILT.html

---

Category 32.1 *Censorship in the USA*

2001-05-21 **pornography children censorship indecent constitution first amendment free speech**

NewsScan

CHALLENGE TO LAW RESTRICTING KIDS' ACCESS TO PORNOGRAPHY [21 May 2001]
The U.S. Supreme Court has agreed to hear a challenge to the constitutionality of a 1998 law passed by Congress imposing criminal penalties on operators of Web sites that expose children to commercially offered "indecent" material. The law does not cover e-mail or chat rooms. The issue is whether the attempt to shield children ends up abridging constitutional rights to freedom of speech. A supporter of the law says: "We're talking about material that would be harmful to minors. That is a test we have applied for years in the real world. If you walk into a bookstore, the pornography is wrapped, or behind a blinder or will be in a place where it is difficult for young people to reach it." An American Civil Liberties Union official who opposes the law counters that it "would send adults to prison for commercial speech that is unquestionably protected for them." (AP/USA Today 21 May 2001)
http://www.usatoday.com/life/cyber/tech/2001-05-21-scotus-online-porn.htm

---

Category 32.1 *Censorship in the USA*

2001-07-30 **child pornography mandatory reporting law enforcement police integrity authenticity presumption innocence guilt proof evidence exculpation credibility**

RISKS 21 57

Brien Webb pointed out some risks of a new law in South Carolina which requires "that private technicians tell police if they find child pornography when servicing computers." Webb writes in RISKS, "Think of the possibilities. You're servicing computers, and you get the idea to have some fun. You take a client's computer, roll the date back, access some child pornography web site(s), reset the date, and call the cops. Carrying it one step further, imagine that this as a political 'dirty trick.' It might just be the mayor or some legislative representative who gets victimized. Who would believe any protestations of innocence?"

http://www.washingtonpost.com/wp-srv/aponline/20010727/aponline203146_000.htm

---

Category 32.1 *Censorship in the USA*

2001-11-29 **code speech constitution first amendment lawsuit jurisprudence DVD decryption software Web posting criminal hacker**

NewsScan

APPEALS PANEL SEEKS ANSWERS ON COMPUTER CODE AS FREE SPEECH [11 May 2001]
A three-judge appeals panel has asked both sides in the case testing the constitutionality of the 1998 Digital Millennium Copyright Law to answer a list of 11 questions focusing on whether computer code can qualify as free speech. The case pits the major Hollywood studios against Eric Corley, the publisher of online magazine 2600. A federal judge previously issued an injunction blocking Corley from distributing a computer code that can break the security lock on a DVD. Corley's appeal argues that the injunction violates his right to free speech. "I've never seen this happen before," says one of Corley's attorneys. "What's clear is that neither Judge Kaplan's decision nor the briefs nor the oral arguments have given them the answer to the questions they think are most important." The questions suggest that the judges are looking beyond Corley's case to how the ruling might apply more generally. One question raised is whether software code is more like a list of instructions -- traditionally protected by free speech -- or a machine that simply happens to be built with speech, which would not fall under the scope of the First Amendment. (New York Times 11 May 2001)
http://www.nytimes.com/2001/05/11/technology/11CODE.html

COURT RULES AGAINST USE OF PROGRAM THAT UNLOCKS DVD ENCRYPTION [29 Nov 2001]
The Motion Picture Association of American (MPAA) has prevailed in the U.S. Court of Appeals against a computer hacker publication's claim to have the right to publish a program that used reverse-engineering to unlock the copyright protection system of DVDs. At issue was the constitutionality of the Digital Millennium Copyright Act (DMCA) of 1998, which was challenged by programmer Eric Corley, who publishes the hacker magazine 2600. Corley and his supporters, which include the Washington-based civil liberties group called the Electronic Frontier Foundation, believe that the DMCA gives too much power to copyright-holders and violates First Amendment rights of researchers and consumers. (New York Times 29 Nov 2001)
http://www.nytimes.com/2001/11/29/technology/29DVD.html

Category 32.1 *Censorship in the USA*

2002-03-25 **library Internet content filtering software children censorware legal challenge lawsuit**

NewsScan

LEGAL CHALLENGE TO CHILDREN'S INTERNET PROTECTION ACT
A coalition of libraries, Web sites and other interested parties has begun offerings testimony in court hearings on the constitutionality of the Children's Internet Protection Act of 2000, which requires public libraries that accept federal financing or technology discounts to install software filters to protect children from adult material on the Internet. In the words of Senator John McCain (R-Ariz.), the law passed by Congress is intended to allow "local communities to decide what technology they want to use, and what to filter out, so that our children's minds aren't polluted." Coalition members include the American Library Association, the American Civil Liberties Union, and one Republican lawmaker who had originally supported the legislation but changed his mind about it when he discovered that his own campaign site was blocked out by one popular filtering program. (New York Times 25 Mar 2002)
http://partners.nytimes.com/2002/03/25/national/25LIBR.html

PROTECTING CHILDREN OR ABRIDGING FREE SPEECH?
A second week of testimony has begun [April 2, 2003] in Philadelphia in a federal district court that is hearing a case to decide a constitutional challenge to the Children's Internet Protection Act (CIPA), signed by President Clinton in 2000 and intended to protect children from violence and pornography without abridging the free-speech rights of adults. Shown a ring binder filled with pornographic images and asked by a government attorney, "Is it your testimony that I have the right to look at these Web pages?" librarian Candace Morgan said "Yes, it is," and added later: "We have sex manuals with similar pictures to this one." Another witness, Chris Lemmon, said he found pornographic sites involving elderly women "disturbing." The plaintiffs in the case are arguing, among other things, that CIPA relies on technology that can not distinguish between protected and unprotected speech. The government's position is that libraries that don't want to use software filters to protect children can simply refuse to accept federal subsidies since CIPA applies only to institutions that receive government funding.
(AP/Washington Post 1 Apr 2002)
http://www.washingtonpost.com/wp-dyn/articles/A47070-2002Apr1.html

COURT OVERTURNS LAW REQUIRING SOFTWARE FILTERS
A three-judge federal panel in Philadelphia struck down a provision of the Children's Internet Protection Act (CIPA) requiring public libraries to install software on library terminals to filter out pornographic material. The law applied to libraries that received federal technology funding, and supporters of the law had maintained that Congress has the right to decide what it does or doesn't want to fund. But the Court ruled that the legislation was fatally flawed because there currently exists no software that can with complete precision filter only the targeted material -- and nothing else by accident. The case is likely to be appealed to the U.S. Supreme court. (San Jose Mercury-News 1 Jun 2002)
http://www.siliconvalley.com/mld/siliconvalley/3379690.htm

Category 32.1 *Censorship in the USA*

2002-04-05 **library Internet content filtering software children censorware legal challenge lawsuit**

NewsScan

LIBRARY NET PORN CASE WILL BE APPEALED REGARDLESS OF OUTCOME
A decision from the three-judge federal appeals court in Philadelphia hearing the dispute over the constitutionality of the Children's Internet Protection Act (CIPA) will be handed down next month [May 2002], but is certain to be appealed to the Supreme Court, no matter how the judges decide. One of the judges observed, "We're stuck right in the heart of the First Amendment when we're talking about libraries." Another judge, concerned that decisions on what constitutes pornography were being left to "nameless and faceless" people in software filtering firms, asked "What right does the government have to require this kind of filtering system?" (CIPA requires libraries that accept federal funding to use such systems to protect children from pornography and violence.) Critics charge that the software filters are blunt instruments that cannot reliably discern the difference between pornography and constitutionally protected information. An ACLU lawyer calls the law "a sham," since "everybody knows you can't comply with its terms." A Justice Department lawyer sees the issues differently: "There is no constitutional right to immediate, anonymous access to speech, for free, in a public library." And then adds: "Even if you assume that libraries have a right to provide unfettered access to the Internet, they don't have a right to do so with a federal subsidy. The crux of this matter is whether or not Congress has the power to decide how to use its money." (Reuters/USA Today 4 Apr 2002)
http://www.usatoday.com/life/cyber/tech/2002/04/04/library-porn.htm

---

Category 32.1 *Censorship in the USA*

2002-04-12 **computer games standards monitoring labeling censorship children commerce regulation ratings**

NewsScan

FTC SCRUTINIZES 'MATURE' VIDEO GAMES
The Federal Trade Commission has requested information on sales of mature-themed video games to minors, as a precursor to an expected June report on media violence. In December, the FTC issued a report that offered four suggestions for the movie, music and games businesses: establish industry standards on advertising in places where the primary audience is under 17; develop better labeling of ratings within ads; improve self-regulation with regard to retailer compliance; and implement industry sanctions for non-compliance with sales and advertising sanctions. Since the video game rating system was instituted in 1994, more than 7,000 games have been rated, with some 500 earning an "M" (mature) rating, meaning they are not intended to be played by children under 17. (Reuters/USA Today 11 Apr 2002)
http://www.usatoday.com/life/cyber/tech/2002/04/11/ftc-video-games.htm

---

Category 32.1 *Censorship in the USA*

2002-04-17 **virtual child pornography free speech SCOTUS lawsuit ruling judgement decision constitution**

NewsScan

COURT SAYS THAT TO HAVE CHILD PORNOGRAPHY YOU NEED A CHILD
The U.S. Supreme Court has ruled that portions of the Child Pornography Prevention Act of 1996 are unconstitutional because they infringe on First Amendment free-speech rights. (In U.S. law, images have traditionally been considered a form of "speech.") The 1996 law banned "virtual" pornography that uses computer-manipulated images rather than real children to portray children engaged in sex acts. Justice Anthony M. Kennedy wrote in the majority opinion that the government "has shown no more than a remote connection between speech that might encourage thoughts or impulses and any resulting child abuse. The mere tendency of speech to encourage unlawful acts is not a sufficient reason for banning it." (New York Times 17 Apr 2002)
http://partners.nytimes.com/2002/04/17/national/17PORN.html

Category 32.1 *Censorship in the USA*

2002-04-26 **parental consent violent sexual videogames free speech legal judgement**

NewsScan

JUDGE SAYS GOVERNMENTS [CAN] RESTRICT KIDS' ACCESS TO VIDEO GAMES
Remarking that "video games have more in common with board games and sports than they do with motion pictures," U.S District Judge Stephen Limbaugh has ruled in support of a St. Louis County ordinance requiring children under 17 to have parental consent before they can buy violent or sexual videogames (or play such games in video arcades). Judge Limbaugh believes the ruling had nothing to do with free speech, because the games provide "no conveyance of ideas, expression, or anything else that could possibly amount to speech." The Interactive Digital Software Association, which had challenged the ordinance, plans to appeal the ruling, asserting that it "is clearly in conflict with virtually every other federal court decision on this and related issues." (AP/USA Today 24 Apr 2002)
http://www.usatoday.com/life/cyber/tech/2002/04/24/judge-games.htm

---

Category 32.1 *Censorship in the USA*

2002-05-07 **video games sex violence standards proposed legislation law**

NewsScan

BILL WOULD BAN SALE OF VIOLENT VIDEO GAMES TO KIDS
California Congressman Joe Baca has proposed legislation that would ban to children sales of video games that contain scenes of decapitation and dismemberment, murder, car jackings, illegal drug use, rape, prostitution, assault and other violent crimes. Doug Lowenstein, president of the Interactive Digital Software Association, thinks the bill is "both unnecessary and unconstitutional," but acknowledges: "I certainly respect the concerns that give rise to a bill like this." In introducing the legislation Congressman Baca said: "I've had enough of the violence we're experiencing among our youth. When kids play video games, they assume the identity of the characters in the games ... Do you really want your kids assuming the role of a mass murderer or car jacker when you are away at work?" (Reuters/San Jose Mercury News 6 May 2002)
http://www.siliconvalley.com/mld/siliconvalley/3210541.htm

Category 32.1 *Censorship in the USA*

2002-05-14 **COPA pornography content filterining constitutionality legal challenge**

NewsScan

CHILD ONLINE PROTECTION ACT SURVIVES REVIEW (JUST BARELY)
The Child Online Protection Act, passed by Congress in 1998 and intended to impose prison sentences for posting material "harmful to minors" on a Web site to which minors could have access, survived a lower court ruling that had declared it unconstitutional. The lower court's decision hinged on its rejection of a clause in the Act defining "objectionable" material as material that did not meet "contemporary community standards," a definition which the lower court said would give veto power over the Internet to "the most puritan of communities." The appellate court thought that point settled the matter, but the Supreme Court sent the case back to Federal District Court with instructions to think through all of the relevant issues before making a decision. Court-watchers expect that the Act will eventually be declared unconstitutional by the Supreme Court, when the lower court is finished reconsidering it. (New York Times 14 May 2002)
http://www.nytimes.com/2002/05/14/national/14SCOT.html

Category 32.1 *Censorship in the USA*

2002-05-17 **COPA SCOTUS ruling**

FindLaw ConstitutionalCaseLaw, http://laws.lp.findlaw.com/us/000/001293.html

SCOTUS: ASHCROFT v. AMER. CIVIL LIBERTIES UNION (05/13/02 - No. 00-1293)
The Child Online Protection Act's (COPA) use of "community standards" to identify what material "is harmful to minors" does not by itself render the COPA statute substantially overbroad under the First Amendment.

To read the full text of this opinion, go to:

Category 32.1 *Censorship in the USA*

2002-05-28 **videogames indecency violence gore obscenity standards restrictions ratings**

FindLaw Download This 87

OF DOOM, GLOOM, FUN AND GAMES
Video games and their designers are all grown up, ready to take on darker, mature themes. The change hasn't slowed their popularity with fans, but it has given lawmakers pause. . . Earlier this month, a federal judge in St. Louis upheld a county law that criminalized the sale of "Mature"-rated video games to anyone under 17, despite the lack of similar laws that would punish the sale of R-rated movies or CDs with parental warnings to those same kids. "I think the root of the problem is that most observers do not yet appreciate the fact that video games are artistic achievements every bit as worthy and creative as a film, a song or a painting," said Douglas Lowenstein, IDSA's president.
http://www.wired.com/news/games/0,2101,52661,00.html

Interactive Digital Software Association
http://www.idsa.com/

Category 32.1 *Censorship in the USA*

2002-05-28 **Web free speech censorship decency violence gore law enforcement police**

FindLaw Download This 87

UNDER FBI PRESSURE, SITE REMOVES PEARL MURDER VIDEO
Saying it was under pressure from the FBI, a Web site that specializes in gruesome images has removed video footage recorded during Wall Street Journal reporter Daniel Pearl's murder. The operator of the Ogrish.com site and the president of its Web hosting company told Newsbytes the FBI ordered the video taken down under threat of a lawsuit, but a spokeswoman for the FBI said the bureau merely made a "courtesy request" on behalf of Pearl's family.
http://www.newsbytes.com/news/02/176762.html

The Daniel Pearl Foundation
http://www.danielpearlfoundation.org/

Category 32.1 *Censorship in the USA*

2002-06-04 **SCOTUS virtual child pornography**

FindLaw Download This 88

SOLVING KID PORN'S 'REAL' PROBLEM
In the aftermath of a U.S. Supreme Court ruling that computer-generated images of minors engaged in sexual acts are not illegal and are in fact protected by the First Amendment, some prosecutors and police investigators have found themselves at a loss for how to proceed in child porn cases. More suspects are claiming that the seemingly illicit pictures and videos found on their hard drives are ersatz, police say. And an Illinois man who had already pleaded guilty to possessing 2,600 images of kiddie porn was freed from jail when a judge ruled that the state's law was unconstitutional because it failed to distinguish between real and fake porn. http://www.wired.com/news/business/0,1367,52945,00.html

Read the Opinion (AMERICAN LIBRARY ASS'N., INC. v. US)[PDF]
http://news.findlaw.com/hdocs/docs/ala/cipa53102opn.pdf

View the Order Enjoining the Enforcement of the CIPA [PDF]
http://news.findlaw.com/hdocs/docs/ala/cipa53102ord.pdf

Category 32.1 *Censorship in the USA*

2002-06-19 **Internet content filters pornography software workarounds exploits**

NewsScan

THE FILTER WARS
Arguing that "intellectual development is one of the fundamental human rights and it's also a right that people under 18 have," programmer Bennett Haselton has made a reputation as a foe of software filters designed to shield children from pornography and violence. He's created an organization called Peacefire.org, which offers free downloads and details methods for getting around filtering software. Haselton says, "This is something that practically nobody else is working on, and only a couple of people in the world actually know as much about the blocking software issue." One of Haselton's many critics, Marc Kanter of Solid Oak Software, which makes the popular CYBERsitter filtering program, says of him: "He's being totally irresponsible. When he started Peacefire, he was a kid himself. Basically he was enticing minors into his beliefs and activities, which was to undermine parents' rights. As an adult now, he should know better than that." (AP/USA Today 17 Jun 2002)
http://www.usatoday.com/life/cyber/tech/2002/06/18/net-filter-war.htm

---

Category 32.1 *Censorship in the USA*

2002-06-20 **child pornography legislation law proposal digital photography simulations free speech censorship**

NewsScan

CONGRESS GETS READY TO CONTINUE FIGHT AGAINST KID PORN
If at first you don't succeed, try, try again, and the House Judiciary Committee is trying once again to write legislation that will not only ban virtual child pornography but also pass Supreme Court muster. The new, more narrowly drafted bill would outlaw child pornography involving any prepubescent child, including computer images of such a child if the images were indistinguishable from actual photos. New York Democrat Jerry Nadler argued against the bill, on the grounds that it would criminalize protected speech, but fellow Democrat Adam Schiff, a Californian, insisted: "If we only go after pornography using real children we will effectively preclude any real prosecution of child pornography." (Reuters/USA Today)
http://www.usatoday.com/life/cyber/tech/2002/06/19/virtual-porn.htm

---

Category 32.1 *Censorship in the USA*

2003-02-20 **online content filter Internet law child pornography ISP Internet service provider**

NewsScan

OPPOSITION TO SOFTWARE FILTERING LAW
The Washington-based civil liberties group Center for Democracy and Technology is considering a legal challenge to a Pennsylvania law that threatens fines on any company providing Internet access to Web sites with child pornography rather than fines on the pornographic sites themselves. CDT associate director Alan Davidson says, "It's sort of this weird world where we're not prosecuting the people producing child pornography," and instead harassing Internet service providers whose existence is necessary for the stability of the Internet. (AP/San Jose Mercury News 20 Feb 2003)

Category 32.1 *Censorship in the USA*

2003-03-04 **children Internet SCOTUS constitutionality free speech pornography violence law**

NewsScan

SUPREME COURT TO REVIEW INTERNET FILTER LAW
The U.S. Supreme Court has agreed to consider the constitutionality of the Children's Internet Protection Act, which requires that libraries receiving federal funding for Internet access must install software filters to prevent children from being exposed to pornography and excessive violence. A coalition of libraries, library users and Web sites successfully challenged the law at the appellate level, where the court ruled that filters were "blunt instruments" that would suppress not only pornography and violence but constitutionally protected speech presented on legitimate sites. It is now being argued that the lower court was wrong when it viewed the case as a first amendment case, and should instead have treated it as one involving the government's broad discretion to decide whether material is sufficiently worthwhile for the government to required to support it with public funds. The government argues that to assert otherwise is to argue that public libraries engage in prior restraints when they fail to provide pornographic magazines or XXX videos to their patrons." (New York Times 13 Nov 2002)

SOFTWARE FILTERING CASE GOES TO SUPREME COURT
Tomorrow the U.S. Supreme Court will hear arguments in a case challenging the constitutionality of the Children's Internet Protection Act of 2001, which requires any library that receives federal money to block access to online pornography and obscenity. In support of the Act, U.S. Solicitor General Ted Olson says that libraries are being asked merely to use the same kind of discretion they've always used in managing their print collections: "Public libraries have broad discretion to decide what material to add to their collections. The use of filtering software to block access to online pornography falls well within the permissible limits of that discretion. (USA Today 3 Mar 2003)

Category 32.1 *Censorship in the USA*

2003-04-16 **free speech censorship hacking information techniques lecture**

NIPC/DHS

April 14, CNET News.com — Court blocks security conference talk.

Washington D.C.-based education software company Blackboard convinced a Georgia state court to block a pair of students from presenting information at a security and hackers' conference on how to break into and modify a university electronic transactions systems. Blackboard argues that the restraining order blocked the publication of information gained illegally, which would have harmed the company's commercial interests and those of its clients. But organizers of the Interz0ne conference in Atlanta contend that Georgia Institute of Technology's Billy Hoffman and University of Alabama's Virgil Griffith's free speech rights were abridged. The information set to be presented was gleaned after one of the students had physically broken into a network and switching device on his campus and subsequently figured out a way to mimic Blackboard's technology, the company told the judge. Because that alleged act would be illegal under the federal and state laws, publication of the resulting information should be blocked, it argued. A hearing on a permanent injunction against publication or presentation of the work will be held in Georgia state court Wednesday.l

---

Category 32.1 *Censorship in the USA*

2004-03-02 **Child Online Protection COPA Act review Congress civil liberties ACLU free speech**

NewsScan

SUPREMES TO REVIEW CHILD ONLINE PROTECTION ACT

The Supreme Court will do a new review of the free-speech ramifications of Congress' latest version of the 1998 Child Online Protection ACT (COPA). The Justice Department's position is that "there is a compelling government interest in protecting minors from the effects of material that is not obscene by adult standards but that is nonetheless harmful to minors... Minors today can search the Web as easily as they can change television channels. Thus, in the seclusion of their homes or those of friends, unsupervised minors can, with the click of a mouse, visit one pornographic site after another." The American Civil Liberties Union (ACLU) says the law violates the Constitution's First Amendment guarantee of free speech: "COPA's bludgeon suppresses an enormous amount of speech protected for adults and is unnecessary and ill-tailored to address the government's interest in protecting children from sexually explicit content." (AP/Washington Post 2 Mar 2004)

Category 32.1 *Censorship in the USA*

2004-03-04 **children personal private information not for sale law**

NewsScan

SENATORS SEEK TO PUT CHILDREN'S DATA OFF LIMITS

U.S. Senators Ron Wyden (D-Ore.) and Ted Stevens (R-Alaska) have introduced the Children's Listbroker Privacy Act, which would limit the sale of personal data on children under 16 without their parents' consent. The bill is part of a larger package of legislation aimed at helping parents fight back against a deluge of commercial messages aimed at their children. Currently companies spend about $12 billion annually on marketing to children, often using lists from brokers like the Student Marketing Group that reveal the child's name, address, age, ethnicity, religious affiliation, sports activities, hobbies and family income level. "Many large companies see childhood as a commercial free-fire zone. But some things shouldn't be for sale, and our children's personal information is one of them," says Gary Ruskin, executive director of Commercial Alert. (Wired.com 4 Mar 2004)

Category 32.1 *Censorship in the USA*

2004-07-13 **US governmetn South Dakota library censorship Internet usage teen objectionable material**

NewsScan

GOV. REMOVES PART OF S. DAKOTA LIBRARY SITE

South Dakota Governor Mike Rounds has had the teen section of the State Library's Web site shut down because it provided links to material he doesn't believe young people should see. The links to which he found objection included one to a Planned Parenthood site and one to Columbia
University's Go Ask Alice! Rounds said: "As a parent, I would be very disturbed to have my children connecting to any of these Web sites." His position is that state government should not feature links to any advocacy groups and that removal of the links isn't censorship because users can still go directly to those organizations' sites. (AP/13 Jul 2004)

Category 32.1 *Censorship in the USA*

2005-01-31 **high school first amendment free speech**

NewsScan;
http://www.knightfdn.org/default.asp?story=news_at_knight/releases/2005/2005_01_31_firstamend.html

SCHOOL NEWS: FIRST AMENDMENT? WHAT FIRST AMENDMENT?

A University of Connecticut survey of more than 100,000 high school students has found that educators are failing to give high school students an appreciation of the First Amendment's guarantees of free speech and a free press. Commissioned by the Knight Foundation, the $1 million, two-year study found that nearly three-fourths of high school students either do not know how they feel about the First Amendment or admit they take it for granted; seventy-five percent erroneously think flag burning is illegal; half believe the government can censor the Internet; and more than a third think the First Amendment goes too far in the rights it guarantees. Knight Foundation chief executive Hodding Carter III says, "These results are not only disturbing; they are dangerous. Ignorance about the basics of this free society is a danger to our nation's future." (Knight Foundation 31 Jan 2005)

Category 32.1 *Censorship in the USA*

2005-03-24 **Federal Election Commission Internet activity rules campaign finance control**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/articles/A63872−2005Mar 24.html

FEDERAL ELECTION COMMISSION OFFICIALS WEIGH LIMITED INTERNET ACTIVITY RULES.

Federal Election Commission (FEC) officials on Thursday, March 24, took their first steps in extending campaign finance controls to political activity on the Internet, asking for public input on limited regulations for the freewheeling medium. Commissioner Ellen Weintraub, who took the lead on drafting proposals with vice chairman Michael Toner, described the steps as "restrained." The commission emphasized a hands-off approach to bloggers, or authors of Web logs, among the loudest and unruliest voices online. The draft guidelines suggest applying limits that exist in other media to certain political advertising on the Web and political spam e-mail. The commission said it was exploring Internet regulation reluctantly - ordered to do so by a court - and with the lightest touch possible, exempting everything except certain kinds of paid political advertising. But the Center for Individual Freedom, a nonprofit advocacy group, said any regulation is too much. FEC Website: http://www.fec.gov/

Category 32.1 *Censorship in the USA*

2006-02-01 **Microsoft blog censorship policy local law violation proof China filter**

EDUPAGE; http://www.internetnews.com/bus-news/article.php/3582016 23

MICROSOFT OUTLINES BLOG CENSORSHIP POLICY

Microsoft has announced details of a new policy on censoring the content of blogs maintained by its customers. According to the new policy, blog content will only be blocked to comply with local laws and with the terms of use of MSN Spaces, the company's blog application. In order to have content blocked, a local government must demonstrate that it violates local laws. Moreover, the content will only be blocked in areas where those laws apply; users in other parts of the world will still be able to see the content. In cases where content is blocked, users will be notified and told that the reason is a government restriction. Microsoft's announcement follows criticism of its decision to comply with requests of Chinese authorities to remove the blog content of an individual the government considered a threat. The announcement also comes on the heels of Google's plan to filter the content of its search results to comply with local laws in China. Both companies said their decisions are based on the belief that it is better to have a presence in countries like China, even if that requires limiting access to certain online content.

32.2 Censorship outside the USA

Category 32.2 *Censorship outside the USA*

2000-01-25 **censorship hate speech Web international British UK England**

Edupage, Wired

In Britain, the Internet Watch Foundation (IWF) announced an expansion of its focus beyond the fight against child pornography. From January on, the IWF would also try to root out hate speech on the Internet. [In many countries other than the US, speech that incites hatred of or violence toward an identifiable group of people is illegal.]

Category 32.2 *Censorship outside the USA*

2000-06-07 **government censorship suppression freedom oppression dictatorship tyranny propaganda fear weakness human rights violations corruption news**

NewsScan

Police in the Chinese city of Chengu . . . arrested 36-year-old Huang Qi on suspicion of "subverting state power" by operating the Web site www.6-4tianwang.com, which publishes information about human rights problems and corruption in China. If tried and convicted Huang could be imprisoned for more than ten years. (Reuters/San Jose Mercury News 7 Jun 2000)

Category 32.2 *Censorship outside the USA*

2000-08-04 **censorship surveillance oppression dictatorship free speech monitoring Internet**

NewsScan, San Jose Mercury News
http://www.sjmercury.com/svtech/news/breaking/internet/docs/278114l.htm

The Xinhua news agency in China is reporting that the Chinese government has created 20 or more special Internet police units around the country to "administrate and maintain order," investigate "criminal cases, such as cheating, property embezzlement, and pornography," and train volunteer "electronic security guards" for banks. Although the Chinese government routinely monitors the activities of its critics, the Xinhua report makes no mention of new government efforts to police political activities on the Internet. (Reuters/4 Aug 2000)

Category 32.2 *Censorship outside the USA*

2000-10-03 **censorship government totalitarian fear restrictions policing content filtering ISP audit trail police law enforcement privacy encryption**

NewsScan, Los Angeles Times
http://www.latimes.com/business/200001003/t000093953.html

In its continuing effort to keep a lid on the impact of the Internet, China's government . . . issued new regulations that hold companies responsible for blocking illegal or subversive content, limit foreign investment, and threaten to close down any unlicensed operations. Internet content and service providers are directed to keep records of all content on their Web sites and all the users who dial into the servers for 60 days, and turn those records over to police on demand. "This creates a system that would require such a scale of enforcement that it could potentially occupy the whole efforts of ICPs," . . .[said] a Beijing-based Internet consultant. "Technology will respond. It will give rise to a whole new generation of encryption techniques." (Reuters/Los Angeles Times 3 Oct 2000)

Category 32.2 *Censorship outside the USA*

2000-11-07 **censorship privacy government restriction law chat e-mail news**

NewsScan, San Jose Mercury News
http://www.mercurycenter.com/svtech/news/breaking/merc/docs/023148.htm

The Chinese government has prohibited Web sites not owned by the state from offering news reports and has issued rules requiring that chat rooms engage only in officially approved topics. Portal sites will need special permission to offer news from foreign media. An executive of the portal site Sohu.com took an optimistic view of the new restrictions: "These were already the unwritten rules. In fact, this is better because we now know what the limits are." (AP/San Jose Mercury News 7 Nov 2000)

Category 32.2 *Censorship outside the USA*

2000-11-29 **international law jurisdiction Web sites hate speech censorship**

NewsScan, San Jose Mercury News
htt://www.sjmercury.com/svtech/news/breaking/merc/docs/077786.htm,
Financial Times http://news.ft.com/news/industries/infotechnology

[In August,] France, where it is illegal to exhibit anything that incites racism, . . . [took] legal action against Yahoo! Inc. because its sites have been used for the sale of Nazi medallions, swastikas, etc. Yahoo has withdrawn customer postings of such items on its French site, fr.yahoo.com, but says it is not technically feasible to keep French users off of sites in other countries. In the U.S., extremist ideas are protected by the First Amendment of the Constitution, which guarantees the right of freedom of speech. (AP/San Jose Mercury News 11 Aug 2000)

[In November, a] Paris court . . . ordered Yahoo! to block French users from accessing Nazi memorabilia on its U.S. sites, citing French anti-racist laws. The ruling . . .[gave] Yahoo! three months to implement some type of system that would accomplish its objective and . . . [imposed] a FFr100,000 (US$13,000) per day fine if it . . . [failed] to comply. Yahoo! had agreed to block the sale of such items on its French language portal following an earlier ruling, but had argued that the ban could not be extended to the U.S. site, both on U.S. constitutional grounds and because it was technically infeasible. But three court-appointed international experts concluded that a system to check the nationality of users, combined with password checks, would identify 90% of French citizens seeking to buy Nazi memorabilia. Industry groups are "deeply concerned" over the implications of the ruling: "Despite the obnoxious nature of the [Nazi] material, this ruling sets a very bad precedent for the future development of services on the Internet," says the head of the e-business unit at the Confederation of British Industry. (Financial Times 21 Nov 2000)

Internet experts Vint Cerf and Ben Laurie . . . [criticized] the decision of a French court to order Yahoo's U.S. portal site to prevent its customers from seeing auctions of Nazi memorabilia. Cerf, who is often described as the "Father of the Internet," . . . [said] that "if every jurisdiction in the world insisted on some form of filtering for its particular geographic territory, the World Wide Web would stop functioning." (BBC News 29 Nov 2000)
< http://news.bbc.co.uk/hi/english/sci/tech/newsid_1046000/1046548.stm >

Category 32.2 *Censorship outside the USA*

2000-12-04 **censorship monitoring anonymity identity repression totalitarian government regulation hypocrisy propaganda**

NewsScan, San Jose Mercury News
http://www.mercurycenter.com/svtech/news/breaking/merc/docs/084179.htm

In announcing new rules to monitor activities on online bulletin boards, China's Minister of the Information Industry said: "Don't misinterpret this. The Chinese government absolutely is not saying people can't use these things, but we must find a more healthy way to manage them to ensure the protection of individuals' reputation and privacy. Anyone who has used the Web knows already that people always use false names. No one uses their own name. If someone attacks someone else there is no way to catch them, no way to sue them." (AP/San Jose Mercury News 4 Dec 2000)

Category 32.2 *Censorship outside the USA*

2001-05-31 **virtual child pornography violent video games legislation proposal**

RISKS 21 45

Marcus de Geus reported on proposals to ban virtual child pornography in the Netherlands:

"The Dutch Minister of Justice, Korthals, has announced measures that will make it illegal to produce or possess child pornography created by means of electronic image manipulation. The proposed legislation appears to be aimed at preventing the production and possession of artificially rendered images that could be interpreted as representations of children involved in sexual acts. Current Dutch law states that the production or possession of pornography is a criminal offence if it involves the physical (ab)use of (real) persons under a certain age. [Based on a report in an e-mail message from Radio Nederland Wereldomroep.] "

The correspondent noted that on the same basis of reasoning (child porn is bad therefore virtual child porn should be banned), it would be possible to ban violent video games (wholesale slaughter is bad therefore virtual wholesale slaughter is bad).

[MK adds: PLEASE don't shower me with abuse for _reporting_ this line of argument.]

Category 32.2 *Censorship outside the USA*

2001-06-07 **censorship government vetting criminal prosecution Web content**

NewsScan

TURKEY'S BATTLE FOR "TRUTH" ON THE WEB
Under a new law passed by the Turkish parliament, Web site operators publishing "untrue news, insults and similar material" are subject to fines of up to $85,000. An earlier draft of the law would have required owners of Web sites to provide local prosecutors printed copies of the site every day. (AP/Salon 7 Jun 2001)
http://www.salon.com/tech/wire/2001/06/07/turkey/index.html

Category 32.2 *Censorship outside the USA*

2001-07-23 **censorship government policies Internet content access China**

NewsScan

CHINA INTERNET USE GROWS WHILE GOV'T CRACKDOWN CONTINUES
China's crackdown on Internet cafes that allow its customers access to material the authorities consider "pornographic, anti-government, violent, unhealthy or superstitious" has led to the closing of more than 8,000 Internet cafes (Wang ba, or "Net bars") since April. At least 15 people have been detained by the police, and two were recently sentenced to up to four years in prison. But interest in the Internet remains strong, and there are now an estimated 26 million Internet users in China, compared to only 4 million two years ago. (San Jose Mercury News 23 Jul 2001)
http://www.siliconvalley.com/docs/news/svfront/078240.htm

Category 32.2 *Censorship outside the USA*

2001-11-19 **content filtering censorship control autocracy women's liberation female autonomy culture conflict**

NewsScan

SOFTWARE COMPANIES VIE TO PROVIDE SAUDIS WITH INTERNET FILTERS
When the Internet was introduced in Saudi Arabia in 1999, the Saudi royal family decreed that all public traffic into and out of the country would have to be funneled through a single control outside Riyadh. The contract for providing the filtering software to make that level of control possible will expire in 2003, and companies from the U.S., U.K., Germany and the Netherlands are engaged in spirited competition for the multimillion assignment. Yale law professor Jack Balkin says, "We have a really serious problem in terms of the American free speech idea. But it is very American to make money. Between anticensorship and the desire to make money, the desire to make money will win out." The sites blocked by the Saudis are pornographic or offer other challenges to Islamic political or cultural sensitivities. (New York Times 19 Nov 2001)
http://partners.nytimes.com/2001/11/19/technology/19SAUD.html

---

Category 32.2 *Censorship outside the USA*

2002-02-22 **ISP Internet service providers hate speech censorship international regulation agreement treaty harmonization cooperation law enforcement investigation prosecution extradition**

NewsScan

EUROPEAN "HATE SPEECH" LEGISLATION WORRIES CIVIL LIBERTARIANS [22 Feb 2002]
A proposal by the Council of Europe that would criminalize racist and other "hate speech" on the Internet is worrying both civil libertarian groups (which regard it as a blow against free speech) and Internet service providers (which are concerned about their legal liability for material posted without their consent). The principal administrator of the Council of Europe thinks that the various countries belonging to the organization must "harmonize" their laws "so that countries can cooperate in criminal investigations regarding the Internet," but the head of the Campaign Against Censorship on the Internet in Britain took a very different view: "This proposal could potentially outlaw free speech. That would be a great infringement of civil rights." (Reuters 22 Feb 2002)
http://www.reuters.com/news_article.jhtml?type=internetnews&StoryID=623493

Category 32.2 *Censorship outside the USA*

2002-05-16 **international censorship Great Firewall of China content filtering**

NewsScan

CHINA SUSPENDS CENSORSHIP OF WESTERN NEWS SITES
Without explanation, the Chinese government has removed blocks on the normally censored foreign Web sites, including those of such news organizations as Reuters, CNN and the Washington Post. It is not known whether the decision would stay in force, and officials at the International Press Centre and the Ministry of State Security provided no information about the new development. The Web sites of the Los Angeles Times, National Public Radio, the San Francisco Chronicle, the Boston Globe, and the Atlanta Journal-Constitution can also now be accessed, whereas the Time magazine, Voice of America, and BBC News sites still appear to be blocked. (Reuters/San Jose Mercury News 15 May 2002)
http://www.siliconvalley.com/mld/siliconvalley/3273080.htm

Category 32.2 *Censorship outside the USA*

2002-09-12 **government censorship international search engine Web content filtering firewall**

NewsScan

WHERE IN THE WORLD IS GOOGLE? HINT: NOT CHINA
As part of a wider clamp-down on the ability of Chinese citizens to use the Internet to learn about the world beyond the country's "Great Firewall," Chinese authorities have blocked access to Google. The Google search engine is especially popular in China because it can run Chinese-language searches. (San Jose Mercury News)

CHINA ENDS BLOCKING OF GOOGLE
Chinese authorities have ended their policy of preventing citizens in that country from accessing the Google search engine, which is especially popular there because of its ability to make it easy to find Chinese-language material online. In its usual style, the government gave no indication of why it was removing the restrictions (nor, for that matter, why it had imposed them in the first place). But censorship in China continues, as evidenced by an increase in selective blocking, which prevents visitors to a Web site from seeing specific items which the government finds politically incorrect. (AP/San Jose Mercury News 12 Sep 2002)

Category 32.2 *Censorship outside the USA*

2002-10-25 **censorship legal restrictions free speech hate search engine Web**

NewsScan

GOOGLE CENSORS SEARCH RESULTS FOR FRENCH AND GERMAN USERS

A report from Harvard Law School found that when users from France and Germany tap Google's search engine, at least 100 sites are automatically deleted from the search results. Most of the missing sites promote either white supremacy or Holocaust denial. Both France and Germany have strict laws banning hate speech, and a Google spokesman says the company must occasionally remove sites to avoid legal liability. Such removals are done in response to specific requests and are not done preemptively, he added. "We carefully consider any credible complaint on a case-by-case basis and take necessary action. We only react to requests that come to us." Harvard Law School researchers found about 65 sites that were excluded from Google.de, the German site, and about 113 sites were missing at Google.fr, the French site. (AP 24 Oct 2002)
http://apnews.excite.com/article/20021024/D7MS6SJ80.htm

Category 32.2 *Censorship outside the USA*

2002-12-04 **censorship international regulations Internet access content filtering firewall pornography politics**

NewsScan

LAND OF THE CENSOR: CHINA
A study by Harvard Law School researchers finds that China is the country with the world's most oppressive censorship of what its citizens can view on the Internet. Chinese authorities block access to 19,000 sites, and also delete individual links or Web pages of which they do not approve. Most of the disapproved sites are political in nature. When it comes to blocking pornography, China (at least for now) cedes the first-place prize to Saudi Arabia: China blocks fewer than 15% of sexually explicit Web sites compared to Saudi Arabia's blocking of 86%. (New York Times 4 Dec 2002)
http://partners.nytimes.com/2002/12/04/international/asia/04CHIN.html

CENSORSHIP IN CHINA: WHAT ARE THEY THINKING?
We've previously reported that Chinese officials have the most stringent Internet censorship program in the world, but haven't remarked on the broad scope of it. It blocks out not only pro-democracy content but also a bit of just about everything else. Jonathan Zittrain and Benjamin Edelman, two Harvard Law School researchers who have been studying international Internet filtering, say that in addition to Taiwanese and Tibetan pro-democracy sites the Chinese also block health sites, U.S. university sites, and sites devoted to comic books, science fiction, etc. Human rights worker Greg Walton comments: "The study's an interesting insight into the Chinese censor's head. If I was a psychologist and I had China's censor on the couch, I'd ask, 'Why are you repressing these things?'" (Wired News 4 Dec 2002)
http://www.wired.com/news/politics/0,1283,56699,00.html

Category 32.2 *Censorship outside the USA*

2002-12-20 **censorship arrest writer freedom speech international**

NewsScan

CHINESE AUTHOR ARRESTED AFTER INTERNET CRACKDOWN
The novelist and poet Liao Yiwu, who has written about the very poorest social strata in China, is one of several dozen activists detained by law enforcement authorities in the city of Chengdu in southwestern China. Liao's articles about the poor are banned in China but have been published abroad by Web sites critical of the Chinese regime. (USA Today 19 Dec 2002)

Category 32.2 *Censorship outside the USA*

2002-12-31 **video games sex pornography violence age children adults**

NewsScan

EUROPEAN UNION TO RATE VIDEO GAMES FOR SEX AND VIOLENCE
Violent and sexually-oriented computer games sold in Europe will soon be getting classifications established by the European Union: games with no sex or violence at all will get a rating of 3+ and all other games will receive ratings of 7+, 12+, 16+, or 18+. EU secretary-general Patrice Chazerand says: "It is only fitting that an industry exerting increasing influence on people displays an enhanced sense of social responsibility." (BBC News 29 Dec 2002)
http://news.bbc.co.uk/1/hi/technology/2612983.stm

Category 32.2 *Censorship outside the USA*

2003-03-06 **Internet content filtering pornography**

NewsScan

THE AUSTRALIAN APPROACH TO SPAM
Clive Hamilton, the head of an Australian public think tank, thinks that Australia's method of Internet regulation, managed by the Australian Broadcasting Authority, is essentially useless. Referring to a survey finding that 84% of boys ages 16-17 are exposed to pornography on the Internet, Hamilton complained: "The Internet industry has convinced the government that there is little that can be done to prevent pornography coming in from overseas. But this is false. Mandatory filtering by Internet service providers (ISPs) would severely restrict the availability of pornography." Labor information technology spokeswoman Kate Luncy disagrees: "The cost this would place on ISPs would be prohibitive and Internet speeds would be significantly reduced. The end result for consumers would be a slower, more expensive Internet." (The Age 4 Mar 2003)

Category 32.2 *Censorship outside the USA*

2004-03-19 **China free speech blogs web logs shut down forbidden content**

NewsScan

CHINA SHUTS DOWN 'FORBIDDEN CONTENT' ON BLOGS

China has shut down the Web sites containing blogs (i.e., Web logs or online diaries) "because individual postings contained forbidden content." One site was closed simply for "allowing a letter to be posted that was critical of the government." (AP/USA Today 19 Mar 2004)

Category 32.2 *Censorship outside the USA*

2004-05-07 **8600 unlicensed internet cafes political control china**

NewsScan

CHINA SHUTS DOWN 8,600 INTERNET CAFÉS IN 3 MONTHS

Chinese authorities say they have shut down more than 8,600 unlicensed Internet cafés in the last three months in their latest campaign to bring the communication channel under tighter political control. Ostensibly, the crackdown is to protect teenagers from long Internet benders playing combat games and the like. The case of two middle school pupils in Chongqing, who fell asleep on a railway line and were run over on March 31 following a 48-hour interactive gaming session, is being cited. But preventing customers from gaining access to "unhealthy information online" is also a concern behind the drive against unauthorized public Internet venues, which was launched in February and will run until August, says the agency that licenses Internet cafés. Preventing anonymous access to the Internet from cafés has been one prong of Beijing's drive to squelch the Internet's political power for the past 18 months, although the excuse has always been the fire risk and protecting juveniles from abuse. (The Age 7 May 2004) rec'd from John Lamp, Deakin University

---

Category 32.2 *Censorship outside the USA*

2004-06-07 **chid pornography censorship British Telecom British law Page Not Found**

NewsScan

BT SYSTEM FOR BLOCKING CHILD PORN SITES

Using a system called Cleanfeed, British Telecom intends to block its 2.7 million Internet subscribers from reaching child pornography Web sites banned under British law. Attempts to reach the sites will result in a "Page Not Found" error message. Cleanfeed will block sites by filtering out either specific domain names or the unique numeric addresses associated with the Web server hosting the site; it can also block individual pictures on sites. In the U.S., civil liberties groups have fought attempts to force service providers to block access to child porn sites, taking the position that such efforts have the unintended consequence of also blocking thousands of legitimate sites. (AP/Los Angeles Times 7 Jun 2004)

Category 32.2 *Censorship outside the USA*

2004-06-15 **China pornographic site censorship illegal harmful online content**

NewsScan

CHINA CRACKS DOWN ON PORNOGRAPHIC SITES

China has shut down five pornographic Web sites in a new campaign that asks people to report "illegal or harmful" online content. In what's shaping up as a tough new plan to control the Internet, Chinese authorities say they've received more than a thousand complaints about pornographic material on Web sites in just the last few days. Last week, China launched net.china.cn, a site called the Illegal and Harmful Content Reporting Center. It follows the introduction of numerous measures to curb online activities in the communist country, which now has about 80 million Internet users. (The Age 15 Jun 2004) Rec'd from John Lamp, Deakin U.

Category 32.2 *Censorship outside the USA*

2004-06-20 **China government mandate self-discipline pact Internet rules**

NewsScan

SELF-DISCIPLINE IN CHINA

The Chinese government is asking Internet service providers there to sign a "self-discipline pact" and to exercise patriotic judgment: "The basic principles of self-discipline for the Internet industry are patriotism, observance of the law, fairness and trustworthiness." Observance of the pact will require that Web sites post no information "threatening to the national security, social stability or containing superstitious or erotic content." (AP/Los Angeles Times 20 Jun 2004)

Category 32.2 *Censorship outside the USA*

2004-07-21 **Vietnam censorship Internet pornographic anti government crackdown**

NewsScan

VIETNAM STEPS UP CONTROL OF INTERNET

Vietnam has stepped up efforts to control the Internet, instructing Internet service providers to terminate contracts with cyber-cafes that allow customers to access pornographic or anti-government sites. The directive, issued by Minister of Post and Telecommunications Do Trung Ta, is the latest in a string of measures unveiled in recent months to prevent "bad and poisonous information" being circulated online. This latest regulation requires the communist nation's seven state-owned Internet service providers to disconnect cyber-cafes if they allow clients to access forbidden sites. Café owners are also instructed to monitor their customers' use of the Web for any violations of government regulations, such as distributing viruses and accessing pornographic sites or those that "threaten national security." (The Age 21 Jul 2004) Rec'd from John Lamp

---

Category 32.2 *Censorship outside the USA*

2004-07-26 **China Internet censorship cleanup block pornography crackdown**

NewsScan

CHINA WANTS TO CLEAN UP THE INTERNET

Beijing has blocked 988 overseas Web sites and shut down 67 local ones as part of a nationwide campaign to weed out pornographic content on the Internet. The sites shut down during the July 6-21 special operation included Hong Kong sites, and Google was also inaccessible. So far, the
Chinese capital has arrested 13 people suspected of operating the sites. The police had received 10,660 tips from the public, and the majority of those tips were complaints about inappropriate sexual content on the Internet and complaints about pornographic mobile phone short messages. (The Age 26 Jul 2004) Rec'd from John Lamp

---

Category 32.2 *Censorship outside the USA*

2004-08-04 **Vietnam Internet monitoring Cyber cops fraud hacking banned information**

DHS IAIP Daily;
http://www.boston.com/business/technology/articles/2004/08/0
4/cyber_cops_to_monitor_internet_in_vietnam/

August 04, Associated Press — Cyber cops to monitor Internet in Vietnam.

A new police unit will start cracking down on Internet criminals next month as communist Vietnam works to maintain control over its growing number of online users. The special unit will focus on crimes such as credit card fraud, hacking, gambling and posting banned information online, the Vietnam News reported Wednesday, August 4. Although the unit will take action against those who post anti-communist messages, it will mainly focus on financial abuses, said Nguyen Tu Quang, director of Hanoi's Technology University Network Security Center, which trained the cyber officers. The cyber police unit will work in collaboration with Internet service providers, universities, banks, former hackers and other security forces, Quang said. About two million of Vietnam's 81 million people access the Web. The number of users is expected to triple by next year, the paper said.

Category 32.2 *Censorship outside the USA*

2004-08-09 **anti pornography measures China censorship underage surfing**

NewsScan

TOP CHINESE SITES LAUNCH ANTI-PORN MEASURES

Popular Chinese web sites Sina.com, Sohu.com and Netease.com are complying with orders to clean up web content to "create a green environment for millions of underage surfers." The official Xinhua news agency says that technical measures had been taken to clean up the sites and web-links, as well as to block pornographic content in their chatrooms and bulletin boards. On the main page of Sina.com on Friday, small sections where pictures of scantily dressed embracing couples are normally posted had disappeared, but were replaced with news about internet crackdown on pornographic content. However, a word search still yielded Web pages containing revealing pictures of women, such as a Sina.com sports website which contained a series of pictures taken from a British tabloid newspaper. (The Age 9 Aug 2004) Rec'd from J Lamp

---

Category 32.2 *Censorship outside the USA*

2004-11-01 **China Internet café censorship**

NewsScan; http://www.latimes.com/technology/ats-ap_technology12nov01

CHINA CLOSES INTERNET CAFES

China has shut down 1,600 Internet cafes and fined operators a total of $12 million because they allowed children play violent games or commit other violations of the government's policies to clean up Web sites and video games. Investigators have inspected 1.8 million Internet cafes looking for unlicensed operations, has ordered 18,000 of them to "stop operation for rectification" of violations. The country has the world's second-largest population of Internet users after the United States, with 87 million people online. Culture Ministry official Zhang Xinjian says: "Porn, gambling, violence and similar problems have adversely affected the healthy development of the Internet in China." (AP/Los Angeles Times 1 Nov 2004)

Category 32.2 *Censorship outside the USA*

2004-11-08 **Iran censorship pro-democracy websites**

NewsScan;
http://www.nytimes.com/2004/11/08/international/middleeast/08iran.html?oref=
login

IRAN'S CRACKDOWN ON PRO-DEMOCRACY WEB SITES

In the past several months Iran has blocked hundreds of pro-democracy Web sites and arrested such journalists as Mahboubeh Abbas-Gholizadeh and Fereshteh Ghazi, both of whom write about women's issues. But the move to block Web sites has the support of senior cleric Ayatollah Makarem Shirazi, who declared in September that Web sites should be blocked if they "insult sacred concepts of Islam, the Prophet and Imams," or if they publish "harmful and deviated beliefs to promote atheism or promote sinister books." (New York Times 8 Nov 2004)

Category 32.2 *Censorship outside the USA*

2004-11-09 **China censorship video game Taiwan independence political television commercial**

NewsScan; http://apnews.excite.com/article/20041209/D86S32RG0.html

DISSIN' CHINA

Law enforcement authorities in China have banned the new British computer game "Football Manager 2005" because it refers to Taiwan as a separate country, contrary to the mainland government's insistence that Taiwan belongs to China. The government is searching for the game online and in computer software markets, cybercafes, and places that sell pirated software. A spokesman for the game's developer, Sports Interactive, says it's working on a Chinese version for release in China that will comply with local requirements: "We will follow the correct submission and approval process within China and look forward to feedback from the Chinese authorities on any modifications that may be required." Last week China also banned a Nike television commercial it says is disrespectful and blasphemous toward Chinese culture. The ad features NBA star LeBron James in a mock video with a kung fu master, two women in traditional Chinese attire, and a pair of dragons. (AP/9 Nov 2004)

Category 32.2 *Censorship outside the USA*

2005-02-07 **cell phone UK moral London prostitution censorship filtering advertising**

NewsScan; http://wsj.com/

U.K. CELLPHONE COMPANIES REJECT ROLE OF 'MORAL ARBITER'

A London city councilman wants cellphone companies to strangle the vice trade by declining calls to the numbers shown on business cards soliciting prostitution, but most cellphone companies say it isn't their job to interfere with a customer's service. A Vodaphone spokesman says, "We are not content to play the role of moral arbiter." The decision is supported by the English Collective of Prostitutes, which says that women who are unable to advertise in phone booths may be forced to walk the streets, a more dangerous activity than operating from an apartment. Although prostitution itself (though not street solications) is legal in the U.K., the city councilman says a crackdown is crucial because the world's oldest profession has been booming in London ever the fall of the Berlin Wall, when organized crime gangs began to coerce young women from Eastern Europe and Russia to work for them. (Wall Street Journal 7 Feb 2005)

Category 32.2 *Censorship outside the USA*

2005-02-14 **China crackdown café censorship shutdown Internet pornography subversion politics schools**

NewsScan;
http://ap.washingtontimes.com/dynamic/stories/C/CHINA_INTERNET_CRACKDOWN?SITE=DCTMS&SECTION=HOME

CHINA'S CRACKDOWN ON INTERNET CAFES

Chinese authorities shut down more than 12,575 Internet cafes in the last three months of 2004 to create a "safer environment for young people in China," according to the Xinhua News Agency. With 87 million people online, China has the world's second-largest population of Internet users (after the U.S.), and the government actively promotes Internet use for business and education. However, communist authorities block access to Web sites they deem pornographic or subversive and Internet cafes are banned from operating near schools. (AP/Washington Times 14 Feb 2005)

Category 32.2 *Censorship outside the USA*

2005-03-21 **China censorship blocking college campus Webpages discussions politics pop culture pornography**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=7958355

CHINA BLOCKS ACCESS TO CAMPUS WEB PAGES

Chinese officials have blocked outside access to a number of online bulletin boards operated by universities. Such bulletin boards have become popular vehicles for discussion about topics including politics, pop culture, and pornography, subjects which Chinese authorities have not been shy about censoring. Tsinghua University's Shuimu Tsinghua bulletin board was one of those restricted recently, joining bulletin boards at Wuhan University and Nankai University, as well as one at Peking University that was shut down entirely. According to a student from Tsinghua University who asked not to be named, the Ministry of Education's reasoning for blocking outside access was "because the bulletin board was only supposed to be a platform for internal exchange within the university." He added, "Students are calm about it, but it seems that non-student users are angry because they can no longer get access." Reuters, 21 March 2005

Category 32.2 *Censorship outside the USA*

2005-05-09 **Singapore censorship scare tactics University of Illinois Urbana-Champaign graduate student blog shut down A*Star science research SLAPP strategic lawsuit against public participation**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=8422422

STUDENT SHUTS DOWN BLOG AFTER THREAT FROM SINGAPORE

Chen Jiahao, a graduate student in chemical physics at the University of Illinois at Urbana-Champaign, has shut down his personal blog and issued two apologies after an agency of the government in Singapore threatened to sue Chen for defamation. A*Star, the agency in Singapore dealing with science and research, accused Chen, who is from Singapore, of libelous statements that "went way beyond fair comment." The agency demanded a public apology but said Chen's first apology was insincere and insisted on another. A*Star said it welcomes various opinions and perspectives, but many in the journalism community rejected that claim. Singapore has long had a reputation for using tactics including lawsuits to silence critics. Organizations including the Committee to Protect Journalists and Reporters without Borders have decried Singapore's threats to Chen and journalists. "Chen criticized some of A*Star's policies," said Julien Pain, head of Reporters without Borders' Internet freedom desk, "but there was nothing defamatory in what he wrote." Reuters, 9 May 2005

[MK adds: a clear case of a SLAPP, no? (Strategic Lawsuit Against Public Participation)]

Category 32.2 Censorship outside the USA

2006-01-06 **China Web Internet journalist blogger site shut down censorship Microsoft**

EDUPAGE; http://www.nytimes.com/2006/01/06/technology/06blog.html 23

MICROSOFT AGREES TO CLOSE CHINESE BLOGGER'S SITE

Following a formal request from Chinese officials, Microsoft has shut down the blog of a high-profile Chinese journalist. China is well known for censoring public speech it considers critical of the government, and Microsoft's actions are not the first in which non-Chinese companies have complied with Chinese authorities. Officials from Microsoft noted that if their services are to be available in China, the company must comply with local laws. As Brooke Richardson, a group product manager for MSN said, "We think it's better to be there with our services than not be there." Last year Yahoo was faulted by some for cooperating with Chinese officials, and it too stated then that a requirement of continuing operation in the country is to conform to local laws and regulations. Rebecca MacKinnon, a fellow at the Berkman Center for Internet and Society at Harvard Law School, expressed concerns on her blog about Microsoft's action. "Can we be sure," she said, "they won't do the same thing in response to potentially illegal demands by an overzealous government agency in our own country?" New York Times, 6 January 2006 (registration req'd)

Category 32.2 Censorship outside the USA

2006-01-24 **Google censorship search results China laws regulations Reporters Without Borders**

EDUPAGE; http://news.com.com/2100-1028_3-6030784.html 23

GOOGLE TO CENSOR SEARCH RESULTS IN CHINA

Google will launch search and news sites in China this week that will block access to information the Chinese government considers objectionable. Chinese officials have a long track record of censoring speech and ideas, and, according to Andrew McLaughlin, senior policy counsel for Google, the new sites "will comply with local Chinese laws and regulations." Search results from which content has been excluded will notify users that not all results are being displayed. Google said that the decision to offer its services even if they are censored reflects the belief that limited access to Internet resources is better than no access, which would be the alternative if Google did not comply with local legislation. "We must balance our commitments," said McLaughlin, "to satisfy the interest of users, expand access to information, and respond to local conditions." Reporters Without Borders, an organization that advocates for freedom of the press, was highly critical of the decision, saying, "The new Google version means that even if a human rights publication is not blocked by local firewalls, it has no chance of being read in China."

Category 32.2 Censorship outside the USA

2006-01-26 **China government censorship search engine GOOGLE US law**

RISKS 24 15

COMPLEXITY OF SEARCH ENGINE COMPLIANCE WITH LOCAL LAWS

Lauren Weinstein, founder of People for Internet Responsibility < http://www.pfir.org >, wrote a thoughtful analysis of the problems search engine companies such as GOOGLE face in meeting conflicting standards in different nations. For example, GOOGLE recently cooperated with the Chinese government in blocking access to certain materials that frighten certain elements within that totalitarian regime; on the other hand, GOOGLE also refused to cooperate with US federal law enforcement requests for records of user searches because of privacy concerns. Weinstein wrote, "The situation highlights the minefield of issues that Google and other Internet companies now face, and the desperate need for proactive approaches to dealing with the ways that these technologies affect individuals and society."

He also pointed to initiatives in the US Congress that would have significant implications for international relations: "Congressman Tim Ryan has announced a hearing of the Congressional Human Rights Caucus (16 Feb is the date that I've heard) to explore the potential drafting of laws that would limit or otherwise control U.S.-based Internet companies from complying with the censorship demands of foreign countries. Emotions were clearly exasperated by Google's launching of the 'dot-cn' Chinese version of Google search that blocks links as per Chinese government directives, though Google is not alone in this regard among U.S.-based Internet companies."

For a streaming video of a one hour lecture by Lauren Weingstin touching on these issues and other of interest, see < http://neon.vortex.com/lauren-google-2006-01-24.asx >.

Category 32.2 *Censorship outside the USA*

2006-02-03 **Internet pro-terrorism Website US extradition trial freedom privacy**

DHS IAIP Daily; http://www.csmonitor.com/2006/0203/p06s02−woeu.html 23

INTERNET JIHAD: TACKLING TERROR ON THE WEB.

Nearly 18 months ago, Babar Ahmad, a British citizen, was arrested on an extradition request to the U.S. Charged with running Websites hosted in the U.S. that promoted and supported Islamic militancy, Ahmad remains in British custody. He has appealed the extradition order and Britain's High Court will hear the case on Monday, February 20. The proceedings will test the ability of Western governments to put on trial Islamic radicals who use the Internet as a key recruiting and organizational tool. But while the U.S. government pursues those who operate Websites that allegedly encourage terrorism, some argue that the authorities should instead concentrate on shutting down the sites themselves as soon as possible to limit their impact. Ahmad's case illustrates how seriously the U.S. is taking such Websites. His extradition warrant accuses him -- among other things -- of helping to run azzam.com, one of the earliest and most high profile English-language pro-jihad Websites, which for a time was run by an Internet Service Provider (ISP) headquartered in Connecticut. A federal grand jury in the U.S. indicted Ahmad in October 2004 on four charges. If found guilty, he faces life imprisonment.

Category 32.2 *Censorship outside the USA*

2006-02-08 **Yale Website censored Thailand ruler biography**

EDUPAGE; http://chronicle.com/daily/2006/02/2006020801t.htm 23

THAILAND BLOCKS YALE PRESS WEB SITE

Internet users in Thailand will not be able to access the Yale University Press Web site following the government's response to a biography that presents an unflattering image of the country's king, Bhumibol Adulyadej. Thai officials in the Ministry of Information and Communications Technology frequently block access to online materials that include adult or violent content, criticism of the Thai royal family, information about the country's national security, or allegedly false advertising. The book, written by journalist Paul M. Handley, who reported from Thailand for 13 years, will be released by the Yale University Press in July. It is also expected to be banned in the country. Although Handley refused to comment specifically on the government's decision to censor the press's Web site, saying that the book will speak for itself, Yale issued a statement defending the book and the author.

Category 32.2 *Censorship outside the USA*

2006-02-14 **US State Department Internet Freedom Task Force launch censorship political content**

DHS IAIP Daily; 23
http://www.techweb.com/wire/ebiz/180201737;jsessionid=U5ND2C
KBMSPZ4QSNDBCCKH0CJUMEKJVN

U.S. STATE DEPARTMENT LAUNCHES INTERNET FREEDOM TASK FORCE.

The U.S. State Department on Tuesday, February 14, established a task force to investigate the problems posed to the Internet by repressive regimes, a move that followed a call for help by Google Inc., Microsoft Corp. and Yahoo Inc., which have been criticized for censoring information in China. The task force would consider how the use of technology to restrict access to political content has impacted U.S. companies. The panel would also investigate the use of technology to track and repress dissidents and efforts to modify Internet governance structures in order to restrict the free flow of information. The task force is expected to draw upon the department's expertise in international communications policy, human rights, democracy, business advocacy, corporate responsibility and relevant countries and regions, Shiner said. Besides working with U.S. companies and non-governmental agencies, such as human rights groups, the task force will seek help from the European Union and other governments facing similar problems with Internet censorship.

Category 32.2 *Censorship outside the USA*

2006-04-12 **Google China research center content filtering censorship local law compliance Book Search**

EDUPAGE; http://online.wsj.com/article/SB114484852659023945.html 23

GOOGLE REBUFFS CRITICS, EXPANDS CHINESE RESEARCH CENTER

Responding to critics of Google's decision to filter certain content to Chinese users, CEO Eric Schmidt reiterated the company's position that it is better to have a presence in China with some restrictions than not to be there at all. Other Internet companies operating in China face the same restrictions as Google--preventing access to sites the government deems objectionable--and Schmidt said Google has not received any complaints from Chinese users. Noting that one-fifth of the world's population lives in China and that many of them are or will be Internet users, Schmidt said Google would comply with applicable local laws and would expand its research operation in the country. The company currently employs about 30 engineers in its R&D facility in Beijing and plans to increase that number to 100. Schmidt also said Google is working with Chinese libraries to include their books in its Book Search program, which is scanning millions of books for online access.

Category 32.2 *Censorship outside the USA*

2006-05-09 **China censorship students bypass filters firewall**

EDUPAGE; http://www.nytimes.com/2006/05/09/world/asia/09internet.html 23

CHINESE STUDENTS POLICE INTERNET

In China, a government initiative known as "Let the Winds of a Civilized Internet Blow" aims to ensure that online content conforms to government expectations. Students at some Chinese universities are a key part of the effort. At Shanghai Normal University, 500 students serve as Internet monitors, participating in online discussions and trying to steer conversations away from topics considered objectionable. Unknown to most of the other students on campus, the monitors also report some content to campus officials, who delete it. One student monitor said, "Our job consists of guidance, not control." Critics argue that the practice amounts to nothing more than the censorship common to other areas of Chinese life. Chinese officials acknowledged that more than two million images and 600 online forums have been deleted for being "unhealthy." Some students dismissed the efforts, saying that with the Internet, you can always go elsewhere to share your opinions. "It's easy to bypass the firewalls," said one student, "and anybody who spends a little time researching it can figure it out."

Category 32.2 *Censorship outside the USA*

2006-05-12 **China Wikipedia rejection censorship Baidu search engine Biake encyclopedia**

EDUPAGE; http://www.siliconvalley.com/mld/siliconvalley/14563324.htm 23

CHINA REJECTS WIKIPEDIA, STARTS ITS OWN VERSION

Baidu, the leading search engine in China, has launched a site that approximates Wikipedia but with none of the content that prompted the Chinese government to block Wikipedia last year. Chinese authorities exert strong control over Internet content available in the country, and Wikipedia includes enough material deemed objectionable that the entire site is unavailable. Robin Li, chairman of Baidu, said his company's new site, Baike, was inspired by Wikipedia, though he said he has never actually seen Wikipedia. China is second only to the United States in Internet users, and Chinese users have reportedly written more than 25,000 Baike entries in the past week. Li said, "I certainly hope our encyclopedia will be the most authoritative one for any Chinese users."

---

33 Policies, risk analysis, risk management

Category 33 *Policies, risk analysis, risk management*

1997-01-17 **e-mail evidence slurs racism appropriate use policy**

AP

R. R. Donnelly & Sons, a Chicago printing firm, is being sued by over 500 workers after they were fired. As evidence, the workers' lawyers submitted "165 racial, ethnic and sexual jokes" circulated through the company's e-mail system.

Category 33 *Policies, risk analysis, risk management*

1997-01-29 **e-mail appropriate use threats**

UPI

Between November 1994 and January 1995, two perverts exchanged e-mail describing their sexual excitement at imagining violence against women. Jake Baker described his fantasies of raping a named woman from one of his classes at University of Michigan and was arrested and charged with engaging in interstate communications containing threats to kidnap or injure another person. The federal court in Detroit ruled that these sexually-oriented electronic messages do not constitute a threat and are protected speech subject to the First Amendment rights. At the end of January, the 6th U.S. Circuit Court of Appeals upheld the dismissal.

Category 33 *Policies, risk analysis, risk management*

1997-01-30 **censorship appropriate use**

EDUPAGE

In Oklahoma, federal Judge Wayne E. Alley ruled that the University of Oklahoma was entitled to impose restrictions on access to Internet news groups through its computer systems. The judge reasoned that, "The OU computer and Internet services do not constitute a public forum. There was no evidence at trial that the facilities have ever been open to the general public or used for public communication." The services are therefore not subject to First Amendment controls over restriction of content.

Category 33 *Policies, risk analysis, risk management*

1997-02-02 **censorship acceptable use**

EDUPAGE

Japanese companies and the government are planning to provide facilities for blocking access to various undesirable Web sites and are developing a Japanese analog to the US PICS (Platform for Internet Content Selection) scheme.

Category 33 *Policies, risk analysis, risk management*

1997-02-06 **Spam acceptable use**

RISKS 18 81 ff

3 Feb: Cyber Promotions Inc. barred from sending junk e-mail to CompuServe subscribers.
4 Feb: Enjoined not to falsify its From: addresses in junk e-mail to AOL subscribers.
5 May: Cyber Promotions mail-bombed into system failure by an organized attack by cyber-vigilantes.
6 May: CP computers subjected to arp-attack (millions of requests for hardware information)

Category 33 *Policies, risk analysis, risk management*

1997-02-11 **junk e-mail acceptable use**

EDUPAGE

CompuServe won an injunction preventing the cyberscum Cyber Promotions from sending junk e-mail to CompuServe users. Arguments from the defendant's lawyer claiming First Amendment protection for his client were summarily rejected: "[The] plaintiff is not a government agency or a state actor which seeks to preempt defendants' ability to communicate but is instead a private actor trying to tailor the nuances of its service to provide maximum utility to its customers."

Category 33 *Policies, risk analysis, risk management*

1997-02-13 **acceptable use**

RISKS 18 83

The University of Wisconsin-Madison is faced a sexual harassment lawsuit, claiming a former medical professor used campus computers to copy hundreds of pornographic pictures from the Internet. Another employee sued because the professor propositioned her.

Category 33 *Policies, risk analysis, risk management*

1997-02-16 **e-mail acceptable use**

EDUPAGE

EDUPAGE reported: "Early findings of a study e-mail use at a large mid-Atlantic university suggest there is, in general, no more harassment by e-mail than by telephone or snail mail, but that sexual harassment of women by e-mail is four to five times more likely than racial or ethnic harassment. The Prejudice Institute, a nonprofit group in Baltimore that released the study, found that 10% of the women who responded to its survey said that they received threatening e-mail, while 3% of the survey respondents said they had received racial or ethnic hate mail. (New York Times 16 Feb 97)"

Category 33 *Policies, risk analysis, risk management*

1997-02-18 **acceptable use**

RISKS 18 83 ff

In mid-February, two black employees of the Citibank NA unit of Citicorp filed a race discrimination lawsuit because of racist jokes allegedly sent via electronic mail by several bank supervisors. The e-mail was identical to a set of racially charged jokes at the center of a lawsuit against Morgan Stanley & Co. The lawsuit affirms that corporate management did little or nothing to stop the distribution of racist materials.

Category 33 *Policies, risk analysis, risk management*

1997-02-20 **junk e-mail spam**

AP, EDUPAGE

Cyber Promotions, the Satan of Spam, gave up trying to find an ISP that would tolerate their behavior and announced that they would form their own ISP specializing in junk e-mail. Sanford Wallace admits that his firm currently sends out 15-20M junk messages a day. Cyber Promotions began serving as an ISP in early March.

Category 33 *Policies, risk analysis, risk management*

1997-03-02 **junk e-mail acceptable use**

EDUPAGE

The Canadian Advertising Foundation is gearing up to receive and act upon consumer complaints about junk e-mail. The Foundation will publicly shame advertisers who use junk e-mail.

Category 33 *Policies, risk analysis, risk management*

1997-03-04 **junk e-mail acceptable use**

EDUPAGE

In Nevada, sending junk e-mail may soon become a misdemeanor. Other states currently considering such laws include CA, VA and CT.

Category 33 *Policies, risk analysis, risk management*

1997-05-07 **spam ISP VAN**

Wired

In early May, junk e-mailer Cyber Promotions suffered a number of blows. CompuServe won a permanent injunction against all further harassment of its members without explicit permission for junk e-mail by each recipient plus legal costs. Then Earthlink won the right not only to bar Cyer Promotion's spewing e-mail engines but also to forbid the use of its services to mask the origin of the junk; in addition, it demanded $3M in compensatory damages. These ISPs join Prodigy and AOL in their successful attack on the deceitful practices of the premier junk e-mailer in the world. In an unrelated development, vigilantes flooded the Cyber Promo site with millions of _arp_ requests for hardware configuration information, bringing the spammer's servers down.

A few weeks later, Earthlink announced a zero-tolerance policy for spammers and those who use the Earthlink name in fraudulent return addresses. It named eight companies: three companies offering Internet and financial services: Creative Finance Alternatives; Internet Communications; and New York Internet Center; and the other five — Sexy Girls Publishing, LCGM, Real Time Entertainment, S. Maddie Productions and Prosperity Books — that offer pornography. These spammers sent 200,000 messages through Earthlink and generated 16,673 complaints (8%).

Category 33 *Policies, risk analysis, risk management*

1997-05-08 **spam junk e-mail**

EDUPAGE

CompuServe and Cyber Promotions agreed that the junk-mail king would refrain from harassing CompuServe subscribers with unsolicited commercial e-mail. Cyber Promotions also agreed to pay CompuServe $65,000 for legal fees. Unfortunately for us biased anti-spammers, CompuServe agreed to spend $30,000 advertising through Cyber Promotions.

Category 33 *Policies, risk analysis, risk management*

1997-05-20 **appropriate use censorship**

EDUPAGE

The American Library Association published practical guidelines for librarians to help their patrons use the Internet without being pounded for accidental contact with indecent materials. See <http://www.ala.org/news/parented.html> for details.

Category 33 *Policies, risk analysis, risk management*

1997-05-22 **monitoring appropriate use privacy**

UPI

The American Management Association surveyed more than 900 companies and found that about 35% "monitor employees by recording phone calls or voice mail, checking computer files or e-mail, or videotape them at work."

Category 33 *Policies, risk analysis, risk management*

1997-06-10 **spam lawsuit fraud spoof bounced e-mail**

EDUPAGE

Cyber Promotions was back in court when Web Systems of Houston, TX accused the king of spam of including the plaintiff's Internet domain in a fraudulent return address. The victim received large numbers of offensive messages and huge amounts of bounced e-mail. The plaintiffs said they'd try to turn their suit into a class action to force spammers to use their real e-mail addresses in the REPLY-TO field.

Category 33 *Policies, risk analysis, risk management*

1997-07-06 **spam**

EDUPAGE

The Hormel Foods Corporation strongly objects to the use of its trademarked spiced-meat-and-fat-product-in-a-can as a synonym for abuse of the Internet. The company demanded that junk-e-mail panderer Sanford Wallace cease and desist from using "Spam" in its advertising and remove the picture of a can of Spam from its Web site.

Category 33 *Policies, risk analysis, risk management*

1997-07-07 **e-mail policy management**

InfoWorld

Bob Lewis, writing in InfoWorld, recounted the story of an employee who forwarded a mild joke from his boss to three other employees at work using corporate e-mail. As punishment, he was fined a week's pay. Lewis commented that this kind of ham-fisted over-reaction can destroy morale and drive good employees away.

Category 33 *Policies, risk analysis, risk management*

1997-07-29 **spam junk unsolicited commercial e-mail**

AP

Several US law-makers expressed interest in stemming the tide of junk e-mail. Sen. Frank Murkowski (R-AK) proposed a law to require marketers to identify themselves, their telephone number, physical and electronic address, and to clearly label their messages as advertisements. Sen. Robert Torricelli (D-NJ) proposed a bill that would prohibit junk e-mailers from disguising their identity, from using automated programs to gather e-mail addresses from USENET groups, mailing lists and chat forums, and from ignoring REMOVE messages. Rep. Chris Smith (R-NJ) wants an all-out ban on spam by br.oadening existing telecommunication laws to extend the ban on transmission of unsolicited ads through telephone lines to Internet messages.

The ACLU (American Civil Liberties Union) and CDT (Center for Democracy and Technology) argue that government interference with junk e-mail would be in violation of First Amendment protection on speech. Many free-speech advocates support the use of civil law to sue junk e-mailers for damages and to apply cease-and-desist orders. The Direct Marketing Association expresses horror at the thought of government intervention. Chet Dalzell of the DMA says, "When you have any new technology, you'll find there are people who'll push the parameters. But all indications are that marketplace forces will drive development of technology to protect consumers without government regulation."

Category 33 *Policies, risk analysis, risk management*

1997-08-05 **spam netiquette**

EDUPAGE, AP

In August, a coalition of system administrators blocked all inbound e-mail from UUNET, accusing the ISP of refusing to curb its spammers. UUNET officials responded grudgingly within a few days to attack its problems.

Category 33 *Policies, risk analysis, risk management*

1997-08-06 **spam junk unsolicited commercial e-mail**

Newsbytes

Ron Schwartz is a co-author of the textbook "Using Vbscript." He is also an anti-spam activist. When reports surfaced of unsolicited commercial e-mail from AMAZON.COM, however, Schwartz fought back by posting a request on on his AMAZON Web page telling people to buy the book elsewhere. AMAZON rejected accusations that it was using spam and insisted that it sends e-mail only to people who have signed up for such announcements.

Category 33 *Policies, risk analysis, risk management*

1997-08-07 **spam hacking vandalism information warfare**

Newsbytes

An angry hacker posted a 931 Kb file to several USENET groups containing many details of Cyber Promotion's user-IDs, passwords and all of the Internet domains hosted by this company. These included such junk-mailers as answerme.com, cheapcalls.com and savetrees.com as well as many pornography sites such as slutpics.com, nudeteens.com and oralsexpictures.com. The hacker pointed out that Cyber Promotions is the host of "the ever-popular godhatesfags.com domain" which specializes in hate-speech. In addition, the hacker warned Netcom that Cyber Promotions looks at their system every ten minutes to find new e-mail addresses for its junk e-mail lists.

Category 33 *Policies, risk analysis, risk management*

1997-08-11 **appropriate use games porn Internet Web policy productivity**

AP

Maggie Jackson, writing for Associated Press, reported on trends in appropriate-use policies for access to the Web. Some employees note that the Web is so interactive and stimulating that it can be seductive — entire days can be frittered away in fun and games. Employees who download and display pornography and hate propaganda are potentially contributing to a hostile work environment, which in turn can lead to expensive lawsuits and huge fines for the employer. Some organizations have installed filters and find that these programs can help; others have taken a more liberal approach and simply measure the total usage of the Web. Those who seem to be online excessively are warned in a friendly way, and self-policing seems to be getting the desired effects.

Category 33 *Policies, risk analysis, risk management*

1997-08-12 **spam USENET policy cancelbots NoCeM**

ZDNet News

Matthew Broersma, writing in ZDNet News, reported on the volunteer spam-cancelers — USENET administrators who delete junk postings. Using cancelbots, the administrators can catch postings from known spammers or identify multiple postings of the same message to to one or more groups. Another tool for fighting spam on the USENET is NoCeM, which uses shared lists of spammers to blank out such messages from News readers.

Category 33 *Policies, risk analysis, risk management*

1997-08-20 **spam costs**

RISKS 19 32

Keith Lynch commented in RISKS that spam is having unexpected consequences on the Net because of attempts to counter floods of unwanted mail. He suggests that, among other problems, spam-filters often discard non-junk e-mail; writers aware that the USENET and mailing lists are a rich source of e-mail addresses for spammers may reduce their postings and remove their articles from archives; fraudulent return addresses lead to harassment of innocent victims.

Category 33 *Policies, risk analysis, risk management*

1997-09-02 **spam privacy EPIC CDT**

Wired

A clerk at Experian erroneously issued a press release announcing support for the company's "EHI" anti-spam solution from the Electronic Privacy Information Center (EPIC) and the Center for Democracy and Technology (CDT). Unapologetic Experian director Ian Oxman dismissed public repudiation by EPIC's Marc Rotenberg by snapping, ""I think the people who understand the plan won't pay any attention to Marc's sniping. Marc doesn't know what he's talking about." Unfortunately for Mr Oxman, Marc Rotenberg is highly regarded in the online world for his intelligence and integrity.

Category 33 *Policies, risk analysis, risk management*

1997-09-25 **ethics appropriate use guidelines universities colleges**

EDUPAGE

Across the US, academic institutions have been increasing their efforts to train their students in ethical use of computer systems and networks. Some, such as University of Delaware and Cornell University, are making permanent user IDs contingent on successful completion of appropriate-use courses and tests.

Category 33 *Policies, risk analysis, risk management*

1997-10-03 **spam unsolicited commercial e-mail ISP denial of service**

Newsbytes, PR Newsbytes, ZDNET

Apex Global Internet Services (AGIS) sadly had to reconnect Cyber Promotions back to the Internet as a result of a court ruling forcing the ISP to give the junk-e-mail sender 30 days notice before cutting off their service to reduce attacks on AGIS' network by anti-spam vandals. The disgusted ISP had cut off Cyber Promotions and several other spammers in late September after going down under a barrage of pings apparently directed at harassing the spammers. Later in October, Sanford "Spamford" Wallace was quoted in the New York Times as saying that his firm would not be much affected by being thrown off AGIS because they now serve the other parasites who send junk e-mail by supplying consulting services.

Category 33 *Policies, risk analysis, risk management*

1997-10-06 **spam unsolicited commercial e-mail**

TechWeb

Some USENET veterans banded together to re-establish the style of trusted interactions that characterized the USENET before know-nothing scum flooded the Net with unsolicited commercial postings. According to some studies, 80% of the total traffic on the current USENET is now garbage. USENET2 would establish a new top-level domain called net.* and would require all participants to guarantee they would govern their users to prevent spam. In addition, participating ISPs would block all postings with forged headers.

Category 33 *Policies, risk analysis, risk management*

1997-10-19 **junk e-mail regulation**

PR Newswire, EDUPAGE

Apex Global Internet Services, Inc (AGIS) of Dearborn, MI, demanded that all members of the Internet E-Mail Marketing Council (IEMMC) stop sending bulk e-mail through the AGIS network. The chief culprits in the ongoing spam wars, Cyber Promotions, Cybertize E-mail, Integrated Media Promotions, ISG, and Quantum Communications, agreed to stop using AGIS for their junk e-mail as of 97.05.25. The IEMMC proposes to serve as a voluntary watchdog for the junk e-mail industry; however, it is entirely unclear how voluntary agreements among members of the IEMMC could possibly influence non-members, such as the amateurs who use high-volume junk e-mail generators in pursuit of hare-brained and usually fraudulent get-rich-quick schemes. In October, AGIS terminated all services to Wallace's company, but he said it no longer mattered to him — he now serves primarily as a consultant.

Category 33 *Policies, risk analysis, risk management*

1997-10-20 **spam free speech unsolicited commercial e-mail**

COMTEX Newswire (Newsbytes)

Rebecca Vesely stepped into a cross-fire in October when, writing in Wired, she announced that unsolicited commercial e-mail (UCE, "spam", "junk e-mail") is protected speech under the 1st Amendment to the Constitution of the United States and therefore there's nothing anyone can do about it. Wrong, said critics: just because commercial speech is protected against government interference in a public place it does not mean that private resources such as our e-mail accounts can be used with impunity by spammers.

Category 33 *Policies, risk analysis, risk management*

1998-02-08 **spam wars**

EDUPAGE

In February, the FTC initiated actions against spammers with over 1000 letters to people who were sending unsolicited commercial e-mail involving what appeared to be fraudulent activities. Failure to obey the instructions to stop could result in court orders and seizure of the spammers' assets.

Category 33 *Policies, risk analysis, risk management*

1998-02-15 **spam bulk e-mail junk**

EDUPAGE

Spam is facing competition from more ethical bulk e-mailers who send advertisements exclusively to people who request them using a profile of their interests. Some operators hope that their service will help provide an alternative that allows legislators to make junk e-mail illegal — if anyone can define junk e-mail sufficiently tightly for legal applications.

Category 33 *Policies, risk analysis, risk management*

1998-03-12 **spam wars**

EDUPAGE

In March, California state legislator Jim Cunneen introduced a fierce law aimed at allowing punishing civil litigation against spammers who violate ISP terms of service.

Category 33 *Policies, risk analysis, risk management*

1998-03-17 **spam junk e-mail forged headers**

EDUPAGE

The creators of the popular sendmail program widely used for forwarding e-mail throughout the Internet offered a new version with antispam features such as filters to block mail from known spam-sites and the ability to reject messages with forged headers.

Category 33 *Policies, risk analysis, risk management*

1998-03-19 **corporate policy dialup modem firewall**

EDUPAGE

Employees at Sun Microsystems learned that corporate policy requires them to be fired if they violate security policy by having a modem attached to their workstation, thus bypassing corporate firewalls.

Category 33 *Policies, risk analysis, risk management*

1998-03-29 **spam legal action junk e-mail**

EDUPAGE

The notorious "Spamford" Wallace of Cyber Promotion, Inc. paid $2M to settle lawsuits with several ISPs whose resources he had used in massive waves of junk e-mail. He claimed that he was giving up the spamming business.

Category 33 *Policies, risk analysis, risk management*

1998-03-31 **appropriate use pornography corporate policy**

EDUPAGE

According to EDUPAGE, "Two managing directors in the equity research department of the Salomon Smith Barney brokerage firm [were] fired for using company equipment to transmit pornography" in March.

Category 33 *Policies, risk analysis, risk management*

1998-05-03 **pornography inappropriate use business employees Internet**

EDUPAGE

Elron Software makes Internet-usage monitoring software. Keep this in mind when evaluating their survey findings that suggested that more than two thirds of the employees studied logged onto porn sites at work using their employers' equipment. About half that many used news sites. Together, these statistics, if they can be replicated, suggest the startling implication that about 98% of the Internet usage going on at work is for possibly non-essential purposes (the proportion of news-gathering time required for work was unknown). [However, the sample size and hence the precision of the percentage estimates are unknown to this compiler of the InfoSec Year in Review.]

Category 33 *Policies, risk analysis, risk management*

1998-07-16 **spam forgery headers packets impersonation**

EDUPAGE

In Washington state, it is now illegal to send e-mail with forged headers or other bogus indications of origin to Washington residents. The law also applies to Washington residents who send spam out of state. A Seattle man collected $200 from a violator of this law. If more states were to pass laws like this, spammers might go out of business (or offshore). In late Oct, the state charged Natural Instincts, a spamming-engine promoter who allegedly used forged headers to hrass 50,000 victims with the hypocritical subject line, "Did I get the right e-mail address?"

Category 33 *Policies, risk analysis, risk management*

1998-08-02 **e-mail intellectual property appropriate use policy ownershi**

EDUPAGE

In Florida, theAmerican Family Publishers corporation demanded thatan ex-employee return 200 e-mail messages they say belong to them. A circuit court judge began hearing the case at the end of July.

Category 33 *Policies, risk analysis, risk management*

1998-08-18 **spam spam Spam SPAM SPAM! Wonderful SPAAAM!**

EDUPAGE

Braving the contumely of Internet users everywhere, Hormel Foods opened its new site at <http://www.spam.com>. Visitors could order clothing with the Spam(TM) logo — now there's an exciting thought!

Category 33 *Policies, risk analysis, risk management*

1998-09-08 **e-mail privacy ownership subpoena**

EDUPAGE

Microsoft subpoenaed Netscape Corporation to obtain e-mail archives as part of its defense strategy against accusations of market manipulation.

Category 33 *Policies, risk analysis, risk management*

1998-09-15 **DNS Whois database mining spam marketing availability**

RISKS 19 96

Requests for records from the Whois database managed by Network Solutions doubled every 20 days in June and July. Response time began to suffer even after additional hardware was installed. Analysis of the traffic showed that 32% of all the hits came from a single company; it and another top abuser were locked out of the database and response times improved significantly.

Category 33 *Policies, risk analysis, risk management*

1998-09-24 **call screening filter telemarketing answering machine**

EDUPAGE

In the unending battle to foil telemarketers, the Ameritech company announced Privacy Manager, an electronic secretary that intercepts calls placed with caller-ID disabled and electronically demands to know who is calling. If the telemarketers (or anyone) fail to answer, the call is disconnected. Otherwise, the answer is provided to the subscriber for a decision on whether to take the call.

Category 33 *Policies, risk analysis, risk management*

1998-10-04 **spam government international junk e-mail regulation**

EDUPAGE

The British Direct Marketing Association proposed a worldwide opt-out system to cut down on unsolicited commercial e-mail — not for altruistic reasons but to preclude legal bans: "We don't want to ban it because we think that would be closing the door to what could be a very exciting marketing opportunity in the future."

Category 33 *Policies, risk analysis, risk management*

1998-12-14 **spam blacklist unsolicted commercial e-mail UCE crusader ISP**

New York Times
http://www.nytimes.com/library/tech/98/12/biztech/articles/14spam.html

Paul Vixie was profiled in an article published in the December 14, 1999 New York Times. Vixie maintains the Realtime Blackhole List <http://maps.vix.com/rbl/>, a frequently-updated and much-used blacklist of spammers and organization that tolerate or support spammers. ISPs scramble to avoid being on the list. For more information on the fight against spam, see the Coalition Against Unsolicited Commercial Email <http://www.cauce.org/>.

Category 33 *Policies, risk analysis, risk management*

1999-01-05 **e-mail bombs flooding spam autoforwarding mail-storm**

PC Magazine http://www.zdnet.com/pcmag/insites/dvorak_print/jd981208.htm

Famed computer expert and commentator John C. Dvorak warned in one of his opinion columns in PC Magazine that feature-bloat in e-mail programs, trial accounts with ISPs and free e-mail providers were leading to uncontrollable spam and mail-bombing. For example, it was trivially easy to create a new free account, sign up for innumerable news lists with confirmation replies from that account, and then autoforward all the junk to an unsuspecting but soon-overwhelmed victim. Worse still, the victim would be unable to unsubscribe. Dvorak recommended a site for further information on the e-mail threat <http://www.silkroad.com/papers/html/bomb/>.

Category 33 *Policies, risk analysis, risk management*

1999-01-19 **e-mail management policy attachment junk spam waste storm**

PC Magazine http://www.zdnet.com/pcmag/insites/dvorak_print/jd981230.htm

John C. Dvorak wrote in January 1999 that the lack of effective management policy on e-mail usage and storage is leading to a disaster for productivity. It's too easy to send e-mail; people store what they shouldn't; and people get involved in "mail storms" by forwarding message and appending the equivalent of "Me too" just to make their presence known. The author recommended strictly enforced guidelines for efficient use of this communications medium.

Category 33 *Policies, risk analysis, risk management*

1999-01-20 **book spam instructions defense methods techniques**

RISKS 20 17

Alan Schwartz and Simson Garfinkel published _Stopping Spam_ in 1998 (O'Reilly, Sebastopol CA) ISBN 1-56592-388-X. The veteran and respected book reviewer Rob Slade, writing in RISKS 20.17, said, "All ISPs (Internet Service Providers), corporate network administrators, and net help desks should have a copy of this reference handy. Any serious Internet user will also find it well worth the price [U$19.95]."

Category 33 *Policies, risk analysis, risk management*

1999-02-17 **pornography sexual harassment workplace civil liberties**

Atlanta Journal-Constitution

In Decatur, GA, three fire department supervisors were, um, fired when technicians found "inappropriate materials" (arson instructions? incendiary prose? hot porn?) on their computers. The department explained that city policies prohibit sexual harassment; however, the ACLU protested that "mere possession of sexually explicit material does not constitute sexual harassment" and said it might be a violation of free speech rights to prevent an employee from privately viewing such material during spare time on the job." [MK writes: From my point of view, it's the employer's equipment; if some owner wanted to prohibit viewing materials including the letter "e" using their computers, there would be no infringement of anyone's rights unless they were simultaneously ordered to accomplish useful work with those computers.]

Category 33 *Policies, risk analysis, risk management*

1999-02-17 **telephone fraud abuse off-premises extension telco audit inappropriate use employees**

UPI

An article on the UPI news wire (author not listed) on 1999.02.17 noted that an audit of the District of Columbia showed that "more than one third of the 25,000 phone lines billed to the city are actually not being used for District business, costing the city $1.8 million a year." Inspector General E. Barrett Perryman is reported to have said that the "inspectors do not know how the lines ended up in non-city use."

[Comment from MK: Well, those of us who have been in the security field long enough know what's possible. A long-out-of-print book* on telephone fraud pointed out that it is ridiculously easy to generate "off-premises extensions" by fooling telco staff into adding additional numbers to a large account. When no one pays attention to exactly which lines are justified in the monthly bill, the extra lines can go unnoticed for months or years.]

* Haugh, J. J., R. E. Burney, G. L. Dean & L. H. Tisch (1992). _Toll Fraud and Telabuse: A Multibillion Dollar National Problem_. Telecommunications Advisors Inc (Portland, OR). ISBN 0-9632634-2-0. 399 + 431 pp.

Category 33 *Policies, risk analysis, risk management*

1999-02-25 **spam legislation junk e-mail pornography government**

Washington Post, AP

In February, the Virginia legislature passed a law governing unsolicited commercial e-mail (spam). Spammers using forged headers to evade the consequences of their actions would be liable for conviction on a misdemeanor, with fines ranging up to $500. However, if a court decided that the spam was malicious and resulted in more than $2,500 in damages, the offense would become a felony with up to 5 years in prison. In addition, the legislation, which was signed immediately by Governor Jim Gilmore, allowed civil penalties of $10 per message to $25,000 per day. The ACLU vigorously opposed the legislation, arguing on constitutional grounds that it was an unwarranted intrusion on free speech. The ACLU was joined by the Gun Owners of America in its appeal to the governor of Virginia for a veto.

Category 33 *Policies, risk analysis, risk management*

1999-04-15 **employee privacy e-mail monitoring confidentiality**

Wired, AMA http://www.amanet.org/research/monit/index.htm

The American Management Association surveyed 1,054 major US companies on their employee surveillance policies and found that 45% of the respondents monitor e-mail, phone calls and the content of computer files. About 84% of the firms inform their employees of this monitoring. See <http://www.amanet.org/research/monit/index.htm> for details

---

Category 33 *Policies, risk analysis, risk management*

1999-04-29 **privacy e-mail corporate policy dishonesty evidence**

Guardian (London)

Michael Simmonds, head of marketing for the Tory party, leaked a document to the press using e-mail. A copy of the document was found in his electronic out-box and he was fired. Simon Waldman's _Guardian_ article warned that contrary to people's uninformed impressions, e-mail is far from transient; on the contrary, it has a permanence that can exceed that of paper documents. Backups, log files, reconstruction of erased files — any number of mechanisms can make e-mail available to the owners of corporate computer systems. If you don't feel comfortable making an e-mail communication available to your employer, don't write it on corporate computers. In addition, some people's marriages have been wrecked through indiscreet e-mail messages that later came to light; these documents have been introduced into court cases much to the embarrassment of the guilty mates.

Category 33 *Policies, risk analysis, risk management*

1999-06-14 **spam survey study**

USA Today

GartnerGroup surveyed 13,000 e-mail users around the world about their experience with spam. The results were appalling:
* 90% of the respondents received at least one junk e-mail per week;
* 96% of those online for 4 years or more received junk e-mail at least once a week;
* 33% got 6-10 junk messages a week;
* ISPs lose ~7% of their new users every year because of disgust with spam;
* 40% of the respondents agreed that spam should be banned;
* 25% said that spam should be regulated;
* 25% despaired of solving the problem and simply deleted it;
* 3% of the respondents enjoyed it to some extent.

Category 33 *Policies, risk analysis, risk management*

1999-06-24 **anti-spam automated Web site**

New York Times
http://www.nytimes.com/library/tech/99/06/circuits/articles/24spam.html

Julian Haight detests junk e-mail, so he created a useful facility at <http://spamcop.net/> where anyone can submit junk e-mail for automatic followup. The free service parses the spam headers and sends polite e-mail to network administrators warning them about the junk e-mail originating from or being transmitted through their sites. For a modest fee, users can also sign up for an e-mail address that allows automatic filtering of spam and suspected spam, including various levels of severity such as automatic exclusion of e-mail from sites on a blacklist. The users of the free service indirectly help improve the paid service by allowing constant updates of the lists of known spammers. In addition, the site has a page of detailed statistics showing which ISPs and IP addresses are receiving the most e-mail from SpamCop concerning abuse.

Category 33 *Policies, risk analysis, risk management*

1999-11-30 **inappropriate use fired termination employee policy e-mail**

AP, Washington Post http://www.washingtonpost.com/wp-srv/aponline/19991130/aponline1 93057_000.htm

More than 20 employees at the Norfolk, VA Shared Services Center of the New York Times were fired at once when management determined that they had sent "inappropriate and offensive" e-mail on company systems.

Category 33 *Policies, risk analysis, risk management*

1999-12-06 **appropriate use policy termination e-mail**

Information Security Magazine Security Wire, Washington Post 1 9
http://www.washingtonpost.com/wp-srv/aponline/19991130/aponline193057_000.htm

In late November, the New York Times Company fired 23 employees from its administrative services center in Virginia for violating its e-mail policies. No details were released other than to note that the problem involved inappropriate and offensive e-mail.

33.1 Acceptable use policies

Category 33.1 *Acceptable use policies*

1997-06-05 **appropriate use net filter productivity Internet Web**

EDUPAGE

A recent thesis on employee use of the Web for entertainment while being paid for work suggests at least a couple of hours of productivity per week down the tubes. Other more informal estimates range from 5% to 40% lost time. In addition, such goofing-off consumes network resources; pornography and games take up a lot of bandwidth.

Category 33.1 *Acceptable use policies*

1997-08-11 **Internet browsing policy law monitoring prosecution**

PA News

Barclays Bank reported its own employees to the British police after staff were found downloading pornography from the Internet.

Category 33.1 *Acceptable use policies*

1998-01-25 **push pull technology distributed computing**

EDUPAGE

According to EDUPAGE, an October Air Force memo stated that "Effective immediately, all commercially available auto push-pull data gathering applications ... are to be disabled from all networks. Currently, these technologies introduce security risks and impact data throughput on our networks than cannot be tolerated." Makers of PointCast News and other similar products protested that their software is safe.

Category 33.1 *Acceptable use policies*

1998-02-01 **cookies privacy law appropriate use public officials**

EDUPAGE, BENTON, AP

In Tennessee, a newspaper publisher in Cookeville is suing the town administration, demanding to see the cookies.txt files on municipal employees' PCs. The publisher wants to see if civil servants are wasting tax dollars surfing the Net with taxpayers' resources.

Category 33.1 *Acceptable use policies*

2000-02-19 **e-mail privacy policy openness awareness conflict monitoring ownership**

InformationWeek

Thomas York summarized the state of e-mail privacy in an article for InformationWeek in February 2000. He cited a case that made news in November 1999 when the New York Times fired 23 workers in its Norfolk, VA support office for distributing offensive jokes through corporate e-mail. Despite the cries of protest from free-speech advocates, corporate America is increasingly making it clear to employees what has always been true: that corporate e-mail systems and the message that flow through them are company property. However, observers comment that it is unreasonable to bar all personal messages from the systems, especially when employers are glad to see staff working unpaid overtime. The essential rule is that employees must be aware that their communications are being monitored. In addition, employees can use outside e-mail systems (assuming they can get through company firewalls) for more privacy.

Category 33.1 Acceptable use policies

2000-03-10 **appropriate use management policy tools**

NewsScan, MSNBC http://www.msnbc.com/news/380471.asp

As employers increasingly worry about how to maintain control over workers' use of the corporate network for personal activities, such as e-shopping, or pornography perusal, a half-billion-dollar industry is taking off. Dubbed EIM, or employee Internet management, the new field comprises companies that make everything from Web filtering software to programs that track a worker's every keystroke. According to a new International Data Corp. white paper, Internet access control software was a $63-million market last year, and is expected to evolve into a $562-million EIM market by 2004. Currently, "660,000 companies are interested in buying these products," says IDC research director Chris Christiansen. Among those companies is Marriott International, whose senior technical analyst Scott Davis says, "Streaming medias are chewing up a lot more bandwidth than the HTTP protocol did in the past, and we have the HR departments and the corporate policy departments coming to us and telling us the (Internet) policy to implement." Policing those policies is increasingly difficult without adequate EIM software, he adds. (ZDNN/MSNBC 10 Mar 2000)

Category 33.1 Acceptable use policies

2000-04-25 **e-mail expectation of privacy monitoring intrusion employers employees labor relations government board regulations laws**

NewsScan

Many companies now monitor their employee's e-mail and Web activities, assuming they have the inalienable right to ban personal or inappropriate use of office PC. But rebellious workers are now fighting back, using the National Labor Relations Act, a Depression-era law that sired the National Labor Relations Board (NLRB). The quasi-judicial NLRB, which protects workers' rights to organize and communicate freely with each other about work terms and conditions, has weighed in on the employee's side in several recent cases involving workplace electronic monitoring activities. In one case, an employee fired for not apologizing over an e-mail he wrote criticizing a new vacation policy was granted back pay and a chance to rejoin his old firm (he took the pay but refused the job). In another, Pratt & Whitney was forced to back off a total ban on using the office e-mail system for non-business purposes. "The way people work is changing dramatically," says NLRB associate general counsel Barry Kearney. To keep up with the times, the NLRB is now asking branch offices to forward to Washington headquarters any cases involving e-mail or Web use by employees. (Wall Street Journal 25 Apr 2000)

Category 33.1 Acceptable use policies

2000-06-20 **intellectual property peer-to-peer access censorship surveillance filtering monitoring**

NewsScan, San Jose Mercury News
http://www.sjmercury.com/svtech/news/breaking/merc/docs/044058.htm

Universities are struggling over the issues posed by Napster software, which allows people to make unauthorized copies of music. At a University of Southern California forum yesterday, attorney Cara Burns took a dim view of the idea of letting students use university facilities to steal copyrighted material: "There are certain cases when the university has to act as Big Brother. Is that what you send your kids to university for — to download music? ... I am for new technology, but I'm also for artists and artists' right. Napster to me has more to do with stealing. Artists have the right to control their music." Taking a difference approach, USC chief information officer Jerry Campbell argued: "There is a serious principle involved here. We do not censor access... Trying to solve the problem in the courts is just stalling for time. Technology will not be rolled back by any law." (AP/San Jose Mercury News 20 Jun 2000)

Category 33.1 Acceptable use policies

2000-07-11 **privacy executive corporate title officer position responsibilities policy**

NewsScan, San Jose Mercury News
http://www.sjmercury.com/svtech/news/breaking/merc/docs/032861.htm

A new executive position is showing up on the organization charts of companies such as American Express, Citigroup, Prudential, and AT&T: the Chief Privacy Officer, who has broad powers to protect the privacy of consumers who interact with corporate computer systems. George Washington University professor Lance Hoffman says that the new position "attracts people who have a knowledge of history and law. They know something about technology, and they can't get techno-dazzled by explanations that don't hold water. They appreciate what technology can do for good and for evil." (AP/San Jose Mercury News 11 Jul 2000)

Category 33.1 *Acceptable use policies*

2000-09-19 **appropriate use contract regulations agreements online auctions taste obscenity restrictions**

NewsScan, USA Today http://www.usatoday.com/life/cyber/tech/cti549.htm

Online auctioneer eBay has stopped the sale of an autopsy picture and crime scene photographs of three slain boys. A company executive said, "This was the first time a crime scene photo of a minor had been placed on eBay. It was also the first time, that we are aware of, of a coroner's photo being placed on the site. " He added: "We are dealing with some very tough issues because a lot of this type of merchandise is readily available in other arenas. We are also looking at a lot of legal issues involving the rights of people to sell things." But an attorney for the organization Parents of Murdered Children said: "We're not talking First Amendment, we're talking good taste," he said. (AP/USA Today 19 Sep 2000)

Category 33.1 *Acceptable use policies*

2000-10-01 **intellectual property IP copyright violations infringement music academia universities colleges peer-to-peer appropriate-use policy bandwidth saturation availability academia universities colleges policy**

NewsScan, Los Angeles Times
http://www.latimes.com/business/20000831/t000081672.html, San Jose Mercury
News http://www.sjmercury.com/svtech/news/breaking/ap/docs/465588l.htm

A report by the Gartner Group . . . [said] 17 out of 50 — about a third — U.S. colleges and universities surveyed have banned students from using Napster on their campuses. Gartner says the song-swapping service is raising a number of moral and legal issues for school administrators, who are hurrying to establish policies regarding digital music sharing before campuses open for the fall session. Among colleges still allowing Napster use are Columbia, Harvard and Stanford, while New York and Kent State universities have instituted bans. (Los Angeles Times 31 Aug 2000)

Colleges and universities are split on "the Napster issue." Some are blocking Napster, some are not. Among the ones that are not are Georgia Tech, Michigan, Stanford, Duke, and the University of California at Berkeley. A Georgia Tech official says: "We are an educational institution and we will err on the side of unfettered access to information. Once you start down that road ... well, we could tie up an awful lot of staff people and resources trying to evaluate Web sites' content, and we don't want to get into that." Among the ones that are blocking Napster are Yale, Indiana, Southern California, Texas, Ohio State, Northeastern, and Canisius. The first three in this group made their decisions after being sued by two rock groups and the Recording Industry Association of America; the second two chose to block Napster on the grounds that Napster traffic clogged their computer networks; and the last two cited legal and ethical reasons for rejecting Napster and similar programs. A Canisius official explained: "It's not free for you to steal books from the public library, and it's not free to download music you haven't paid for." (AP/San Jose Mercury News 1 Oct 2000)

Category 33.1 *Acceptable use policies*

2000-11-12 **appropriate use monitoring covert channel chat**

NewsScan, Excite http://news.excite.com/news/ap/001112/00/cia-naughty-chat

Although their "misuse of computers" did not compromise any classified information, 160 employees of the Central Intelligence Agency are being investigated for exchanging off-color messages on a private chat room that had been set up covertly on the Agency's classified internal network. One CIA official said that if those agents who created the covert communications facility had put it on the KGB's system "we'd be giving them medals," but that "sadly, it was ours." (AP/ExciteNews 12 Nov 2000)

Category 33.1 *Acceptable use policies*

2000-12-20 **covert channel confidentiality unaware social engineering detailed information auto-reply abuse danger vulnerability**

RISKS 21 16

Dan Birchall wrote an excellent piece for RISKS about the dangers of inadvertently revealing too much information by creating an overly-explicit auto-response for e-mail when one is away from the office. As he pointed out, a detailed message may be OK for close colleagues but wholly inappropriate for publication; for example, "I will be away from [government laboratory] from [departure date] and will return on [return date]. If you need to reach someone from the IT Security staff, Please contact [coworker] at [number] or e-mail to [address]." Such a message is far too revealing for strangers, some of whom may be interested in competitive intelligence (e.g., which conferences you are going to) and others who may be hackers or industrial spies interested in social engineering. Subscribers to e-mail distribution lists may not realize that their autoresponder messages are going to total strangers. Birchall concluded, "send something like this:
>I am currently away from work. If you need to reach someone, please contact John <jsmith> at 555-1212.<
The logic, of course, is that an authorized person already knows where you work, what you do, your e-mail domain, and your area code. Nobody needs to know how long you'll be gone, if there's someone else who can help them."

Category 33.1 *Acceptable use policies*

2001-03-19 **availability saturation e-mail overuse acceptable use**

NewsScan

WASHINGTON FLOODED WITH E-MAIL
U.S. lawmakers last year received 80 million e-mail messages from constituents and special-interest groups, most of which were routinely ignored, according to new study by the Congress Online Project. The number of e-mail messages to Congress has more than doubled in two years, says the group, with senators receiving as many as 55,000 messages per month. And while millions of the messages originate from constituents concerned about Medicare reform, tax cuts and other issues, the study attributed the e-mail explosion in large part to advocacy groups and corporations that increasingly use the Internet to lobby lawmakers day and night, overloading congressional computers and staff. "Rather than enhancing democracy--as so many hoped--e-mail has heightened tensions and public disgruntlement with Congress," says the report. "A growing number of citizens are increasingly frustrated by what they perceive to be Congress' lack of responsiveness to e-mail. At the same time, Congress is frustrated by what it perceives to be e-citizens' lack of understanding of how Congress works." The study urges grassroots lobbyists to adopt a "code of conduct" to curb mass e-mailings to lawmakers and also suggests the federal government to provide lawmakers with additional resources so they can buy new software and hire staff to answer electronic messages. According to the study, it could cost each office $50,000 or more for hardware and software. (Reuters/CNet 18 Mar 2001)
http://news.cnet.com/news/0-1005-200-5173083.html?tag=lh

Category 33.1 *Acceptable use policies*

2001-04-06 **e-mail posting publication confidentiality stock damage information warfare sabotage appropriate use stupidity**

RISKS 21 34

Accordint to a report from the BBC < http://news.bbc.co.uk/hi/english/world/americas/newsid_1263000/1263917.stm >, "A chief executive who used an e-mail to threaten his staff with the sack for being lazy has seen his company's share price collapse after the message appeared on the Internet. Neal Patterson, head of the Cerner Corporation in Kansas City, USA, had no idea his private directive to staff would end up being seen by millions of people on the world wide web. In the three days after the publication of the message, shares in the healthcare software development company plummeted 22% on the stock market."

RISKS correspondent Lord Wodehouse wrote, "It never ceases to amaze me that people armed with a computer and e-mail completely lose their common sense. However it seems to the the type of e-mail that should never have been written let alone sent and not by a senior person in the company. Gerald Ratner built up the family business, piling it high, selling it cheap and making a fortune out of cut-price jewelry. But a throw-away joke in a speech at the Royal Albert Hall in front of Chancellor Norman Lamont brought his empire crashing down around his ears. (he called a item he sold cr*p.) With the Internet the inept director can find that it is even easier to ensure that bad news travels faster and further."

Category 33.1 *Acceptable use policies*

2001-08-31 **Internet chat room hate speech censorship lawsuit ISP Internet Service Provider**

NewsScan

MUSLIM LAWSUIT AGAINST AOL CHARGES "HATE SPEECH" TOLERANCE [31 Aug 2001]
A class-action lawsuit has been filed in Alexandria, Virginia, charging America Online with violating the 1964 Civil Rights act by failing to curtail anti-Muslim "hate speech" in chat rooms for Muslims. An attorney for the Muslim plaintiffs says that the primary objective is to get AOL to enforce the terms of its own service agreement , which prohibits member s from using "offensive" speech in any of AOL's 14,000 chat rooms. An America Online executive calls the lawsuit "totally without merit" and says that the company has "zero tolerance for hate speech." (AP/USA Today 31 Aug 2001)
http://www.usatoday.com/life/cyber/tech/2001-08-31-aol-suit.htm

---

Category 33.1 *Acceptable use policies*

2001-09-20 **monitoring logging confidentiality privacy Internet abuse appropriate use policy**

NewsScan

JUDGES TOLD THEY CAN'T REFUSE TO HAVE THEIR COMPUTERS MONITORED [14 Aug 2001]
In mid-September a policy-making group of 27 judges will decide whether to accept the recommendations of a report urging denial of one court's request to put an end to the monitoring of its computers for Internet misuse. One observer says: "When the courts find themselves as not the arbitrators but the victims of such a policy, all of a sudden you find judges saying 'this could very well be a violation of our rights.' Now the judges are beginning to understand how difficult this has been for the private sector so long." The judge who objects to the monitoring says it should be used to prevent vandal attacks by outside hackers, and not focused on internal computer uses. (AP/San Jose Mercury News 14 Aug 2001)
http://www.siliconvalley.com/docs/news/svfront/060305.htm

COURTS AFFIRM RIGHT TO PRIVACY FOR JUDGES AND STAFFS [20 Sep 2001]
In a move that is likely to set a precedent that could lead to stronger privacy protections for employees nationwide, the 27-judge Judicial Conference of the United States Courts agreed to a computer-use policy that drops language in an earlier draft saying that the nation's 30,000 court employees had no right to privacy when they used the Internet. The final version merely states that the court computers should be used largely for work, and not for viewing pornography, gambling, or exchanging media files for personal use. (Reuters/New York Times 20 Sep 2001) http://www.nytimes.com/2001/09/20/national/20JUDG.html

---

Category 33.1 *Acceptable use policies*

2001-10-15 **acceptable use corporate policy bandwidth saturation throughput availability denial of service streaming audio video employees survey study**

NewsScan

RECORD NUMBER OF OFFICE WORKERS ACCESS STREAMING MEDIA
A record number of U.S. office workers took advantage of their corporate networks' high-speed Internet connections to access streaming audio or video media last month, including media from foreign countries. In most cases, people were trying to follow news related to last month's terrorist attacks. More than half (55.8%) of all employees who logged on from work last month watched or listened to streaming media, up from 50% in August, according to Nielsen/NetRatings. The previous record was set in November 2000, when 52.8% of office employees accessed streaming media while at work. Among the three formats available for streaming media, the most popular was RealNetworks' RealPlayer, followed by Microsoft's Windows Media and Apple's QuickTime. "What we saw starting with (Sept.) 11th was an unprecedented amount of ... live usage and an unprecedented amount of broadband-video usage" that continued through the month, said RealNetworks media manager Ben Rotholz. (Wall Street Journal 15 Oct 2001)
http://interactive.wsj.com/articles/SB1002819156270229840.htm

---

Category 33.1 *Acceptable use policies*

2001-11-18 **content filtering edit selection private control censorship Web discussion board chat room**

NewsScan

MONITORING THE MESSAGE BOARDS [18 Nov 2001]
With the U.S. at war with terrorism, various Web services are choosing to decline submissions from people saying the country "deserved" to be attacked or making other comments along those lines. Stephen Killeen of Terra Lycos U.S. says that, in the past, "we would err on the side of `If it's distasteful, let it stay.' Now, we err on the side of `If you want to post this kind of information, you don't have to do it here.' The sentiment in the United States changed on Sept. 11 about what's acceptable and what's not in terms of what you can say." Of course, people are free to set up Web sites of their own and post whatever they want, just as private companies are free to accept or reject anything they want. UCLA law professor Stuart Biegel says, "In times of war, there has been a willingness among Americans to give up some rights -- to honor curfews, martial law, and even restrictions on speech. The filtering of Internet message boards is part of all this." (San Jose Mercury News 18 Nov 2001)
http://www.siliconvalley.com/docs/news/svfront/censor111801.htm

---

Category 33.1 *Acceptable use policies*

2002-01-20 **Internet content filtering students schools portable games music piracy instant messaging appropriate use policy**

NewsScan

VIRGINIA COUNTY RECALLS STUDENT LAPTOPS [20 Jan 2002]
Henrico County, Va. school officials are recalling all 11,000 laptop computers that it distributed to its high school students in order to retrofit them with security software that will prevent students from using the devices for accessing pornography or changing their grades -- abuses that reportedly have occurred since the machines were handed out last fall. Game and music downloading capabilities will also be eliminated or heavily restricted and instant messaging will be limited to home use. Teachers have complained that in-class use of entertainment file-sharing and messaging are disruptive. (AP/Wall Street Journal 20 Jan 2002)
http://interactive.wsj.com/articles/SB101156380380877324O.htm

---

Category 33.1 *Acceptable use policies*

2002-03-22 **e-mail user interface management reliability productivity**

NewsScan

A GOOSE AND GANDER STORY: AOL TIME WARNER WORKERS HATE AOL MAIL SYSTEM
When AOL and Time Warner merged, executives of the new company required the divisions of the old Time Warner to adopt AOL mail system for internal use throughout the new company. But now that policy has been reversed, because managers and employees complained bitterly that AOL's consumer-oriented system is unfit for serious business use, maintaining that the software crashes, messages can't handle large attachments, communications sent to large groups of people are mis-identified as spam and thrown away, and so forth. Staffers in Time's Washington bureau apparently began to mock the AOL mail system by singing out, "So easy to use, no wonder it's number one." So employees began relying less on e-mail and more on other forms of communication. One staffer said, "If all goes well, we'll never have to use e-mail and we'll start talking to each other again." (Wall Street Journal 22 Mar 2002)
http://www.online.wsj.com/ (sub req'd)

Category 33.1 *Acceptable use policies*

2002-03-28 **free speech property e-mail corporation employee lawsuit SCOTUS**

NewsScan

CALIFORNIA CASE PITS SPEECH RIGHTS VS. PROPERTY RIGHTS
The California Supreme Court has agree to review a case involving a disgruntled Intel employee who sent 30,000 e-mail messages to company employees at their places of work. The employee, backed by the American Civil Liberties Union and the Electronic Frontier Foundation, sees the case as one raising fundamental free speech rights denied to an individual who wished to circulate his opinion; in contrast, the lower courts have viewed it as a property-rights case, since the messages were sent not to employees at their homes but to their company e-mail addresses. The appellate court's majority ruled that "Intel is as much entitled to control its e-mail system as it is to guard its factories and hallway." A dissenting opinion argued that it could be considered a property-rights case only if Intel had shown that its property had actually been harmed, and there was no such showing. (San Jose Mercury News 27 Mar 2002)
http://www.siliconvalley.com/mld/siliconvalley/2948781.htm

Category 33.1 *Acceptable use policies*

2002-08-02 **e-mail content inspection limits regulations rules employee employer policy suitability**

NewsScan

LAWSUIT OVER CONTENT OF EMPLOYEE E-MAIL
The Virginia-based nonprofit American Center for Law and Justice has filed a lawsuit against a Dallas school district over its policy restricting the content of employee e-mail messages. The policy allows employees to send "work-related" or "private" messages -- but does not allow "religious worship" or "proselytizing." The suit is being filed on behalf of a female employee who was threatened with having her e-mail privileges suspended after she sent e-mail with religious content to her friends. (AP/San Jose Mercury News 1 Aug 2002)

Category 33.1 *Acceptable use policies*

2002-08-30 **availability prompt response policy e-mail customer relations management CRM**

NewsScan

COMPANIES LAX ON ANSWERING E-MAIL
Companies' efforts to shift customer relationship management to the Web and e-mail may backfire unless they institute a prompt response mechanism, says a new study by Jupiter Research. Only half of the companies surveyed responded to a customer's question or issue within 24 hours, while a third took three days or longer. "That lack of response could drive consumers back to more costly channels such as the telephone," says Jupiter analyst David Daniels. "Consumers are definitely concerned about this." And while self-service is catching on with consumers savvy enough to navigate their way through a Web site, companies should be cautious about relying on it too heavily. "Self-service really lends itself to commodity goods categories (like books or CDs). When it gets up into more complicated situations, such as computing products or wireless phones, consumers absolutely said they want a real-time solution. Those frequently-asked-question lists are not necessarily specific enough to meet their needs," says Daniels. (CNet News.com 29 Aug 2002)
http://news.com.com/2100-1017-955947.html?tag=fd_top

Category 33.1 *Acceptable use policies*

2002-10-25 **copyright intellectual property piracy corporate policy**

NewsScan

HOLLYWOOD GOES TO WORK TO STOP DIGITAL PIRACY
Hollywood studios and record companies are asking the heads of U.S. corporations to prevent their employees from using high-speed company networks to download copyrighted material from peer-to-peer services such as Kazaa and Gnutella which are used to exchange songs and movies. The letter sent by these groups suggests that businesses could be held liable for the copyright infringements made by their workers. (Reuters/USA Today 25 Oct 2002)

Category 33.1 *Acceptable use policies*

2002-11-26 **university policy copyright infringement intellectual property student seizure**

NewsScan

NAVAL ACADEMY SEIZES STUDENT COMPUTERS FOR ILLEGAL COPYING
The U.S. Naval Academy in Annapolis, Maryland, has seized about one hundred student computers it suspects were used to receive illegally downloaded music and movies. Guilty students could receive punishments ranging from loss of leave time to court-martial and expulsion — far stricter punishments than are meted out to civilian students who are not charged with misusing federal property. It is not uncommon for students to be oblivious, indifferent, or positively hostile to the notion that it is wrong to steal copyrighted material. One student at an east-coast university says of music and video file-copying, "This is a lot better deal than going out and spending $15 for twenty other tracks on a CD you don't want. It takes you 5 or 10 seconds to type in. There's no risk, and it's one of those things where you don't see the victim." (Washington Post 26 Nov 2002)

Category 33.1 *Acceptable use policies*

2003-01-24 **Internet access office work appropriate use economics**

NewsScan

CRACKDOWN ON OFFICE SURFING COULD AFFECT WEB PROFITS
Office workers with corporate broadband networks have long enjoyed high-speed access to online entertainment, shopping and other personal pursuits, but a widespread crackdown on non-work-related Internet use may be looming, driven by cost-cutting efforts and increased scrutiny of workers' surfing habits. "I think it was an issue of productivity — people were spending too much time on these sites. I know people who were bidding on eBay all day long," says one office worker who admits to logging on to online dating sites several times a week. According to Websense, an estimated $85 billion in productivity is lost annually to workers wasting time on the Net. But the corporate backlash is bad news for Web sites courting broadband users at a time when nearly 87% of people accessing the Net from work are using a broadband connection, compared with about 28% from home. Companies that stand to lose from the crackdown include game sites like "The Sims," e-commerce hot spots like eBay, online dating sites like Matchmaker.com, and news and entertainment outlets offering rich media formats such as video and audio clips. "Given that about 40% of the activity (in many of these areas) is coming from work, if (blocking) became a pervasive practice in the workplace, it would impact the business," says a Bear Stearns analyst. A network performance analyst at a Fortune 10 company argues that companies have to take steps to protect their network resources: "If you're looking at a company with an $82 million IT budget, and 10% of the network is going to nonwork uses, you're saving $8 million if you can stop it." (CNet News.com 24 Jan 2003)

Category 33.1 *Acceptable use policies*

2003-02-06 **appropriate use productivity work telecommuting Internet access home**

NewsScan

PEOPLE WHO PLAY AT WORK, WORK AT HOME
What employers lose in productivity when workers goof off, bidding on eBay and circulating jokes, is made up in the home, according to a survey by the University of Maryland and Rockbridge Associates. The study found that employees with Web access both at home and at work spend an average of 3.7 hours a week doing personal online chores in the office. Those same employees, however, spend an average of 5.9 hours a week at home catching up on work. "I think what this says is the Internet is actually helping business productivity," says Roland Rust, director of the Center for eService at the U. of Md.'s Robert H. Smith School of Business. Rust warns that, based on his findings, employers should think twice about banning personal online activities in the office. (Wall Street Journal 6 Feb 2003)

Category 33.1 *Acceptable use policies*

2003-02-13 **copyright intellectual property piracy violations guide policy employers corporations**

NewsScan

FILM, MUSIC GROUPS TARGET WORKPLACE PIRATES
The Recording Industry Association of America and the Motion Picture Association of America have published a guide for employers, asking major corporations to curb illicit file-swapping by workers on company time. The guide, titled "A Corporate Policy Guide to Copyright Use and Security on the Internet," requests that businesses advise employees against copyright abuse using corporate computer systems and warns that such abuse is illegal, damages corporate reputations, increases corporate network security risks, and can put organizations at risk of legal liability. The guide cites a case in which an Arizona company paid a $1 million settlement in April 2002 to the RIAA after workers were found to be accessing and distributing thousands of music files via the company server. (Reuters 13 Feb 2003)

Category 33.1 *Acceptable use policies*

2003-03-14 **copyright intellectual property rights education awareness**

NewsScan

INTERNET BOOKENDS: #1, KAHN ON COPYRIGHT
Internet co-founder (with Vint Cerf) Bob Kahn is head of the Corporation for National Research Initiatives (CNRI), which he founded in 1986. In an interview with John Gehl for the ACM online publication Ubiquity, Kahn talks about the state of the Internet, including the need for more education about copyright law: "We [at CNRI] have been promoting copyright and, more generally, intellectual property protection in the network probably as much as anybody in the research world. CNRI built a system for the U.S. Copyright Office to manage the registration of copyright claims and the attendant submission of copyright information and digital objects online; the system is called CORDS (cords.loc.gov). In my view, one of the problems that has not been satisfactorily dealt with in this country is the widespread lack of respect for the value of intellectual property. People think that they can do anything they want with intellectual property just because they themselves don't happen to see any cost associated with accessing it on the net and, perhaps sending it to others or otherwise using it. I think this is clearly an educational issue as much as it is a constitutional issue." (Ubiquity 13 Mar 2003)
http://www.acm.org/ubiquity/interviews/r_kahn_1.html

Category 33.1 *Acceptable use policies*

2003-03-18 **copyright infringement intellectual property workplace piracy monitoring employers liability**

NewsScan

RECORD LABELS WARN COMPANIES OF 'SIGNIFICANT LEGAL DAMAGES'
The Recording Industry Association of America has sent letters to about 300 companies, informing them that their computers were being used by workers for illegal file-swapping and threatening "significant legal damages" for employers and employees alike. The new tactic is the RIAA's first systematic effort to tackle digital music piracy that occurs using corporate networks, following a similar effort to enlist universities in the fight against illegal file-sharing. Copyright law experts said companies might be liable for piracy on their networks if they know about it and don't intervene, but it's unclear whether companies have an obligation to police their networks and remove unauthorized copies of songs without being asked to. "I think what they're trying to do is get people thinking 'Gee, I'm in this gray area, and I don't want to be the guy who gets fingered for the test case,'" says one intellectual property attorney. "As a corporation, do you really want to be in the news defending the right of your employees to have pirated music on your network?" About 35% of the letters went to information technology companies, 20% to healthcare firms, 20% to manufacturers, and the rest to miscellaneous industries. (Los Angeles Times 18 Mar 2003)

Category 33.1 *Acceptable use policies*

2003-03-26 **pornography library government computer usage trial**

NewsScan

LIBRARY PORN CASE GOES TO TRIAL

A group of librarians in the Minneapolis library system has filed a federal lawsuit against that system, alleging that administrative failures have created an intimidating, hostile and offensive workplace. "We were living in hell, and they were unwilling to acknowledge the problem," says one librarian. The dispute arose in 1997, soon after the Minneapolis libraries installed Internet access, and a number of library visitors began displaying on publicly accessible computer images of "virtually every imaginable kind of human sexual conduct." (AP/USAToday 26 Mar 2003)

Category 33.1 *Acceptable use policies*

2003-04-22 **copyright infringement University Pennsylvania student accounts revoked**

NewsScan

PENN STATE PULLS THE PLUG ON STUDENTS' ACCOUNTS
Pennsylvania State University has suspended the Internet accounts of about 220 students after investigations showed they were using the school's broadband network to trade in "publicly listed copyright infringing materials." The school said connections will be restored once the copyrighted files have been removed from the systems. The move came about a month after the school had issued a warning to its 110,000 students, alerting them that illegal trading of copyrighted materials was against the law, and just weeks after the Recording Industry Association of America slapped four students at Rensselaer Polytechnic Institute, Princeton University and Michigan Technological University with lawsuits. (Internet News 22 Apr 2003)

Category 33.1 *Acceptable use policies*

2003-09-12 **state workers e-mail privacy publicity pubilc documents private business venture first amendment advocates**

NewsScan

STATE WORKERS' PRIVATE E-MAIL IS PRIVATE
The Florida Supreme Court ruled Thursday that state workers' private e-mails cannot be treated as public documents just because they are created or stored on government computers. The ruling came in a case brought by the St. Petersburg Times, which had sued the city of Clearwater for access to the e-mail records of two city employees who had exchanged messages regarding a private business venture. The city allowed the workers to determine which e-mails should be made public, a decision challenged by the newspaper and First Amendment advocates. Florida Attorney General Charlie Crist expressed disappointment with the ruling: "If the taxpayers pay for the computers, they ought to have the right to see what's on them." St. Pete Times attorney George Rahdert noted that the 1967 law covering public records was written before electronic communications were commonplace. "The problem is public records law is kind of paper-bound. It doesn't really account for the way that people are communicating important information." (St. Petersburg Times 12 Sep 2003)

Category 33.1 *Acceptable use policies*

2003-10-03 **peer-to-peer copyright infringement file-sharing University of Florida**

NewsScan

U. OF FLORIDA PULLS THE PLUG ON P2P USERS
Students returning to the University of Florida this fall have discovered a new utility on the school network: Icarus (Integrated Computer Application for Recognizing User Services), a open-source program developed by campus personnel to thwart students' obsession with peer-to-peer file-sharing. Last spring, the university received about 40 notices of copyright violations per month and at peak times 90% of all the traffic on the housing network was P2P. "We needed something to stem the flow. We were spending too much time tracking people down," says Robert Bird, supervisor of network services for UF's housing department, who reports that the debut of Icarus has reduced P2P use by 90%. When students first register on the UF network, they must pledge not to share copyright files. Icarus then scans their computer, flags any worms, viruses or file-sharing software, and gives instructions on how to disable those programs. First-time offenders receive a pop-up warning and are disconnected from the campus network for 30 minutes, but a repeat performance results in being disconnected for five days. Third-time violators are subject to the school's judicial process and are cut off form the network indefinitely. The new system has some students grumbling, but most seem resigned to the new restrictions. "While file-sharing is nice, it's not worth risking college or your future," says one. (Wired.com 3 Oct 2003)

Category 33.1 *Acceptable use policies*

2003-11-05 **personal surfing good thing increase productivity lower stress**

NewsScan

PERSONAL SURFING AT WORK CAN BE A GOOD THING
Here's a new book that turns conventional wisdom about personal surfing on company time on its head. Claire Simmers and Murugan Anadarajan have co-authored a human resources guide to worker Web use that indicates a looser attitude toward personal surfing can yield some beneficial side effects. "Personal Web usage in the workplace has a negative perception, especially among administrators who often see it as inefficient and creating a decrease in work productivity," says Simmers. But according to the authors' research, personal surfing at work can result in better time management, lower stress levels, improved skill sets and a happier balance between work and personal life. (AP 5 Nov 2003)

Category 33.1 *Acceptable use policies*

2004-10-25 **survey mp3 Australia cost appropriate use office policy bandwidth waste productivity**

NewsScan; http://australianit.news.com.au/articles/0

WORK MP3s ARE A $AU60M PROBLEM

Office workers downloading files to build music and video collections cost Australian businesses $AU60 million a year, a new survey has found. Exinda Networks, a Melbourne-based supplier of network management and monitoring systems, collated recent data from the Australian Bureau of Statistics and one of the nation's largest private Internet service providers, covering around 10,000 online users. Australian businesses, which spend a total of $AU450 million a year in Internet costs, were forking out an estimated $AU4.9 million a month for employees' music and video files, the study found. This was the equivalent of one million MP3 files daily and does not include lost productivity costs. (The Australian 25 Oct 2004)

Category 33.1 *Acceptable use policies*

2005-02-11 **blog weblog work fire employment termination judgement courtesy foolish stupid rude crude crass insulting anonymous consequences pseudonym journalist criticism sarcasm appropriate use**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A15511-2005Feb10.html

BLOGGING WHILE YOU WORK: MAYBE NOT A GOOD IDEA

Using the pseudonym "Sarcastic Journalist," reporter Rachel Mosteller of the Durham (N.C.) Herald-Sun newspaper wrote this entry on her personal blog one day last year: "I really hate my place of employment. Seriously. Okay, first off. They have these stupid little awards that are supposed to boost company morale. So you go and do something 'spectacular' (most likely, you're doing your JOB) and then someone says 'Why golly, that was spectacular.' then they sign your name on some paper, they bring you chocolate and some balloons... Okay two people in the newsroom just got it. FOR DOING THEIR JOB." The day after her posting, Sarcastic Journalist was fired (even though it did not identify the newspaper in her posting). Lee Rainie, director of the Pew Internet & American Life Project, comments: "We all complain about work and our bosses. And the ethos of the blogosphere is to be chatty and sometimes catty and crude. Even in an era of casual Fridays, that is not what companies want to be portrayed by the world." And labor lawyer Gregg M. Lemley notes: "In most states, if an employer doesn't like what you're talking about, they can simply terminate you." (Washington Post 11 Feb 2005)

Category 33.1 *Acceptable use policies*

2006-03-10 **employment law file deletion company laptop undelete secure wipe lawsuit criminal hacking unauthorized**

RISKS; CNET news.com http://tinyurl.com/ne3xx 24 20

USING SECURE WIPE UTILITY LEADS TO LAWSUIT FOR HACKING

Declan McCullagh summarized an interesting interpretation of law that occurred in the US Court of Appeals for the 7th Circuit in March 2006. It seems that Jacob Citrin used to work for International Airport Centers. He quit and returned his laptop computer to them. They prepared to sue him for allegedly violating his employment contract by going to business for himself in the same field. When they searched his hard drive looking for juicy files to undelete as part of their preparation for the civil case, they discovered that he had wiped files rather than deleted them: the old files were unrecoverable. So they accused him of violating 18 USC §1030, the Computer Fraud and Abuse Act of 1986.

McCullagh wrote:

>That law says whoever "knowingly causes damage without authorization" to a networked computer can be held civilly and criminally liable.

The 7th Circuit made two remarkable leaps. First, the judges said that deleting files from a laptop counts as "damage." Second, they ruled that Citrin's implicit "authorization" evaporated when he (again, allegedly) chose to go into business for himself and violate his employment contract.

The implications of this decision are broad. It effectively says that employees better not use OS X's Secure Empty Trash feature, or any similar utility, because they could face civil and criminal charges after they leave their job. (During oral argument last October, one judge wondered aloud: "Destroying a person's data--that's as bad as you can do to a computer.")

Citrin pointed out that his employment contract permitted him to "destroy" data in the laptop when he left the company. But the 7th Circuit didn't buy it, and reinstated the suit against him brought by IAC.<

33.2 Spam, spim, spit & splogs

Category 33.2 *Spam, spim, spit & splogs*

1997-06-12 **spam FTC fraud spoof address headers fines regulation**

AP

The FTC warned spammers that fraudulent return addresses on junk e-mail and outright scams being advertised through unsolicited e-mail could result in injunctions and fines up to $10,000 per incident for repeat offenders. The Commission invited consumers to contribute information about fraudulent junk e-mail. See <http://www.ftc.gov/> for information about the FTC and send copies of junk e-mail that has fraudulent headers or reply-to entries and some physical address to <consumerline@ftc.gov>.

Category 33.2 *Spam, spim, spit & splogs*

1997-06-15 **spam FTC fines regulations**

EDUPAGE

The FTC announced that some of the flood of spam annoying e-mail users is fraudulent, and the Commission intends to find and punish such spammers. Some estimates of spam suggest that up to 30% of the e-mail entering AOL every day is spam.

Category 33.2 *Spam, spim, spit & splogs*

1997-09-02 **spam forgery trademark lawsuit defamation fraud denial of service DoS trademark defamation spoof**

Wired

In mid-April, two well-known science fiction afficionados begain receiving a flood of outraged correspondence and a tide of bounce messages when someone used James MacDonald's online pseudonym, "yog," to spam the world with propaganda for his own science-fiction site. In August, MacDonald and his colleague Jeffry Dwight launched a civil suit against Carlos Lattin, who allegedly sent the spam, charging him with illegal misappropriation of MacDonald's name and also with "trademark infringement, unfair competition, defamation, deceptive trade practices, and false designation of origin."

Category 33.2 *Spam, spim, spit & splogs*

1997-10-02 **junk e-mail unsolicited commercial spam civil law**

UPI

In another attempt to use civil law to stop abuse of the Net, AOL sued Over the Air Equipment Inc. for refusing to stop sending AOL customers junk e-mail. In addition, the suit alleges, the defendent used false e-mail headers and illegally used AOL trademarks to lend a spurious air of authenticity to their junk.

Category 33.2 *Spam, spim, spit & splogs*

1997-10-21 **spam civil litigation lawsuit ISP**

EDUPAGE

EDUPAGE reported, "America Online is suing Prime Data Worldnet Systems for evading AOL's anti-spamming measures to send large quantities of unsolicited email messages to America Online subscribers."

Category 33.2 *Spam, spim, spit & splogs*

1997-11-13 **spam civil lawsuit damages fraud ISP criminal charges**

Business Wire

SimpleNet, a San Diego ISP, filed suit against several originators of spam. The plaintiff demanded an injunction to stop the spam and damages for the trouble the unsolicited e-mail caused. They also asked the San Diego County District Attorney's Office to consider bringing criminal charges under the California Data Access and Fraud Act. The defendants allegedly used forged headers to avoid identification for the hundreds of messages per hour which bombarded the ISP.

Category 33.2 *Spam, spim, spit & splogs*

1998-01-20 **spam information warfare hacktivists protests ISP**

EDUPAGE

EDUPAGE reported that when Sanford Wallace and Walt Rines, notorious ur-spammers, found a new ISP, the service was swamped with phone calls, e-mails and even threats. One of the beleaguered executives of the ISP said, "There are two kinds of terrorists in this: the spammers and the antispammers, and I'm not sure which camp is more objectionable to deal with."

Category 33.2 *Spam, spim, spit & splogs*

1998-08-16 **e-mail service contract tort breach spam libel lawsuit**

EDUPAGE

Earthlink Network, an ISP, erroneously terminated filmmaker Peter Hall's account because they thought he was a spammer. He sued them for $7M in damages or libel, breach of contract, negligence and a violation of the Electronic Communications Privacy Act.

Category 33.2 *Spam, spim, spit & splogs*

1998-12-21 **spam civil lawsuits ISP win**

http://news.com.com/2100-1023-219361.html?legacy=cent

In December of 1998, AOL announced that it had won lawsuits against three spammers and started nine more lawsuits in five states. Full details of the all the settlements were not released, but the courts ruled in AOL's favor on grounds of trademark violations, and copyright violations. The losing defendants included LCGM of Madison, Wisconsin; Prime Data Systems of Bowling Green, Kentucky; and a company called IMS (location not specified).

The report by Jim Hu of CNET News.com continued with the following list of upcoming lawsuits (quoting directly from the article):

Virginia
• AOL takes on Power Promo and Mr. Forrest Dayton for "prolific" spamming of its members, and selling software to circumvent antispam filters.

• AOL also takes action against GreatDeal.Net for spamming AOL members.

California
• AOL takes on Virtual Girlfriend for peddling a fraudulent software package and being associated with other of fraudulent email offers sent to AOL members.

• AOL also takes action against Michael Persaud et.al., alleging that Persaud sent millions of emails to AOL members under false names--even after receiving a cease and desist order.

• AOL files suit against USA Home Employment for continuing to peddle its "get rich quick" schemes despite being issued a cease and desist request from AOL.

Iowa
• AOL takes on National Health Care Discounts, alleging that the company used spammers to generate sales leads.

Florida
• AOL takes action against Global Marketing Solutions for spamming AOL members and attempting to circumvent AOL's antispam filters.

• AOL also takes on First Class Advertising for spamming AOL members and attempting to circumvent AOL's antispam filters.

New York
• AOL files suit against the Christian Brothers, alleging that they spammed members trying to sell apricot seeds as a "miracle" cure for cancer and used the AOL.com domain name to give the impression that the products were affiliated with AOL.

Category 33.2 *Spam, spim, spit & splogs*

2000-01-11 **spam unsolicited commercial e-mail opt out Web service marketing**

Edupage, New York Times

Anti-spam activists howled with derision as the Direct Marketing Association launched e-MPS, a Web site that requires consumers to opt out of receiving junk e-mail from those few spammers who care about consumer preferences.

Category 33.2 *Spam, spim, spit & splogs*

2000-01-19 **pornography unsolicited commercial e-mail junk spam pornography fraud deception hyperlink source**

RISKS 20 77

Pornography-promoters have taken to inserting innocuous labels for URLs such as links to electronic postcards but actually linking to hard-core sites. One RISKS correspondent noted that linking to such sites at work can cause difficulties for employees. MORAL: do not link to URLs from people you don't know without checking the actual destination.

Category 33.2 *Spam, spim, spit & splogs*

2000-01-24 **spam unsolicited commercial bulk e-mail advertising**

NewsScan, Los Angeles Times
http://www.latimes.com/business/20000124/t000007408.html

A study by Ernst & Young had depressing news for anti-spam activists. About 14% of US consumers who receive junk e-mail actually click on the URLs in the messages (although it wasn't clear whether they were trying to complain or actually interested in the products). Apparently this rate of click-through was 3 to 10 times higher than for banner ads. Brace yourselves for continued onslaughts of garbage from unscrupulous low-lifes sending out millions of unwanted messages so as to trap a few victims in their web of greed. [Aw, come on — tell us how you really feel, Mich.]

Category 33.2 *Spam, spim, spit & splogs*

2000-02-16 **mailstorm junk unsolicited commercial e-mail closed list**

RISKS 20 79

Junk e-mailers were reportedly using closed e-mail lists as a form of spam relay for unauthorized mail. Using a forged header including the desired target's e-mail address as the REPLY-TO or FROM address, the criminal sends the junk e-mail to a closed list which bounces the entire message to the victim along with notification that the victim is not authorized to post to the list. Recommendations [from MK]:

A) Turn off automated notification of rejection altogether on all closed lists; or if you feel that the notification messages are important, then

B) Configure the listserv to send back only the title of a rejected message, not the complete text; or if you feel like addressing the potential vulnerability head-on,

C) Design a check of a log file so that the listserv for a closed list can quickly identify a mailstorm and stop it by turning off automated notification of rejection when it is being abused.

Category 33.2 *Spam, spim, spit & splogs*

2000-04-11 **spam unsolicited commercial text junk advertising unscrupulous creeps jerks idiots sociopaths**

NewsScan

Spammers have started using the text-messaging services on some cell phones to send unsolicited messages, probably by simply trying consecutive numbers until they find valid ones. An executive of a company called Plugout.com, which sends unsolicited text messages about its products, says: "What better way to reach your target market? [The company sells cell phone accessories.] We look at it as if we're doing these people a favor if they're looking for these kinds of products." One irate AT&T Wireless customer replied: "Clearly the sender knows it's going to interrupt somebody's day... They're not doing me any favors by soliciting me over my cell phone." (Washington Post 11 Apr 2000)

Category 33.2 *Spam, spim, spit & splogs*

2000-05-19 **spam filter pornography QA quality assurance design flaws false positives rules criteria**

RISKS 20 89

Gary Cattarin analyzed the antispam filters in MS-Office 2000's Outlook program. The assumptions behind MS engineers' spam-identification rules resulted in false positives (non-spam being identified and filed as spam). For example, the rules included >Body contains ",000" AND Body contains "!!" AND Body contains "$"< and therefore caught an inoffensive non-spam message from Cattarin to one of his friends. Analysis of the porn filters for Outlook 2000 revealed the following rules as described by the correspondent (material between > and < is a direct quotation):
>Subject contains " sex"
Subject contains "free" AND Subject contains "sex"
The first is set up with a leading space to only accept the *word* "sex", so those of us who live here in Middlesex county don't lose any local-related mail. But the writer of the second wasn't so careful — what if the Middlesex News offers free subscriptions? That's Spam, yes, but not porn (I guess that's why that newspaper changed its name...).

(2) Don't address your dear friend as such — note the rule:
Body contains "Dear friend"
My golly! I can't send some good old-fashioned heartfelt feelings to my dear friends!! (oops, double "!!" — I got excited!)<

[Peter G. Neumann decided to print the entire analysis of the filtering rules in a separate issue (20.89x) for fear that the normal issue of the RISKS Digest would be blocked because of the key words and phrases in the report itself.]

Category 33.2 *Spam, spim, spit & splogs*

2000-06-05 **antispam signature strings filters false positive errors restrictive**

RISKS 20 91

William Coburn illustrated the risks of relying on generic strings when trying to identify unsolicited commercial e-mail ("spam"). Two of the strings he used to use were "friend@" and "@public.com" in the e-mail header FROM field. By monitoring the rejection log, he was able to discover that e-mail from a legitimate correspondent called Mr Friend had also been blocked. When he informed the hapless Friend, this chap commented that he had wondered why so many of his e-mail messages apparently went astray. Coburn concluded, "he risk here, is that automated processes can chug along for years without anyone ever noticing that they are broken."

Category 33.2 *Spam, spim, spit & splogs*

2000-07-12 **spam e-mail relay design**

RISKS 20 95

Google allows anyone to "e-mail these results to friends" for its search results. However, as Lloyd Wood pointed out in RISKS, one can erase the generated text and put anything one wants in the message, providing an anonymizing relay for unsolicited bulk e-mail.

Category 33.2 *Spam, spim, spit & splogs*

2000-08-03 **spam unsolicited commercial e-mail junk lawsuit opt-in surveys**

NewsScan, New York Times
http://www.nytimes.com/library/tech/00/08/biztech/articles/03spam.html

Online market research Harris Interactive, which regularly conducts surveys of 1.5 million registered participants, is suing America Online and other Internet service providers it claims used the service of a nonprofit organization known as MAPS to illegally block e-mail from Harris survey participants. MAPS is an acronym for Mail Abuse Prevention System, and the service it provides is called the Realtime Blackhole List. The Harris lawsuit, which also names as defendants such companies as Microsoft Hotmail, BellSouth, Juno Online Services, and Qwest Communications, says that it never sends unsolicited mass mailings and that all of its survey participants have voluntarily registered to receive Harris questionnaires. (New York Times 3 Aug 2000)

Category 33.2 *Spam, spim, spit & splogs*

2000-09-25 **unsolicited commercial e-mail junk industry consortium alliance association regulation complaints privacy standards**

NewsScan, Wall Street Journal

http://interactive.wsj.com/articles/SB96982808494289528.htm

Several leading e-mail marketers, including DoubleClick and 24/7 Media, . . . banded together to form the Responsible Electronic Communications Alliance, which plans new "privacy protection standards" aimed at reducing spam e-mail. The proposed standards are based on guidelines issued by the Federal Trade Commission, including giving recipients a way to register complaints and "opt out" of further mailings. The companies acknowledged that their move to establish standards is an effort to forestall government regulation: "The industry came together because it recognizes that if it's going to grow and prosper it's got to respect privacy, and we're not unaware that if we don't go ahead and do it, the government might," says Washington lawyer Chris Wolf, who will serve as the group's president. (Wall Street Journal 25 Sep 2000)

Category 33.2 *Spam, spim, spit & splogs*

2001-01-10 **spam personal preferences arrogance stupidity auction**

NewsScan

E-BAY PONDERS THE MEANING OF THE WORD "NO"
Online auctioneer eBay has told its 6 million users that some sort of system glitch had misinterpreted the desire of many of them to receive its "valuable email communications with news, offers and special events." According to eBay, "many of your Notification Preference defaults were set to 'no' rather than to 'yes,' which means that unlike other eBay members, you're not receiving these types of communication." So it has changed those Notification Preferences from 'no' to 'yes," and that has angered many eBay uses, even though the company insists: "Our history tells us that the great majority of people leave it in the 'yes' position." (Washington Post 10 Jan 2001)
http://washingtonpost.com/wp-dyn/articles/A39734-2001Jan9.html

---

Category 33.2 *Spam, spim, spit & splogs*

2001-01-18 **antispam IP block e-mail diversion misleading messages lies collateral damage unexpected consequences**

RISKS 21 22

Bennett Haselton of Peacefire, an activist organization that fights censorware and spam, was blocked by Hotmail starting around August 2000 so that Hotmail users could not successfully send e-mail to Peacefire.org: "If you tried to send mail to a peacefire.org address from HotMail, you'd get a fake error message a day later saying that there was a problem on the recipient's end -- when it was really HotMail blocking the message from being delivered."

Apparently the problem arose because of HotMail's attempts to fight spam: ". . . HotMail didn't single us out for anything, we just happened to be in the same IP address block as other sites that were the original target of the boycott (e.g. ListSorcerer.com). When our ISP, Media3, didn't kick them off, the boycott organizers expanded the 'boycott list' to include hundreds of unrelated sites also hosted by Media3." Haselton noted that although Peacefire.org addresses were now unblocked, many other innocent users were still prevented from receiving e-mail from HotMail subscribers.

Category 33.2 *Spam, spim, spit & splogs*

2001-02-02 **privacy e-mail antispam corporate policy**

NewsScan

EBAY TO CONCEAL CUSTOMER E-MAIL ADDRESSES
To protect its customers from receiving unsolicited mail from spammers, as well as to prevent the same customers from concluding their deals outside the system, online auctioneer eBay has decided to conceal the e-mail address of its customers. Under the new arrangement, buyers or sellers who wish to contact another other user will enter the user's name in a form and eBay will forward the messages, unread, to the person for whom they are intended. (AP/San Jose Mercury News 1 Feb 2001)
http://www.mercurycenter.com/svtech/news/breaking/ap/docs/810995l.htm

---

Category 33.2 *Spam, spim, spit & splogs*

2001-02-12 **spam instant messaging peer-to-peer networking**

NewsScan

WILL INSTANT MESSAGING DRAW INSTANT SPAM?
Online marketers are salivating at the prospects for combining the power of instant messaging with peer-to-peer networks to create a new wave of Web advertising that some critics charge is more invasive than spam. When people sign onto file-swapping networks like Napster, many expose their instant messaging handles and entertainment tastes, opening up a new channel for targeted advertising. "It's a chilling thought," says Jason Catlett, president of Junkbusters. "The songs that make you visible to the world on Napster say a lot about you. Many people don't realize that when they're using these P2P services they are becoming publishers of their personal collections -- it's like putting your CD collection in the window fronting the street." In a sign of things to come, online ad agency L90 last week inked a deal with peer-to-peer network Aimster in one of the first exclusive partnerships to promote goods to consumers via instant messaging. Aimster plans to start an IM advertising campaign, featuring clients such as Aerosmith, Microsoft and Columbia Tristar. "Essentially, it's the next wave of commercialization of the Net," says Aimster CEO Johnny Deep. "Instant messaging is the delivery vehicle for everything in the same way the Web used to be the delivery vehicle. Now we're using IM for everything, for MP3s, sending movie trailers, software, text." (CNet News.com 16 Feb 2001)
http://news.cnet.com/news/0-1005-202-4851077.html

Category 33.2 *Spam, spim, spit & splogs*

2001-05-02 **spam volume growth news group**

RISKS 21 39

Peter G. Neumann reported in May that for the first time ever, the number of spam messages exceeded the number of legitimate messages to RISKS. He commented, "I hate to recommend draconian anti-spam measures, but the problem is clearly out of control. We are of course opposed to short-sighted legislation and censorship -- especially if it overzealously filters out desired e-mail. Perhaps it is time to implement some radical techniques such as that described in a 1992 paper by Cynthia Dwork and Moni Naor, Pricing Via Processing Or Combatting Junkmail, Proc. Crypto 1992, LNCS 740."

Category 33.2 *Spam, spim, spit & splogs*

2001-05-26 **spam unk unsolicited commercial e-mail cell phones short-messaging service SMS regulation fraud**

RISKS 21 44

Simon Waters reported from Britain on a new variant of the old 809-pager-message scam (in which pagers were fed numbers in the Caribbean which racked up huge long-distance charges); seems some people have been sending "urgent" requests to call a high-cost "premium" number (equivalent to the US 900 numbers).

Category 33.2 *Spam, spim, spit & splogs*

2001-10-08 **spam unk unsolicited commercial e-mail cell phones short-messaging service SMS regulation**

NewsScan

SPAM COMES IN SHORT MESSAGES, TOO [28 Mar 2001]
Millions of Americans who now have short-messaging service (SMS) capability on their cell phones are discovering the dark side of the service -- they are being bombarded with unwanted commercial messages. Cell phone companies say they are powerless to stop the abuse. The problem stems partly from the fact that the account numbers for short-messaging phones are easily identifiable (usually they're just the user's cell phone number plus the name of the service provider). The practice is raising the ire of cell phone users because most get charged for receiving SMS messages, and the FCC says the legal status of cell phone spam is murky. Meanwhile, the number of phones capable of sending or receiving SMS messages is expected to increase to 110 million in 2002 from 37 million in 1999, according to the Yankee Group. (Wall Street Journal 28 Mar 2001)
http://interactive.wsj.com/articles/SB985735340294663006.htm (sub required)

WIRELESS SPAM [13 Apr 2001]
The text-messaging services now included as a standard feature by many wireless companies make it simple for senders of junk mail to target a specific audience by geographic location and pass the costs of their messages on to the people being spammed. Todd Bernier, a wireless technology analyst with Morningstar, predicts: "This will become a huge problem when text messages become more popular in the states. The industry is going to have to do something to control itself. People just won't tolerate it." (AP/USA Today 13 Apr 2001)
http://www.usatoday.com/life/cyber/tech/2001-04-13-wireless-spam.htm

AD FIRMS TARGET ASIAN CONSUMERS WITH SMS [8 Oct 2001]
Ogilvy Interactive, part of the UK's WPP Group, has designed an outreach campaign for the Love Singapore coalition of more than 150 churches based on wireless short messaging (SMS). Consumers who've registered to receive them find messages like "Thank me it's Friday. Signed, God." on their mobile phone screens. Another SMS ad campaign touted a new Coca Cola fruit juice called Qoo so effectively that within nine weeks, Qoo became the No. 1 juice drink in Singapore. The company sent a picture message showing a blue-skinned animated Qoo character to 500 young people in the hope they would send it on to their friends. About half a million mobile users in Singapore have now received the character. "We knew we wanted to target teenagers with this brand," says a Coca Cola spokeswoman. "I think SMS speaks to this group of people especially when traditional methods like TV campaigns are less effective." About 5.6 billion text messages are sent a year in Asia, according to market research firm Mobile Streams. (Wall Street Journal 8 Oct 2001)
http://interactive.wsj.com/archive/retrieve.cgi?id=SB1002497419688848160.djm (sub req'd)

Category 33.2 *Spam, spim, spit & splogs*

2001-10-26 **spam unsolicited commercial bulk e-mail techniques countermeasures remote control modem**

RISKS 21 72

[Greg Searle provided RISKS readers with an excellent overview of the technical measures being used by spammers to get their material through to their victims. What follows is the complete text of Mr Searle's essay, which ends with a brief summary of the fundamentals of antispam origin-tracing.]

Here's the bag of tricks that many spammers are using to keep you from finding out who really sent you the spam:

1. The obvious - find an open e-mail relay, and use it for "e-mail laundering". Forge the e-mail headers, and the e-mail becomes untraceable. All you see is the IP for the open relay, and whatever the spammer wants you to see afterward. The "From" header is always forged, and complaining to the ISP behind the "From" address is pointless. The most you can do is complain to the company that owns the open relay, and hopefully they will close it. Unfortunately, new mail servers appear on the net every day, and many IT "professionals" setting up these systems are just not aware of the open relay problem. There are many web pages which have the sole purpose of finding and listing these open relays.

2. Include a "relay" URL in the spam for potential customers. This URL is typically a "throwaway" account opened on one of the many free webpage services (tripod, geocities, angelfire, etc.) with false credentials. The spammer only expects this URL to exist for a day or two, as the provider will quickly terminate the page once complaints start coming in. The URL typically points to a file or page that will redirect the customer to the true page.

3. There are some businesses that are specifically set up to relay URLs for spammers. One of these is 1freesite.net (G Stubberfield Enterprises). Spammers hire the business to set up a relay page on their server, so they can include this page in their e-mails.

4. Obfuscate the URL in an attempt to make it untraceable. Do you know that IP addresses can be expressed as a single, decimal digit? Browsers will accept this digit and translate it into a valid IP address. Encoding the URL in hex is another trick. Browsers will convert two-digit hex digits that are preceded by a percent sign into a valid character. The URL specification also allows usernames and passwords in a URL. This can be used to mislead. For instance, the URL http://www.webservice.com:www.server.com@192.168.10.10/spampage.html seems to point to "webservice.com", but the piece of the URL before the second colon is really the "username", the piece before the at sign is the "password", and the real web server is the IP after the at sign! Most web servers simply ignore the user name and password if they don't need it. These techniques can be combined to make a URL really hard for a person to decode.

5. Compose the relay webpage in JavaScript. Encrypt the "real" web page and any URL's, and have a JavaScript function decode it.

6. Ask customers to respond to the message. Include a valid "Reply To" header that is different from the "From" header. The e-mail client will recognize this and send any responses to the "Reply To" address. The e-mail account set up to receive these messages is usually a "throwaway" address set up on a free mail service with false credentials.

7. Include an unlisted phone number, which is protected by the telephone company and is untraceable.

8. Included an executable at the URL enclosed in the message. This executable is typically compressed to obfuscate its contents from prying binary file editors. The executable then forwards the customer's computer to the business's true URL. Anybody who opens this executable file is too ignorant to know any better.

All of these methods, except for the telephone number and the reply-to address, are completely reversible to expose the company behind the e-mail. If the computer can get to the final page, then so can the person operating the computer, given enough knowledge of the technology involved. There is one particularly nasty spammer, hosted at sexmansion.com and web69.com, that includes a doubly-compressed executable in the page that they set up on a "throwaway" site. Their extremely explicit e-mailings point to this executable's URL. This executable is a dialer application that redirects the user's modem to an offshore telephone number and sends their browser to one of the above mentioned domains. This appears as a charge on their telephone bill. This business was rather clever with the obfuscating technology used to hide their presence, but the same technology can be used to unravel the obfuscation and find the business behind it.

Category 33.2 *Spam, spim, spit & splogs*

2001-11-13 **e-mail address harvesting interception eavesdropping confidentiality harvesting sale contract violation insider crime danger spam unsolicited commercial bulk e-mail forged IP headers SMTP bounce rejection messages**

RISKS 21 76

In an interesting RISKS sequence of messages, Nickee Sanders reported that an e-mail bounce message appeared to indicate that someone had sent spam using her e-mail address as the source. Andrew Klossner responded to her puzzled account by explaining, "That 'original message' was never sent. The 'bounce notification message' was forged by the spammer. And it worked -- you paid close attention to it."

Allan Hurst then provided a detailed experimental analysis of what happened to e-mail addresses which were never made public (they were used only for test purposes). He wrote, "Within two months of opening the Yahoo! Mail account, it started receiving spam, none of it from Yahoo. Within three days of opening the HotMail account, it started receiving spam, in amounts far larger than the Yahoo account." Given that he explicitly opted out of any e-mail address sharing, then "Either Yahoo Mail and HotMail are lying about not publishing or selling addresses, or someone's harvesting e-mail addresses by sniffing packets. (Hence the subject of this message.) As much as I'd like to bash the vendors . . . I strongly suspect the answer is that someone's found a way to harvest e-mail addresses. (Keep reading.)"

His next test involved an e-mail address on MyRealBox.com, where he was very confident that the Internet service provider "do NOT sell the MyRealBox accounts, nor use them for marketing purposes of any kind." After about six months of completely spam-free existence of this new address, "Suddenly, I was flooded with everything from 'failed delivery' messages to angry missives threatening me with bodily harm for spamming them." Mr Hurst wondered exactly where the spammers picked up his e-mail address? And how could such abuse be stopped?

Several other contributors chimed in with evidence that unused e-mail addresses were nonetheless being addressed by spammers.

The next wave of responses suggested that the spammers were likely using a dictionary or brute-force attack on the ISPs: trying out every possible alphanumeric combination to find valid e-mail addresses (those that did not bounce). Although this might seem like a lot of work, Walter Dnes explained, "With today's fast computers and broadband, the above is feasible."

Category 33.2 *Spam, spim, spit & splogs*

2001-12-28 **antispam filter software quality assurance**

NewsScan

AOL TREATS HARVARD ACCEPTANCE LETTERS AS JUNK MAIL: WHY? [28 Dec 2001]
AOL's spam-filtering software thwarted Harvard College's attempt to use e-mail to give applicants the joyous news that they'd been accepted. An AOL spokesman was unable to explain why this happened. [Presumably the messages contained no objectionable words or graphics, but of course very few people can be certain of that, since very few people actually received them.] An AOL spokesman said: "We fight a daily battle against spam at the server level, where we filter it out. Spam is our No. 1 problem. But it's hard to say what would have caused the system to filter e-mail from Harvard." [Question to AOL: What about e-mail from NewsScan? We promise to be good, or at least better.] (Boston Globe/Atlanta Journal-Constitution 28 Dec 2001)
http://www.accessatlanta.com/ajc/epaper/editions/friday/news_c3c211257171a1e100c2.html

---

Category 33.2 *Spam, spim, spit & splogs*

2002-01-08 **viral marketing e-mail chain letter consumer spam junk e-mail worm social engineering**

NewsScan

VIRAL MARKETING GOES MAINSTREAM
Viral marketing is set to invade your in-box, say advertisers who are looking to this upstart marketing method to boost their outreach efforts. "At the moment, say 'viral marketing' and you still think teens and fashion brands -- cool things for cool people distributed via e-mail. But the principles that make viral marketing work should be taken on board by any brand-owner wanting to target any age group," says marketing consultant David Nichols. "Grown-up viral marketing is about involving people in things they love as a way of introducing a dialogue between brand and consumer." E-based marketing will become more prevalent, say many experts, but also will become increasingly permission-based. "I'm not convinced there is a future for viral marketing involving messages thrown out to hundreds of people in the hope someone will pass it on," says Tim Patten of marketing group HHCL Digital Solutions. "But I do believe there is value where people agree to receive messages, then -- on the strength of the value of that message -- decide to pass it on." Key to the success of these marketing efforts will be companies' willingness to participate in a true dialogue with their customers: "Too many marketers still believe when they speak consumers will listen. The enthusiasm amongst marketers for developing new ways of pushing information at consumers has not been matched by an enthusiasm to listen to what consumers say." says Mark Curtis, a partner at marketing consulting group Fjord. (Financial Times 8 Jan 2002)
http://news.ft.com/news/industries/internet&e-commerce

Category 33.2 *Spam, spim, spit & splogs*

2002-01-10 **spam filters false positives reliability program design bounce**

RISKS 21 84ff

In January 2002, AOL's spam filters rejected Harvard University's admissions-department e-mail. In the absence of any information from AOL (policy precludes their revealing any explanation of their anti-spam policies) analysts speculated that simply sending large numbers of similar messages to AOL members was enough to trigger false-positives in the filters. In discussion on the RISKS Forum, correspondents pointed out that e-mail reliability is still nowhere near that of the U.S. Postal Service. The problem was exacerbated by the lack of a bounce message to the originators; thus neither sender nor recipient could be expected to know that the messages had been discarded. Some commentators snidely suggested that using AOL as an e-mail service might be a legitimate basis for rejecting applicants. . . .

Category 33.2 *Spam, spim, spit & splogs*

2002-01-14 **spam unsolicited commercial bulk e-mail countermeasures lawsuits statistics growth**

NewsScan

THE SPAM WARS
There has been a 16-fold increase in the number of unsolicited commercial e-mail messages in the past two years (according to the spam-filtering company Brightmail), and little progress has been made in fighting it, although sporadic lawsuits have sometimes yielded (very) small (and often uncollectable) cash judgments against the spammers. The president of the anti-spam Junkbusters Corporation has compared such lawsuits to "mopping up an oil spill with a toothbrush." Yet some anti-spammers feel the effort is worthwhile, and Bennett Haselton, who recently won four judgments of $500 each in Washington state, plans to publish a how-to guide for the spam-perplexed, hoping that if [more] people "get in the habit of taking legal action if they get spammed, then it's going to become so expensive that spammers have to get out of business." (AP/San Jose Mercury News 14 Jan 2002)
http://www.siliconvalley.com/docs/news/svfront/031444.htm

Category 33.2 *Spam, spim, spit & splogs*

2002-01-24 **antispam excess algorithm wrong bad error false positive reject verification**

RISKS 21 89

Jonathan Kamens reported his frustration at trying to reach another RISKS contributor whose Internet service provider blocked his e-mail for spurious reasons. It happened that Mr Kamens was unable to send his e-mail through his usual DSL line, so he sent his message via his ISP's SMTP server. The intended recipient's mail server rejected the message because, as Mr Kamens explained it, ". . . this site's system administrators have decided to block all E-mail for which the host name in the envelope address can't be matched up obviously (using a simple string comparison) with the host name of the mail server sending the message. In other words, if you have your own domain name, but you send E-mail through your ISP's mail server, you simply can't send E-mail to this site."

When he tried again, this time via his restored DSL service, his mail was rejected because his mail server was incorrectly labeled as a spam relay.

Although the site claimed that they would correct mistaken assignments to the rejection list, Mr Kamens found it particlularly irritating that the administrators of this picky site did not provide any way to reach them online. [MK adds that presumably, even if they had, the explanation or complaint would never make it to their e-mail inbox if it came from the affected mail server.]

Category 33.2 *Spam, spim, spit & splogs*

2002-02-12 **spam unsolicited commercial e-mail chain letter Ponzi scheme pyramid fraud settlement government regulators**

NewsScan

FTC's FIGHT AGAINST SPAM
Saying that the Federal Trade Commission is "going after deceptive spam and the people who send it. We want it off the Net," FTC chairman Timothy Muris has announced that the agency has settled charges against seven people who ran an e-mail chain letter promising returns of up to $46,000 on an investment of only $5. The letter received responses from more than 2,000 people in nearly 60 countries. The research firm Jupiter Media Metrix says that Internet users received on the average 571 pieces of mail last year generated by unsolicited commercial mass-mailings of everything from pornography to fake diplomas; the firm predicts that number is likely to rise to 1,500 a year by 2006. (Reuters/USA Today 12 Feb 2002)
http://www.usatoday.com/life/cyber/tech/2002/02/12/ftc-spam.htm

---

Category 33.2 *Spam, spim, spit & splogs*

2002-03-11 **spam opt-in opt-out lies fraud falsehood address harvesting**

RISKS 21 94ff

Discussion in RISKS erupted over a familiar scam from spammers: claiming that they are offering opt-in lists (invitations to join, permission to send) when in fact their unwanted messages reveal that they will take absence of response as tacit approval of continued spamming. The danger in replying is that since the spammers are evidently liars, they are probably lying about the results of using their opt-out e-mail addresses and so one's address is likely to be sold to yet another spammer as being validated.

Category 33.2 *Spam, spim, spit & splogs*

2002-03-12 **spam fraud abuse regulators legal action court proceeding injuction DNS Domain Name System**

NewsScan

FTC CRACKS DOWN ON SPAM
A U.S. District Court, acting at the request of the Federal Trade Commission, has closed down the U.S.-registered Web sites of three U.K.-based companies of sending unsolicited commercial e-mail message (or "spam") to sell about $1 million worth of phony Web addresses such as ".usa," ".sex," and ".store" for $59 each. The Web sites closed were called www.dotusa.com, www.dotsex.com, and www.dotstore.com. The defendants say they are denying the allegations and are appealing the ruling. An FTC official says: "These scammers conned consumers in two ways. They sent deceptive spam, and they sold worthless Web addresses from their Web sites. By closing down this operation we're sending a strong signal: We will not tolerate deceptive spam." (New York Times 12 Mar 2002)
http://partners.nytimes.com/2002/03/12/technology/12SPAM.html

---

Category 33.2 *Spam, spim, spit & splogs*

2002-03-22 **anti-spam blackhole blacklists administration policies defaults**

RISKS 22 01

Eric Murray reported in RISKS on some of the dangers of sloppy administration of anti-spam blacklists that interfered with legitimate mailings from his site. In one case, a blacklist operator chose to include an enormous block of IP addresses because one ISP was refusing to deal with one spammer; his response to complaints was, "Too bad for you, you should move." In the second case, recipients were running software that checked a whitelist of approved sources; when that list was shut down, the software received no confirmations on its checks of originating addresses and cheerfully blocked everything -- but everything -- coming into its clutches.

Category 33.2 *Spam, spim, spit & splogs*

2002-04-03 **lawsuit ISP fraud spam solicitation pornography**

http://news.com.com/2102-1023_3-874664.html?tag=st_util_print

AOL won a civil lawsuit against a pornographic spammer, Netvision Audiotext of Fort Lauderdale, Florida and forced the ISP to stop soliciting the business of spammers in violation of its own professed policies.

Category 33.2 *Spam, spim, spit & splogs*

2002-04-10 **P2P peer-to-peer AI artificial intelligence anti-spam filter e-mail signature content inspection**

NewsScan

INTELLIGENT SPAM FILTER
A new spam-filtering technology code-named Folsom uses a combination of peer-to-peer communications and machine learning to intercept nearly all unwanted e-mail, according to its creators. The peer-to-peer part of the technology enables a user to identify a message as spam mail, which the program then assigns a "signature" based on its content. The signatures are sent to one of numerous distributed servers where they're automatically downloaded by other members of the network and used to block copies of the same message. The machine learning part of the equation targets new spam by looking at the words and phrases in previously identified spam messages and making a judgment about the new mail. The developers say in tests of e-mail streams containing 40% to 60% spam mail, Folsom managed to reduce the percentage to "near zero" with very few "false positives." "It's a very interesting concept," says a spokesman for the Coalition Against Unsolicited Commercial Email. "Spam is getting worse, both in terms of raw volume and percentage." (New Scientist 9 Apr 2002)
http://www.newscientist.com/news/news.jsp?id=ns99992141

Category 33.2 *Spam, spim, spit & splogs*

2002-04-22 **spam costs study research industry information warfare**

NewsScan

JUNK MAIL FALL-OUT
The founder of the anti-spam SpamCon Foundation says that "spam is a theft of both my time and my money," and industry research groups bear him out: Ferris Research has concluded that the time lost to the task of deleting spam costs about $200 per in-box a year (and destined to go higher), and a Gartner Group study found that Internet service providers lose $1 million for every 7 million of its members, largely because spam drives customers away. Does the future look brighter for haters of unsolicited commercial e-mail messages? Not likely. The head of the anti-spam organization Spamcop.net says: "It's an arms race. Once you close down an avenue for the spammer, he just has more of an incentive to find new ones." (San Jose Mercury News 20 Apr 2002)
http://www.siliconvalley.com/mld/siliconvalley/3108519.htm

Category 33.2 *Spam, spim, spit & splogs*

2002-04-22 **biometric identification authentication I&A access control**

Security Wire Digest 4 31

SAFLINK INTRODUCES SAFSOLUTION FOR WINDOWS
SAFLINK, a developer and integrator of biometric security solutions, last week released SAFsolution: Windows Workstation, a software product designed to replace text-based passwords with biometric authentication. The software is designed to work with a wide variety of biometric hardware: voice, face, and iris recognition devices, as well as fingerprint scanners.
http://www.saflink.com

Category 33.2 *Spam, spim, spit & splogs*

2002-05-22 **spam content filtering blunder quality assurance QA**

NewsScan

AT&T's FILTER FILTERS AT&T's MAIL
An example of foot-in-mouth filtering? AT&T Broadband offered its high-speed Internet users an e-mail software filter to block spam, but later found out that it had blocked its own messages to customers notifying them of a rate increase. An AT&T executive tried to put the best face on it: "If there is a silver lining, it appears our spam filtering system works so well that it even deletes mass e-mails from our own company." The company will resend customer notices of the rate increases. (AP/USA Today 2002)
http://www.usatoday.com/life/cyber/tech/2002/05/22/e-mail-filter.htm

---

Category 33.2 *Spam, spim, spit & splogs*

2002-05-22 **spam filters content filtering research**

RISKS 22 08ff

Peter G. Neumann noted that the RISKS Forum reached 98% spam content in its inbasket during a 10-day period with over 1,000 messages received. He installed SpamAssassin and the rate fell to near zero. Unfortunately, false positives continue in this field, and his announcement about spam was itself rejected by a number of spam filters because it included the trigger phrase "o-n-e h-u-n-d-r-e-d p-e-r-c-e-n-t g-u-a-r-a-n-t-e-e-d" which had to be hyphenated in the followup to avoid triggering the same filters.

Category 33.2 *Spam, spim, spit & splogs*

2002-07-05 **spam junk phone calls cellular mobile costs consumers direct marketing**

NewsScan

NUMBER OF JUNK CELL PHONE CALLS INCREASING
Cell phones, with their numbers unlisted, have generally been shielded from telemarketers, but that shield is becoming less effective, and an increasing number of junk calls are reaching -- and angering -- cell phone users on vacation, in their cars, or in other places they don't want to take unwanted calls (let alone have to pay for them). Companies, consumer groups, and even the Direct Marketing Association have all recognized the growing problem, and state and federal legislators are trying to deal with it through legislation. Consumer advocate Robert Biggerstaff expresses his indignation in these words: "If you eat up my minutes of cell time, you're forcing me to subsidize your advertising." (New York Times 5 Jul 2002)
http://partners.nytimes.com/2002/07/05/business/05JUNK

Category 33.2 *Spam, spim, spit & splogs*

2002-08-22 **junk fax federal regulators fine fraud deception lawsuit**

NewsScan

JUNK FAXES
The Federal Communications Commission wants to levy a $5.4 million fine on Fax.com, a company that uses a fax-number database to distribute faxed ads for its customers (restaurants, auto repair shops, and so forth). The FCC said that Fax.com has "engaged in a pattern of deception to conceal its involvement in sending the prohibited faxes," which has been banned since the passage of the Telephone Consumer Protection Act of 1991. Fax.com's attorney, Mary Ann Wymore, regards the ban as "a clear infringement on commercial speech rights," and predicts it ultimately will be overturned by the U.S. Supreme Court. (Wall Street Journal 8 Aug 2002)

MAD AS HELL OVER JUNK FAXES
Steve Kirsch, a Silicon Valley entrepreneur and philanthropist, is suing the fax-broadcasting company Fax.com for $500 billion (repeat: billion) in statutory damages, assuring skeptics: "This is not a publicity stunt; our goal is to shut Fax.com down and make any advertiser thinking of sending an unsolicited fax think twice... I have the resources, time and money." (San Jose Mercury News 22 Aug 2002)

Category 33.2 *Spam, spim, spit & splogs*

2002-09-09 **spam wireless LAN local area networks ISP Internet service provides wardriving hijacking penetration**

NewsScan

DRIVE-BY SPAM ATTACKS HIT WIRELESS LANs
The proliferation of unsecured corporate wireless networks is fueling a surge in drive-by spamming, a security expert warned attendees of the First International Security Users Conference in London. "These people simply drive up to a building armed with their pornographic e-mail, log into the insecure wireless network, send the message to 10 million e-mail addresses and then just drive away," said Adrian Wright, managing director of Secoda Risk Management. With more ISPs instituting no-spamming rules, these unsecured networks have become easy targets for would-be spammers. All they have to do is find an unprotected SMTP (simple mail transfer protocol) port on a company's server and then pose as legitimate users of the network — the mail server can't tell the difference. Wright warned that between 60% and 80% of corporate wireless networks are unsecured, often because managers fail to change default settings when they install a wireless LAN. The security hole has led to the new phenomenon of "wardriving" — driving around a city until you find an unsecured wireless LAN — which leads to "warchalking" — drawing a symbol in chalk on a wall or pavement to mark the presence of a wireless networking node. And the practice isn't just confined to metro areas, said Wright, producing a photo of a warchalking symbol drawn on a buoy floating at sea. (CNet News.com 6 Sep 2002)
http://news.com.com/2100-1033-956911.html?tag=fd_top

Category 33.2 *Spam, spim, spit & splogs*

2002-10-21 **spam cellular phones wireless law legal restrictions database**

NewsScan

ENDING MARKETING CALLS TO CELL PHONES
To help telemarketers comply with a 1991 federal law banning auto-dialed or prerecorded commercial calls to cell phones, the Direct Marketing Association has identified 280 million existing and prospective wireless numbers for its member businesses to avoid calling. Member companies have been afraid they'll get into trouble for inadvertently calling cell phone numbers not readily distinguishable cellular from landline numbers. (New York Times 21 Oct 2002)

Category 33.2 *Spam, spim, spit & splogs*

2002-11-12 **anti-spam e-mail address change consumers costs marketing businesses**

NewsScan

E-MAIL ADDRESS CHURN GIVES E-TAILERS HEARTBURN
Almost a third of U.S. Internet users change their e-mail addresses each year, costing businesses millions in potential sales, according to a new study by NFO WorldGroup. Reasons cited for changing e-mail addresses include changing jobs, switching ISPs, or evading spam. Recently, 87% of total respondents had changed a personal e-mail address and 35% had changed a work address. At least 16% said the change was intended specifically to shake off spammers whose tactics have become increasingly aggressive and subject matter increasingly offensive. The high turnover rate has caused headaches for legitimate businesses, however, who lose contact with customers who may have volunteered their e-mail addresses as part of the business relationship. "It's too much of a hassle to update their personal information with the sites," says an NFO marketing manager. "They look at it and think if they have to go through this process with 20 Web sites, it's too much trouble. Whereas with contacting 20 friends, that's a different thing." Return Path, an e-mail change-of-address company, estimates that e-mail churn cost businesses between $3 billion and $4 billion in 2000 due to lost sales, wasted e-mail acquisition marketing and unnecessary e-mail delivery costs, with those losses rising to $10 billion to $20 billion in five years. (Wired.com 12 Nov 2002)
http://www.wired.com/news/business/0,1367,56049,00.html

Category 33.2 *Spam, spim, spit & splogs*

2002-11-14 **spam chat rooms study test investigation**

NewsScan

THE PRICE OF CHATTING MAY BE GETTING SPAMMED
A new study by the Federal Trade Commission and other federal agencies and northeastern states has found that your participation in chat rooms will substantially increase the possibility that your name will be captured by spammers to send you junk e-mail. Surprisingly, online dating services and resume services were found to be relatively safe from spammers [but not necessarily from bad experiences, we suppose]. In an undercover operation, all the e-mail addresses planted on 250 new accounts used in chat rooms began to receive spam messages. Close behind were newsgroups [not NewsScan, which is not a newsgroup], which generated junk mail for 86% of the undercover e-mail accounts. (USA Today 14 Nov 2002)
http://www.usatoday.com/tech/news/2002-11-13-spam-study

Category 33.2 *Spam, spim, spit & splogs*

2002-11-27 **anti-spam research archive database filters fight battle**

NewsScan

SPAM ARCHIVE PROJECT SEEKS CONTRIBUTIONS
CipherTrust wants your spam, including every e-mail come-on for Viagra, "free" pornography, and adult services. But they aren't masochists — they're hoping to build an archive of spam (www.spamarchive.org) that programmers and researchers can use in the never-ending fight against unsolicited e-mail. The company hopes to collect at least 10 million spam samples within a year, and is already well on its way to meeting its goal. "This should eliminate one of the big bottlenecks for people who want to make anti-spam tools," says one programmer who has developed mail-filtering programs. "You can write all the code you want, but it won't do a whole lot of good unless you have a large amount of spam to test your algorithms on." CipherTrust says it will use the archive to help its technicians improve "IronMail," its proprietary anti-spam product. Still, even the best junk e-mail filters won't stop determined spammers, says programmer and open source enthusiast Eric Raymond: "It's like a whack-a-mole game: you shut down (spam e-mail) servers in one place, and the same spammers pop up again in another place running a shoestring operation out of their basement. But in a weird way, that sort of highlights one of the Internet's strengths, that it's very hard to lock someone out of communication or suppress speech." (Washington Post 26 Nov 2002)

Category 33.2 *Spam, spim, spit & splogs*

2003-01-06 **spam consumer attitudes**

NewsScan

SURPRISE — MOST E-MAIL USERS HATE SPAM
In an anticlimactic finding, a Harris Interactive poll released Friday reveals that 96% of the 2,221 respondents find unsolicited commercial e-mail annoying, and nearly three quarters of those favor making spam illegal. Pornographic spam messages were deemed most troublesome, according to 90% of respondents, while 79% cited mortgage and loan come-ons as objectionable. Less annoying (but not by much) were investment opportunity and real-estate spam. Meanwhile, consumers needn't look for a break from spam mail any time soon — despite a recent crackdown by the Federal Trade Commission on fraudulent schemes advertised on the Internet, the incidence of spam continues to grow. According to anti-spam software maker Brightware, unsolicited messages made up 40% of all e-mail in November — up from 13% a year earlier. The Senate Commerce Committee passed a bill last May to set guidelines for unsolicited e-mail, but no further action has been taken by the full Senate. (Wall Street Journal 3 Jan 2003)

Category 33.2 *Spam, spim, spit & splogs*

2003-03-06 **anti-spam research**

NewsScan

THE IETF APPROACH TO SPAM
The Internet Research Task Force — loosely affiliated with the Internet Engineering Task Force standards group — has formed an Anti-Spam Research Group, which will focus on the problem of spam proliferation and make suggestions on ways to change basic e-mail technology to foil the bulk e-mailers. "Once considered a nuisance, spam has grown to account for a large percentage of the mail volume on the Internet," says the group's Web site. "The purpose of the [research group] is to understand the problem and collectively propose and evaluate solutions to the problem." First steps will include classifying different kinds of spam and antispam proposals, and studying ways to track down spammers, who are often difficult to identify. A first meeting is set for March 20 at the IETF's San Francisco gathering. (CNet News.com 6 Mar 2003)
http://news.com.com/2100-1032-991305.html

Category 33.2 *Spam, spim, spit & splogs*

2003-03-24 **anti spam software developed challenge response**

NewsScan

NEW ANTI-SPAM SYSTEM BEING DEVELOPED

A California start-up company created by well-known software designer Phil Goldman (formerly of Apple, General Magic, WebTV and Microsoft) has designed an e-mail service that takes a "challenge-response" approach to blocking spam. When a user receives a bulkmail message from an unknown source the system intercepts the message and requires the sender to give indication (by filling out a form) that the message is not an instance of spam. The service will cost $9.95 a year, so Forrester Research analyst Jim Nail note skeptically: "It's a really nice product, and it's pretty easy to use. The question is how big a market. Do people want to pay anybody anything for these features?" (New York Times 24 Mar 2003)

Category 33.2 *Spam, spim, spit & splogs*

2003-03-25 **Hotmail outgoing spam Microsoft**

NewsScan

HOTMAIL TARGETS OUTGOING SPAM

To fight unsolicited bulk commercial e-mail, Microsoft's free Hotmail e-mail service has limited to 100 the number of messages that a user can send in a 24-hour period. The limit, which was imposed earlier this month, will not apply to Hotmail subscribers who purchase extra storage. (AP/San Jose Mercury News 25 Mar 2003)

Category 33.2 *Spam, spim, spit & splogs*

2003-04-22 **anti spam debate**

NewsScan

THE BEAUTY OF SPAM IS IN THE EYE OF THE BEHOLDER
Brightmail, which makes spam-filtering software for corporations and Internet service providers, says that 45% of the mail it now sees is spam (unsolicited bulk-distributed messages), and AOL says 2 billion spam messages are sent to its 35 million customers each day, accounting for more than 70% of the total AOL incoming traffic. But the spam creators are getting tired of having figures like these flouted as though spam was a bad thing. Bob Dallas of an e-mail firm in Ohio says, "We have allowed these spam cops to rise out of nowhere to be self-appointed police and block whole swaths of the industry. This is against everything that America stands for. The consumer should be the one in control of this." E-mail marketer Alyx Sachs thinks the same way Bob Dallas does: "These antispammers should get a life. Do their fingers hurt too much from pressing the delete key? How much time does that really take from their day?" (New York Times 22 Apr 2003)

Category 33.2 *Spam, spim, spit & splogs*

2003-04-24 **anti spam hide from spammers preserve e-mail address**

NewsScan

HOW TO HIDE FROM SPAM-MONGERS
Researchers at the Center for Democracy and Technology have competed a study that seeks to answer the question: how do spammers find you? They found that e-mail addresses posted on Web sites or in newsgroups attract the most spam, because spam-mongers use harvesting programs such as robots and spiders to collect e-mail addresses listed in those places. So if you've ever provided your e-mail address as part of an eBay transaction, or responded to an online job listing, or participated in a discussion board, it's likely that your e-mail address is now making the rounds on junk e-mail lists. One way to avoid the harvesting in the first place, says the team, is to replace characters in an e-mail address with human-readable equivalents — for example jane@domain.com would become jane at domain dot com. Another successful evasion technique is to replace the characters in an e-mail address with the HTML equivalent. Over the course of the six-month study, 97% of the spam was sent to addresses that had been posted on public Web sites, especially those that were linked to major portals such as AOL and Yahoo. (BBC News 24 Apr 2003)

Category 33.2 *Spam, spim, spit & splogs*

2003-04-24 **anti spam initivate markerters consortium e-mail productivity**

NewsScan

CONSORTIUM OF ONLINE MARKETERS ANNOUNCES ANTI-SPAM INITIATIVE
The E-mail Service Provider Coalition (ESPC), a consortium of online marketers such as DoubleClick and iMakeNews, is launching what it calls Project Lumos, which will provide a way for high-volume e-mail senders to have their mailings certified by ESPC to ensure they follow ethical practices. Under Project Lumos there will be four levels of accountability: certification to ascertain the mailer's identity; standardization of all sender info including identification and trackability; proof of sender ID in the SMTP message header; and various performance monitoring activities. The project seeks to accommodate the interests not only of the receivers of commercial e-mail, but also those of the senders of such mail. According to ESPC, "E-mail is indeed a killer app and has been a major component in the productivity and efficiency gains of the digital economy. But those gains will be lost if e-mail becomes unreliable as a communications tool. Businesses will not be able to use e-mail if they cannot have a reasonable assurance that their messages will be delivered." (ComputerWorld 24 Apr 2003)

Category 33.2 *Spam, spim, spit & splogs*

2003-04-29 **spam zombies relay junk e-mail Trojan horses proxy crime**

NIPC/DHS

April 25, SecurityFocus — Rise of the spam zombies.

Pressed by increasingly effective anti-spam efforts, senders of unsolicited commercial e-mail are using Trojan horses to turn the computers of innocent netizens into secret spam zombies. One of those programs, popped up last week. "Proxy-Guzu" arrives as a spam, and when executed by an unwitting user, the Trojan listens on a randomly-chosen port and uses its own built-in mail client to dash off a message to a Hotmail account, putting the port number and victim's IP address in the subject line. The spammer then routes as much e-mail as he or she likes through the captured computer, knowing that any efforts to trace the source of the spam will end at the victim's Internet address. "As a general rule it's legal to send someone an e-mail even if they don't want it," says Mark Rasch, a former Justice Department computer crime attorney. "But once you break into their computer and get their computer to send e-mail to someone else, then you're violating federal and state computer crime laws."

Category 33.2 *Spam, spim, spit & splogs*

2003-04-30 **spam spyware adware relay viruses hijack Outlook ICSA**

NewsScan

SPAMMERS USE VIRUSES TO HIJACK COMPUTERS
As efforts to tackle junk e-mail ramp up, unscrupulous spammers increasingly are hiding their identities by taking over innocent users' accounts using e-mail messages that resemble computer viruses. Like many other viruses, these programs exploit weaknesses in Microsoft's popular Outlook e-mail package. One of the first hijacking programs to emerge was called "Jeem," which contained a hidden e-mail engine that enabled it to route messages via the infected computer. Another, called Proxy-Guzu, comes as a spam message with an attachment. When the unsuspecting recipient clicks on the attachment, the computer contacts a Hotmail account and transmits information about the infected machine, making it possible to route e-mail through that machine. "Spammers are beginning to use virus-like techniques to cover themselves," says Larry Bridwell, content security programs manager at ICSA Labs. "Spam is one of the two things that the security industry is going to be asked to deal with. The other is adware or spyware." (BBC News 30 Apr 2003)

Category 33.2 *Spam, spim, spit & splogs*

2003-05-01 **spam cell phones text messages 2025551212@cellphonecarrier.com telemarketers**

NewsScan

SPAM HEADING FOR CELL PHONES
The spam that now accounts for as much as three-quarters of total e-mail volume is heading for a cell phone near you, according to a panel of telecom experts at a forum on spam held Thursday. Federal law prohibits most telemarketers from dialing cell phones, but there are no laws preventing them from sending text messages to addresses like 2025551212@cellphonecarrier.com. Because many text messaging services carry a per-message charge, the cost to consumers could mount quickly. Text messaging has yet to catch on in the U.S., and it may never happen if spammers start exploiting it, said phone-company officials. Wireless spam is already a problem in Japan, where text messaging has been a popular feature for years. "As data traffic over wireless networks continues to grow, so will spam," warned an NTT executive. (Reuters 1 May 2003)

Category 33.2 *Spam, spim, spit & splogs*

2003-05-20 **spammer your computer money issue hijacking backdoor software**

NewsScan

ARE YOU A SPAMMER?
Hundreds of thousands of computers are now being used without their owners' knowledge to forward spam around the world. William Hancock, chief security officer of Cable & Wireless, says: "This is not about a hacker trying to show off, or give you a hard time. This is about money. As long as there are people who want spam to go out, this is not going to go away." And how do the hijacked victims feel? They usually feel ignorant and in the dark. A network abuse engineer with Earthlink explains, "People are shocked. Someone will say, 'I thought my computer was running a little slow, but I had no idea it was being used to send spam.'" A common way for spammers to pull this trick off is to use a backdoor in the software used to link several computers or "proxy servers." (New York Times 20 May 2003)

Category 33.2 *Spam, spim, spit & splogs*

2003-05-20 **hacker hijack computer remotely spam e-mailers messages bounce AOL KaZaA virus software computer**

NIPC/DHS

May 20, New York Times — Hackers hijack computers remotely in new surge of spam.

As spam has proliferated many mass e-mailers have become more clever in avoiding the blockades by aggressively bouncing messages off the computers of unaware third parties. In the last two years, more than 200,000 computers worldwide have been hijacked without the owners' knowledge and are currently being used to forward spam, according to AOL and other Internet service providers. Last Thursday, 17 law enforcement agencies and the Federal Trade Commission issued a public warning about some of the ways spammers now commandeer computers to evade detection. Mostly, the spammers are exploiting security holes in existing software, but increasingly they are covertly installing e-mail forwarding software, much like a computer virus. In the last six months, an increasingly common trick has been for spammers to attach rogue e-mail-forwarding software to other e-mail messages or hide it in files that are meant to emulate songs on music sharing sites like KaZaA.

Category 33.2 *Spam, spim, spit & splogs*

2003-05-22 **fight spam internationally Bill Gates protecting American computers anti-spam business lost productivity**

NewsScan

THE NEED FOR INTERNATIONAL COOPERATION TO FIGHT SPAM
The president of Brightmail (a company that helps Internet providers block spam) predicts that by the end of this year half of all e-mail will be spam messages, and says that spam costs U.S. businesses $10 billion a year in lost productivity. Microsoft chairman Bill Gates has called for international organizations to join the anti-spam effort, and Sen. Charles Schumer (D,NY) says: "As soon as we tighten up our laws here and institute vigorous enforcement, those who want to violate our laws move abroad. A global agreement will ensure that anti-spam standards protecting American computers are enforceable both here and abroad." (AP/San Jose Mercury News 22 May 2003)

Category 33.2 *Spam, spim, spit & splogs*

2003-05-22 **spam battle Direct Marketing Association DMA e-mail advertisements $7 billion sales**

NewsScan

STUDY SHOWS SPAM PAYS
While the battle against spam intensifies, the Direct Marketing Association has just released figures showing that commercial e-mail advertisements generated more than $7 billion in sales last year. The DMA's study is intended to bolster its claim that commercial e-mail plays a significant role in the U.S. economy. According to the report, about 36% of e-mail users, or 21% of all adult Americans, have purchased a product or service as the result of receiving commercial e-mail over the past year, with purchases valued at an average of $168. About 9% of these e-mail users said they made their purchases as the result of unsolicited commercial e-mail. (Wall Street Journal 22 May 2003)

Category 33.2 *Spam, spim, spit & splogs*

2003-05-27 **spam cure disease Cnet blocking software death e-mail**

NewsScan

SPAM'S CURE COULD BE WORSE THAN THE DISEASE
CNet columnist Declan McCullagh worries that the proliferation of spam-blocking software incorporating challenge-response technology could lead to the death of e-mail. Challenge-response systems require the human sending a message to perform a simple task such as clicking on a link or typing a special password to get past the barrier. The problem is, says McCullagh, that many challenge-response systems are poorly designed, and could causes big headaches for administrators of legitimate e-mail newsletters (such as NewsScan Daily) that go out to large numbers of people. "Big corporations may be able to afford to hire someone to sit in front of a computer and spend all day proving they're not a spam bot, but nonprofit groups, individuals and smaller companies probably can't," says McCullagh. Earthlink has already announced its intentions to make a challenge-response system available to subscribers by the end of May, and other ISPs may follow suit — a scenario that has veteran list operators concerned. Dave Farber, a computer scientist at the University of Pennsylvania who runs the "interesting people" list, says: "If I start getting a flood of challenges from Earthlink IPers that require my response I will most likely declare them spam and you will stop receiving IP mail. I fully expect this to be the case for almost all the legitimate mailing lists you are on and count on." Meanwhile, editors at the popular Macintosh newsletter TidBits, have told readers: "Be warned that we will not answer any challenges generated in response to our mailing list postings. Thus, if you're using a challenge-response system and not receiving TidBits, you'll need to figure that out on your own." (CNet News.com 27 May 2003)

Category 33.2 *Spam, spim, spit & splogs*

2003-06-02 **law school spam course seminar marketing e-mail**

NewsScan

LAW SCHOOL DISHES UP COURSE ON SPAM
Students at John Marshall Law School in Chicago will be able to bone up on the legal issues surrounding unsolicited commercial e-mail this fall, in what's reputedly the first law school course offered dealing exclusively with the subject of spam. "This seminar will investigate legal and policy issues raised by e-mail marketing and spam," reads the description for associate professor David Sorkin's seminar titled "Current Topics in Information Technology Law: Regulation of Spam and E-mail Marketing." Sorkin's course will address "litigation and legislation involving spam and e-mail marketing; the application of tort law and other traditional doctrines to spam; concerns related to constitutionality, jurisdiction, extraterritoriality, privacy, content and public policy; regulatory perspectives; issues faced by Internet service providers and legitimate e-mail marketers; legal aspects of blacklisting and other antispam measures; and other relevant issues." (CNet News.com 2 Jun 2003)

Category 33.2 *Spam, spim, spit & splogs*

2003-06-25 **spam E-Mail Ronnie Scelson spammer**

NewsScan

SPAMMER: 'I HATE SPAM AS MUCH AS THE NEXT GUY'
Ronnie Scelson, known as the Cajun King of Spam, sees himself as a good spammer, not a bad spammer: "I hate spam as much as the next guy. What I do is not illegal. It's the people who spam sex, Viagra, and get-rich-quick schemes that give commercial e-mailers a bad name. He says that the 60-70 million ads he send out each day all give customers the option to be removed from mailing lists, do not hide behind forged e-mail addresses, do not get routed through foreign relays, and always leave contact information. Scelson makes more than $30,000 a month when business is good, and lives a typical middle-class life — except that he keeps a 9mm gun close to him because his life is threatened so often by anti-spammers. (USA Today 25 Jun 2003)

Category 33.2 *Spam, spim, spit & splogs*

2003-07-28 **spam costs e-mail insfrastructure**

NewsScan

THE COSTS OF SPAM (NOT INCLUDING BLOOD PRESSURE MEDS)
Spam costs senders almost nothing, but takes a heavy toll on those who receive it. Ferris Research says the cost of spam is $10 billion in the U.S.; Nucleus Research pegs the figure at $87 billion. Is the problem being overblown? Wharton School marketing professor Peter S. Fader says: "I am deeply skeptical that these crude top-down methods are accurate. Hitting the delete key is far more efficient than carrying your physical mail from the mailbox over to the trash can." And he even sees an upside: "Spam, although it is a bad thing per se, is fostering the growth of the e-mail infrastructure." But that new infrastructure also comes with a price: Ferris Research says corporations will spend $120 million this year on antispam systems, and The Radicati Group claims the correct figure is closer to $635 million. Ah, what to do, what to do? America Online now discards, each day, nearly 2 billion e-mail messages flagged as spam — but then has to contend with complaints [including NewsScan] about "false positives" (mail falsely treated as spam). Ferris Research says: "We think companies lose $3 billion dealing with false positives." (New York Times 28 Jul 2003)

Category 33.2 *Spam, spim, spit & splogs*

2003-08-25 **spam spammer New Zealand give up threats**

NewsScan

NEW ZEALAND SPAMMER 'OUTED' — SAYS HE'LL GIVE IT UP
Shane Atkinson, a New Zealand man who was recently identified in a local newspaper as a major spammer, says he's giving up his business after being inundated with threatening phone calls and having his personal information posted on the Net. And while vigilantes may rejoice at such intimidation methods, industry analysts says the potential for wrongful targeting is too great and, in any event, there's always a steady supply of replacements. "You'll put a dent in it but somebody else will be there to take his place," says Gartner research director Maurene Caplan Grey. "The spam kings know how to get around the system. The only ones you'll frighten are the occasional spammers trying to make a few extra bucks this weekend." According to a recent estimate, about 200 spammers are responsible for 90% of the spam-mail sent out globally. Meanwhile, it's not just the spammers who profit from their activities; other beneficiaries include the providers of e-mail addresses, suppliers of spamming software, offshore Internet service providers and even legitimate spam-filtering software vendors. (TechNewsWorld/E-Commerce Times 25 Aug 2003)

Category 33.2 *Spam, spim, spit & splogs*

2003-09-02 **Spammer spiders chain letters collect e-mail addresses U.S. DoE Department Energy hoax advisory website web search usernames Spamfire**

NIPC/DHS

September 02, CNN — Spammers turn to chain letters to collect addresses.

While not as efficient as "spiders" which automatically crawl the Web in search of addresses, computer experts warn that some spammers are using chain letters to collect e-mail usernames. "Chain letters are the ideal place to collect addresses. I've seen several hundred on one e-mail," said Bill Orvis, who maintains the U.S. Department of Energy's hoax advisory Web site. "Just by forwarding a message to a dozen friends, it only takes a few generations before you fill the network with messages," he said. Michael Herrick, whose Spamfire software helps individual users filter junk e-mail, doesn't think spammers are using chain letters in this way. Herrick, however, admits that the practice could be a good way to bypass e-mail filters which block messages from senders who are not known to the recipient. Spammers could use chain letters to discover the addresses of people with whom you frequently communicate. Spam purporting to be from someone in your address book would sneak by filters.

Category 33.2 *Spam, spim, spit & splogs*

2003-09-11 **you've got spam sex to get attention e-mail holidays tricks terminator for governor**

NewsScan

BREAKING NEWS: YOU'VE GOT SPAM
Analyst Matt Cain of META Group says that spammers "used to use sex to get your attention, then e-mails tied to holidays like Mother's Day. Now, it's topical come-ons" such as breaking-news headlines "The intent of every spammer is to try every trick to get you to open a message." And Ken Schneider of Brightmail thinks the trend will grow and grow: "You can be sure there will be substantially more spam during the presidential primaries next year. People will take advantage of any current event to make a buck." More than 20 million messages with references to the California recall — many of them hawking "Terminator for Governor" T-shirts and adult DVDs for another candidate — were sent in the past month, and 100 million are expected before the recall election is over. Gubernatorial candidate and porn star Mary Carey is angry that a distributor of adult DVDs is using her run for office to sell two of her films for $14.95. "I'm very upset, because it offends people, and they're profiting from my name." (USA Today 11 Sep 2003)

Category 33.2 *Spam, spim, spit & splogs*

2003-09-15 **anti-spam pay stop fighting Global Removal do-not spam list**

NewsScan

ANTI-SPAM EFFORT WOULD PAY SPAMMERS TO STOP
A new anti-spam service, called Global Removal, is taking a different approach to fighting spam — it's proposing to pay spammers for cooperating with their effort. Internet users fed up with junk e-mail would pay a $5 lifetime fee to have their e-mail addresses put on a Global Removal do-not-spam list. Addresses on the list would be cross-referenced and deleted from mailing lists maintained by Global's partners, which include more than 50 known spammers and an equal number of legitimate e-mail marketers. These partners would be rewarded for their diligence through an affiliate program, which would pay $1 for every new subscriber that they bring to the service. In order to avoid a new flood of spam touting Global Removal's service, the spammers would be allowed to send only one message to their purged mailing lists. "Despite the urban legend, these guys don't really want to keep these names on their lists if they know that the people aren't going to be receptive to advertising," says Global CEO Tom Jackson. "They can make more money for less effort through our program." Critics say the flaw in Global's sales pitch is that subscribers would still receive junk e-mail from spammers not affiliated with Global and that Global's spammers could always renege on their deal and go back to their old lists. One intellectual property lawyer says, "It's a little like paying protection money to mob bosses. There's precious little assurance about the comprehensiveness of the protection, or that the prices won't go up at the whim of the 'bosses.'" Still, if spammers "could be assured some minimum bit of income by not sending me mail, it's a better deal for them and a relief to me." (Wired.com 15 Sep 2003)

Category 33.2 *Spam, spim, spit & splogs*

2003-10-06 **spam fight legitimate e-mail unsolilicted**

NewsScan

FIGHTING SPAM: RAISE THE BRIDGE OR LOWER THE WATER?
Many software experts now believe that the best way to fight spam is not by targeting it directly but instead by concentrating on the identification of legitimate mail. VeriSign executive Nico Popp explains, "People have been spending all their time creating filters to find the bad guys. We want to turn that on its head and find ways to identify the good guys and let them in." The idea would be to develop the Internet equivalent of caller ID, with a technology that identifies senders and lets receivers presume that un-identified senders are sending junk mail. Richard Reichgut of AuthentiDate says, "It's not easy to change something as successful and widely used as e-mail. But the only way to fix e-mail is to have a strong way to know who is sending you mail." (New York Times 6 Oct 2003)

Category 33.2 *Spam, spim, spit & splogs*

2003-10-09 **spam elude antispam cracker unsolicited e-mail new methods**

NewsScan

NEW BREED OF 'SPACKERS' ELUDES ANTISPAMMERS
Computer crackers have joined forces with spammers to devise new ways of defrauding hapless Internet users. The latest technique enables spammers to create Web sites that are virtually untraceable, making it impossible for antispammers to shut down those sites by conventional means. Typical of the scam is a group in Poland currently advertising "invisible bulletproof hosting" for $1,500 a month, which provides its clients protection from network sleuthing tools such as 'traceroute' and 'whois' by routing traffic through thousands of hijacked computers (most of them home computers running Windows and having broadband connections). The technique is effective. "You're not going to have much success trying to follow IP addresses through hacked hosts," says one security researcher. "About all you can do is follow the money — sign up for whatever it is they're selling and try to figure out who's behind the whole thing." Fueling the new tactics is an influx of "engineers who have been laid off or fired, and people who really know what they're doing with networking and DNS," says Steve Linford, head of the Spamhaus Project. "Hackers used to detest spammers, but now that spamming has become such a big business, it's suddenly cool to be a spammer." (Wired.com 9 Oct 2003)

Category 33.2 *Spam, spim, spit & splogs*

2003-10-21 **spam decoy Yahoo mail Address Guard base name junk**

NewsScan

YAHOO DEPLOYS E-MAIL DECOYS
Yahoo now offers its e-mail customers a new way to evade spam — its AddressGuard feature allows subscribers to create a fictitious "base name" and then up to 500 variations on that name that can be used in online shopping and banking transactions as well as online community discussions. If an address starts to draw spam, it can be discarded and another one selected. Yahoo's anti-spam arsenal also includes new spam-blocking software along with the option to receive e-mail only from known sources. Yahoo has also changed its rule on viruses, now requiring users to scan all attachments before downloading them. Yahoo VP Brad Garlinghouse says the company has to keep tweaking its technical defenses because legal battles can't do the job alone. "Legislation and litigation, it's something of a whack-a-mole problem," he says, referring to the arcade game where players are challenged to hit an ever-increasing number of pop-up figures. An August survey of Yahoo users found that 77% said they would rather clean a toilet than sort through the junk e-mail in their in-box. (Reuters 21 Oct 2003)

Category 33.2 Spam, spim, spit & splogs

2003-11-09 **spam fraud blacklist lawsuits investigation blocking spoofing DDoS zombie**

NYT
http://www.nytimes.com/2003/11/09/business/yourmoney/09spam.html?th=&pagewanted=print&position=

The Spamhaus Project <http://www.spamhaus.org/> was profiled in a New York Times article by Saul Hansell in November 2003. One of the best indications that the group of volunteers running this project have been effective is that they have often been assaulted by spammers using DDoS attacks.

Notes from the Web site:

* Spamhaus tracks the Internet's Spammers, Spam Gangs and Spam Services, provides dependable realtime anti-spam protection for Internet networks, and works with Law Enforcement to identify and pursue spammers worldwide.

* The Spamhaus Block List (SBL) is a realtime blocklist of spam sources and spam services. The SBL can be used by almost all modern mail servers, by setting your mail server's anti-spam DNSBL feature (sometimes called "Blacklist DNS Servers" or "RBL servers") to query sbl.spamhaus.org. Use of the SBL is free for users with normal mail servers (but networks with heavy email traffic should see DataFeed).

* The Spamhaus Exploits Block List (XBL) is a realtime database of IP addresses of illegal 3rd party exploits, including open proxies (HTTP, socks, AnalogX, wingate, etc), worms/viruses with built-in spam engines, and other types of trojan-horse exploits.

* The Register Of Known Spam Operations (ROKSO) database collates information and evidence on the known spammers and spam gangs, hard-line spam operations that have been terminated by a minimum of 3 consecutive Service Providers for serious spam offenses. ROKSO assists ISP Abuse Desks and Law Enforcement Agencies.

The section on ROKSO has the following information:

200 Known Spam Operations responsible for 90% of your spam.

90% of spam received by Internet users in North America and Europe can be traced via redirects, hosting locations of web sites, domains and aliases, to a hard-core group of around 200 known spam operations, almost all of whom are listed in the ROKSO database. These spam operations consist of an estimated 500-600 professional spammers loosely grouped into gangs ("spam gangs"), the vast majority of whom are operating illegally, and who move from network to network seeking out Internet Service Providers ("ISPs") known for lax enforcing of anti-spam policies.

These are the spammers you definitely do NOT want on your network.

Many of these spam operations pretend to operate 'offshore' using servers in Asia and South America to disguise the origin. Those who don't pretend to be 'offshore' pretend to be small ISPs themselves, claiming to their providers the spam is being sent not by them but by their non-existent 'customers'. Some set up as fake networks, pirate or fraudulently obtain large IP allocations from ARIN/RIPE and use routing tricks to simulate a network, fooling real ISPs into supplying them connectivity. When caught, almost all use the age old tactic of lying to each ISP long enough to buy a few weeks more of spamming and when terminated simply move on to the next ISP already set up and waiting.

ROKSO is a "3 Strikes" register. To be listed in ROKSO a spammer must first be terminated by a minimum of 3 consecutive ISPs for AUP violations. IP addresses under the control of ROKSO-listed spammers are automatically and preemptively listed in the Spamhaus Block List (SBL).

For Law Enforcement Agencies there is a special version of this ROKSO database which gives access to records with information, logs and evidence too sensitive to publish here.

Category 33.2 *Spam, spim, spit & splogs*

2003-11-11 **christmas spam spammonger Clearswift cheap loans festive gifts**

NewsScan

ALL I WANT FOR CHRISTMAS IS… MORE SPAM?
While you're decking the halls with boughs of holly, spammongers are cooking up their own holiday plans, which (surprise!) involve sending even more spam than usual! Net filtering firms report that spammers are already altering their messages in an attempt to cash in on the festive season, offering more single products and high-tech gadgets such as DVD burners as potential gifts. Oh, and of course — more cheap loans to pay for it all! "Not only are spammers developing more and more cunning ways of getting around e-mail filtering technology, but their marketing strategy is clearly up to scratch, too," says Alyn Hockey, research director at Clearswift, a spam filtering firm. Clearswift reports that the number of spam e-mails offering cheap loans aimed at Christmas shoppers doubled in October as a percentage of overall spam. (BBC News 11 Nov 2003)

Category 33.2 *Spam, spim, spit & splogs*

2003-11-13 **Spam clogs blogs ISP prevent spammers viagra Comment Spam Manifesto bloggers e-mail accounts disabled**

NewsScan

SPAM CLOGS BLOGS

Most weblogs are designed to allow readers to post comments on entries, but that capability is being abused by spammers, who leave remarks like "Sounds great!" submitted by names like "Generic Viagra," complete with links to questionable sites. Howard Rheingold, a futurist who touts the power of online communities, worries that the recent invasion could derail the revolution in public discourse just as it's gathering steam. "It forces you to either turn off the comments and lose some of the value of the medium, or spend your time deleting spam," says Rheingold. Meanwhile, some inveterate bloggers are taking matters into their own hands. Adam Kalsey, who's run his own blog for the past three years, has penned a "Comment Spam Manifesto," which warns spammers: "What you failed to understand is that bloggers are smarter, better connected and more technologically savvy than the average e-mail user. We control this medium that you are now attempting to exploit. You've picked a fight with is and it's a fight you cannot win." Kalsey tracks spammers down and reports them to their ISPs and domain registers in an effort to get their accounts canceled. "The blog immune system does seem to be responding," he says, noting that he receives help from other bloggers in his spam-slamming activities. (AP 13 Nov 2003)

Category 33.2 *Spam, spim, spit & splogs*

2003-11-16 **spam anti-spam human error AT&T e-mail message**

RISKS; http://boston.internet.com/news/article.php/3097171 23 4

Human Error Leads to AT&T's Anti-Spam Gaffe

After seeing a rush of spam, and brainstorming possible remedies, AT&T sent out a mass e-mailing to business partners and customers asking for the IP addresses of all outbound SMTP servers (to be used for a white list), threatening to cut off e-mail access of nonresponders. Subsequently, they sent a follow-up apology, with a request to disregard the first e-mail, claiming that the original notices went out as a result of "human error". [Source: Ryan Naraine, 22 Oct 2003, Jupitermedia Corporation; PGN-ed]

[For those who don't get it, MK adds that most spammers do not belong to the ISPs they spam.]

Category 33.2 *Spam, spim, spit & splogs*

2003-11-22 **Spam murder threat Charles Booher kill five years prison 22 calibre**

NewsScan

GETTING SOME RAGE OUT: MAN THREATENS MURDER AFTER GETTING SPAMMED
A few months ago 44-year-old Charles Booher, a self-described non-violent person, went bonkers after receiving too much spam, and sent a series of e-mail messages threatening to kill the spammer. Now Booher's been charged with 11 violations of interstate communications, for which he could be sentenced to five years in prison and a $250,000 fine if found guilty. His current thoughts: "If I could go back, I wouldn't have done it. I would have realized sooner that I needed to shut my Web site down, to shut down my e-mail, and to re-evaluate the way I was using the Internet." In one of the messages he told the spammer: "I will locate you, disable you using a quick 22 calibre shot to your lower spine and then duck tape... I am going to cut into the left side of your brain using a power drill and an ice pick." Reflecting on the messages he sent to the spammer, Booher now says: "It felt like I was just getting some rage out." (San Jose Mercury News 22 Nov 2003)

Category 33.2 *Spam, spim, spit & splogs*

2003-12-02 **spammers anti-spam groups targeted e-mail worms Spamhaus Project Steve Linford**

NewsScan

SPAMMERS TARGET ANTI-SPAM GROUPS WITH E-MAIL WORM

Virus experts say a new worm, dubbed W32/Mimail-L, has been unleashed by a vengeful spammonger intent on paralyzing anti-spam groups via a crippling barrage of data — a so-called denial of service attack. "It's the third Mimail variation to come after us, except this one is trying to do more," says Steve Linford, founder of the Spamhaus Project. The nasty worm comes as an attachment to an e-mail from "Wendy" who describes an erotic encounter and then offers photos. Clicking on the attachment launches the worm. In a new twist, a follow-up e-mail is sent to the infected user announcing that an order for a CD containing child pornography images will be sent to their mailing address. Virus experts say the impact of this latest worm has been minimal, compared with the problems caused by last summer's plague of viruses, "but what this shows is that there is more evidence that virus writers and spammers are now colluding," says Sophos senior technology consultant Graham Cluley. (Reuters 2 Dec 2003)

Category 33.2 *Spam, spim, spit & splogs*

2003-12-31 **spim instant messenger spam clogging users pornography e-mail marketers**

NewsScan

GET READY FOR SPIM

Instant messenger spam, dubbed "spim," is increasingly clogging users' computers, popping up with the real-time regularity of instant messages and annoying users who complain they're now receiving several messages a day. Users can either accept or decline the spim, which often contains a link to — what else? — a pornography site. Ferris Research estimates about 500 million spim messages were sent in 2003, double the number sent in the previous year. And while instant-messenger spam "isn't nearly the industry that e-mail spam is,… it's starting to increase," says the CEO of an antispam consulting firm. Experts warn that the recent crackdown on conventional spam may push illicit marketers to explore new avenues, including instant messaging. "The irony is that focusing like a laser on our No. 1 concern — spam — has painted e-mail spammers into a corner like never before and incited them to find other ways to try and reach our membership online," says an AOL spokesman. (Wall Street Journal 31 Dec 2003)

Category 33.2 Spam, spim, spit & splogs

2004-01-19 **phishing SPF senders permitted from DNS e-mail servers authentication anti-spam**

RISKS; http://spf.pobox.com/ 23 16ff

SPF = "SENDER POLICY FRAMEWORK" OR "SOME PROBLEMS to FACE"?

Andrew Rose posted a note in RISKS alerting readers to a new project called SPF (Sender Policy Framework, <http://spf.pobox.com>) that uses "SPF records" to be published in the domain name system (DNS). E-mail sent with fraudulent headers would be identified because the sender would not match an authorized SMTP server registered in the DNS by means of these records. Rose wrote, "The technical work on SPF is now complete and adoption has started. Several thousand domains have published SPF records including some very large domains such as aol.com. Plugins exist for most of the popular MTAs - the only notable exception being MS Exchange." [MTA = Message Transfer Agent]

In a sharply worded riposte in RISKS 23.18, Markus Fleck-Graffe attacked the whole idea of SPF, pointing to these failings among others:

1) All forwarded e-mail must be rewritten (e.g., mailing lists must destroy the original header to substitute their own authorized domain);

2) Forwarded e-mails require a database of reverse mappings to allow bounce messages to reach the original sender;

3) Spammers will subvert the system by establishing their own SPF-enabled infrastructure using temporary domain names;

4) Worms will use the authentic e-mail addresses of their infected host PCs.

Also in RISKS 23.18, Ian Jackson criticized the SPF group for not using the IETF RFC mechanisms to stimulate discussion and improvements of the proposal but rather, "going for a publicity campaign to `bounce' people into adoption."

In RISKS 23.19, Lawrence Kestenbaum detailed the misery caused by spammers and worms that use his e-mail address in FROM lines, causing thousands of bounce messages to arrive at his address daily. He wrote in exasperation, "The critics of SPF suggest that spammers would simply find or invent other addresses to use. Frankly, I don't care about that, so long as they stopped plastering my personal address on hundreds of thousands of fraudulent and disreputable spam messages and viruses, and clogging my server's net connection with vast piles of misdirected bounces."

In RISKS 23.21, Ben Rosengart recommended doing away with the SRS (Sender Rewriting Scheme) part of SPF, leaving forwarded e-mail with the original header unchanged. Peter da Silva pointed out that "Implementing SPF would do nothing for the people receiving thousands of bounces (myself included). It would simply add another filter that bounced messages back to us because `we' weren't using the right server."

Dmitri Maziuk added to the conversation with the observation that "We know that slapping a band-aid onto implementation to fix deficiencies in design doesn't work and creates more problems…." He wrote, "We already have directory servers, we already have digital signatures. All we need is a way to query Domain Name Service for directory server of a domain, and a standard directory query-response for an e-mail address and associated public crypto key." He also darkly suggested that there would be resistance to this scheme from political forces who actually support spam for their own purposes: "…all "anti-spam" legislations are really there to legalize it. Ergo, all you're going to achieve by implementing SPF, blocklists, blacklists, whatever, is to open yourself to lawsuits from `legal' spammers."

In RISKS 23.23, Jonathan de Boyne Pollard bitterly points out that SPF is a short-term move in an arms race and that it fails to solve the underlying problems of SMTP (which include failure to authenticate message origins). He ends, "perhaps the fact that widespread adoption of SPF will do serious damage to the SMTP mail architecture is a good thing. In the battle against unsolicited bulk mail, we've concentrated upon the wrong problem time after time, with mechanisms that address the wrong thing and that don't address the actual "unsolicited" and "bulk" qualities of undesirable mail. SMTP has become less usable, more patchy, and more balkanised with each new bodge, yet continues to bend and not quite break completely. Perhaps the adoption of SPF will turn out to be the straw that finally breaks the camel's back, and that thus finally forcibly weans us off this bad habit of addressing the wrong problem."

Category 33.2 *Spam, spim, spit & splogs*

2004-01-22 **AOL email caller ID anti spam**

NewBits; http://zdnet.com.com/2100-1104_2-5145065.html
http://msnbc.msn.com/id/4028710/
http://www.globetechnology.com/servlet/story/RTGAM.20040122.wadware0122/BNStory/Technology/

AOL tests caller ID for e-mail

America Online is testing an antispam filter intended to accurately trace the origin of e-mail messages, a move that could bring new accountability to the Net if it proves reliable. The online unit of media giant Time Warner last week implemented SPF, or Sender Permitted From, an emerging authentication protocol for preventing e-mail forgeries, or spoofing. The trial involves the company's 33 million subscribers worldwide and is the first large-scale test for the protocol, which standards groups are considering along with various other e-mail verification proposals.

Category 33.2 *Spam, spim, spit & splogs*

2004-01-23 **Can-Spam Act California law suit ineffective useless stupid pointless legislation**

NewsBits; http://www.wired.com/news/business/0,1367,62020,00.html

With This Law, You Can Spam

California lawyers and law enforcement officials continued their assault on the Can- Spam Act Thursday, calling it ineffective and warning attendees at a conference on spam and the law that a solution to the spam scourge is still a distant dream. Signed into law by President Bush on Dec. 16, 2003, the Controlling the Assault of Non-Solicited Pornography and Marketing Act requires e-mail marketers to include legitimate return addresses and opt-out information in all e-mail messages that they send.

Category 33.2 *Spam, spim, spit & splogs*

2004-01-27 **spam history culture documented**

NewsScan

THE CULTURE OF SPAM

Who would ever have thought that spam would someday be chic, the subject of an avant-garde show titled "Reimaging the Ordovician Gothic: Fossils from the Golden Age of Spam." The display considers how future historians would view today's culture if all they had to go on was a vast collection of junk e-mail. A classification scheme sorts the spam into such categories as Real Estate, Urgent Messages, Work at Home, Goods and Personal Appearance, and the artists have scrawled representative excerpts from each on the walls of a gallery stairwell and packed suitcases with diet pills, house blueprints and some of the other wares frequently hawked online. Just as paleontologists have a hard time recreating the real Ordovician period, which ended about 443 million years ago, the perceptions about modern culture drawn from spam are quite misleading (and humorous): "Little is known of the physiology of the Ordovician body, but the outward appearance was greatly enhanced by drugs which shaped one to look more like those celebrated in Ordovician PORNOGRAPHY. These pills occasionally took the form of patches and other accessories. It is believed that, for a time, these patches took on significance as ultimately ceremonial jewelry," reads one of the plaques in the show. The display is on view at the Spaceworks Gallery in Manhattan through Feb. 7. (AP 27 Jan 2004)

Category 33.2 *Spam, spim, spit & splogs*

2004-01-28 **FTC adult spam labels Can-Spam Act**

NewsBits; http://zdnet.com.com/2100-1104_2-5149613.html
http://www.washingtonpost.com/wp-dyn/articles/A57681-2004Jan28.html

FTC proposes adult spam labels

The Federal Trade Commission on Wednesday proposed a mandatory tag for commercial e-mail that contains pornographic material--a stipulation of the new federal antispam law enacted this month. The FTC, which is charged with enforcing the Can-Spam Act, short for Controlling the Assault of Non-Solicited Pornography and Marketing, proposed a rule that would require senders of adult-related e-mail to include the phrase, "Sexually-Explicit-Content:" in messages. That way, recipients would be able to recognize and easily filter such e-mail before viewing it, according to the FTC and backers of the law.

Category 33.2 *Spam, spim, spit & splogs*

2004-02-02 **anti-spam spam countermeasure penny message micropayment Microsoft Yahoo defeat**

NewsScan

PENNY A MESSAGE?

Microsoft and Yahoo are giving new life to the debate over whether imposing a small charge on senders of bulk e-mail messages would be the best way to defeat spam. Yahoo executive Brad Garlinghouse says that requiring electronic stamps for e-mail would force mailers to send only those offers a significant number of people might accept. "All of a sudden, spammers can't behave without regard for the Internet providers' or end users' interests." The idea doesn't sit well with everyone. Carnegie Mellon University professor David Farber, who runs a popular e-mail list focused on technology policy, warns: "I suspect the cost of postage will start out small and it will rapidly escalate." But the Internet Service Providers are more receptive to such plans, and Linda Beck of EarthLink says: "Sending large volumes of e-mail involve costs that are paid for by the ISPs and eventually by consumers. Should there be some sort of financial responsibility borne by the originators of these large-volume programs? I think there should." On the other hand, Charles Stiles, the manager of America Online's postmaster department, suggests that the plan simply won't do what it's meant to do, and reminds everyone that "it is the spammers who are the ones with the big pockets." (New York Times 2 Feb 2004)

Category 33.2 *Spam, spim, spit & splogs*

2004-02-03 **spam expensive Transatlantic Consumer Dialogue junk e-mail**

NewsScan

SPAM ISN'T JUST A PAIN: IT WILL ALSO COST YOU MONEY

A majority of consumers surveyed by the Trans-Atlantic Consumer Dialogue said they are shopping less on the Internet — or not there at all — because they dislike receiving unsolicited junk e-mail. The report says, "It is very clear that the majority of citizens are very troubled by unsolicited commercial e-mails. It is also very clear that bona fide businesses are losing money because the disreputable image of spam is making consumers uneasy about engaging in e-commerce." Marc Rotenberg of the Electronic Privacy Information Center concurs with the report's findings and says: "If you continue at this pace, in five years from now I do not think the Internet will be very popular." Peter Ferguson, chairman of the OECD working group on information security and privacy, explains that most governments now view the Internet as a key to the global economy, and he warns: "Spam has certainly the capacity to interfere with that." (Reuters/Los Angeles Times 3 Feb 2004)

Category 33.2 *Spam, spim, spit & splogs*

2004-02-05 **spam spammers junk e-mail service names alias inbox random number name generator**

NewsScan

WHAT'S IN A NAME?

Ever wonder how spammers come up with all those weird aliases they use to pepper your inbox with unwanted messages? Names like Elfrieda Billman and Beiderbecke P. Sawhorse? One possible source is a Web site run by August Kleimo, who built a random name-generator (www.kleimo.com/rand/name.cfm) using all the surnames from the 1990 U.S. census (free on the Census Bureau's Web site). Kleimo says he gets about 3,000 visitors a day, many of them hunting for unusual names to use for fantasy gaming characters, but admits it's possible that spammers are picking up some ideas from his site also. Other name-generator sites include one by Mike Campbell, a software developer and amateur etymologist. Behind the Name (www.behindthename.com/random.html) allows visitors to generate names in various languages, from Icelandic to classical Greek. Chris Pound, who works in the IT department at Rice University, has written more than 40 name generators, one of which merges names from the worlds of Harry Potter and Dickens (www.ruf.rice.edu/~pound). Security experts say it's difficult to outsmart spammers who use randomly generated names that can slip under the radar of so-called Bayesian filters, which target common words used in spam, like Viagra. A human might detect an obviously fake name, but "a filter can't really see the irony of Tupperware J. Smithington," says ePrivacy Group's chief privacy officer. (New York Times 5 Feb 2004)

Category 33.2 *Spam, spim, spit & splogs*

2004-02-06 **spam anti-spam lawsuits Penny Black Microsoft**

NewsScan

MICROSOFT'S "PENNY BLACK" WOULD MAKE SPAMMERS AY A PRICE

Microsoft's new "Penny Black" research project is named after an 1830s stamp used in Britain that reversed the cost of postage to the sender, rather than the original method of charging the letter recipient — but the Microsoft plan would go the other way, and force the sender of an e-mail to incur some kind of cost. Microsoft also is aiming to raise the cost of sending mass e-mail in other ways: it is suing e-mail marketers in New York and Washington for sending massive e-mailings that that slow down the Internet. (Reuters/Los Angeles Times 6 Feb 2004)

Category 33.2 *Spam, spim, spit & splogs*

2004-02-12 **antispam challenge-response keyspace automated retry weakness problem CAPTCHA**

RISKS 23 19

CHALLENGE/RESPONSE SPAM BLOCKING HAS WEAKNESSES

Thomas Harrington reported on weak implementation of the challenge-response system (CAPTCHA) designed to identify human beings to prevent spam from reaching Earthlink customers. Seems the system is using only a limited number of images of funny-looking numbers and letters that a person can interpret but a 'bot can't. In addition, the system seems to allow unlimited retries, opening the method to automated attack, especially since the total number "of correct answers is very small, so this would be nowhere near as challenging as a typical dictionary-style attack."

Category 33.2 *Spam, spim, spit & splogs*

2004-02-12 **spam volume e-mail Hotmail Microsoft statistics**

http://download.microsoft.com/download/2/e/2/2e2850b8-2747-4394-a5a9-d06b5b9b1a4c/callerid_email.pdf

HOT GRIDDLE FOR SPAM

In Microsoft's "Caller ID for E-Mail: The Next Step to Deterring Spam," the author states, "As of mid-2003, about 83% of the e-mail messages received by Microsoft® Hotmail® on a typical day are spam, unwanted and unsolicited e-mail sent indiscriminately to users. That's around 2.5 billion out of nearly 3 billion messages, and the numbers keep climbing."

Category 33.2 *Spam, spim, spit & splogs*

2004-02-15 **spam Website masquerading deception US government Federal Trade Commission FTC**

NewsScan

FTC WARNING ABOUT PRIVATE NO-SPAM REGISTRY

The Federal Trade Commission has cautioned computer users not to fall victim a Web site claiming to offer an e-mail version of the federal do-not-call registry. Despite the official-looking appearance of the site's URL, the "Do Not Email Registry" has no affiliation with the U.S. government, and is apparently a scam for collecting e-mail addresses on behalf of spammers. However, the site's operators say their registry serves "legitimate direct marketers" who want to make sure their mailings don't go to spam opponents. The e-mail addresses collected by the registry are made available to bulk mailers in an encrypted form allowing them to check for any overlap with their own mailing lists without seeing the actual addresses. (Washington Post 15 Feb 2004)

Category 33.2 *Spam, spim, spit & splogs*

2004-02-20 **anti-spam do-not-spam lists Federal Trade Commission FTC mixed success**

NewsScan

DON'T-BOTHER-ME LISTS HAVE MIXED SUCCESS

A poll by the Associated Press has found that three-fourths of the people who signed up for the government's new do-not-call registry received fewer telemarketing calls, but the same poll found that few people noticed any difference in the six weeks since a new federal anti-spamming law took effect. The anti-spam bill encourages the Federal Trade Commission to create a do-not-spam list of e-mail addresses, but FTC officials are doubtful of that approach, because of the decentralized and unregulated nature of the Internet. (San Jose Mercury News 20 Feb 2004)

Category 33.2 Spam, spim, spit & splogs

2004-02-24 **e-mail sender authentication Caller ID spoofing spam**

http://www.microsoft.com/mscorp/twc/privacy/spam_callerid.mspx

In February 2004, Microsoft announced the "Caller ID for E-Mail Technical Specification." The Microsoft announcement included the following text:

"Caller ID for E-Mail: The Next Step to Deterring Spam" is the Microsoft draft specification to address the widespread problem of domain spoofing. Domain spoofing refers specifically to the use of someone else's domain name when sending a message, and is part of the larger spoofing problem, the practice of forging the sender's address on e-mail messages.

Caller ID for e-mail would verify that each e-mail message originates from the Internet domain it claims to come from. Eliminating domain spoofing will help legitimate senders protect their domain names and reputations, and help recipients more effectively identify and filter junk e-mail.

• Send your comments. We are circulating this initial technical specification for comment because we believe that your feedback can help make it stronger. Before sending a response, please make sure that you have reviewed and that you agree to the terms and conditions outlined in the specification. Please send your questions, suggestions, and comments to LessSpam@microsoft.com.

• Implement the Caller ID for E-Mail specification. For instructions on how to protect your domain name from spoofing using Caller ID for e-mail, please see "Protecting Domain Names from Spoofing: A Guide for E-Mail Senders."

If you're interested in implementing this specification in software, please review the terms of the Caller ID for E-Mail Implementation License before you begin, as the patent license expands upon the rights that Microsoft would grant you or your organization.

The site includes links for two documents: "Caller ID for E-Mail: The Next Step to Deterring Spam" and "Protecting Domain Names from Spoofing: A Guide for E-Mail Senders" which are both available as PDF documents.

Category 33.2 Spam, spim, spit & splogs

2004-03-12 **electronic e-mail junk spam anti-spam ISP lawsuit litigation**

NIPC/DHS

March 10, Associated Press — ISPs sue over spam e-mails.

Some of the nation's largest Internet providers, in an unusual joint effort, said Wednesday, March 10, they filed six lawsuits against hundreds of people who were accused of sending millions of unwanted e-mails in violation of the new U.S. law against "spam." The legal actions represent the first major industry actions under the "can spam" legislation that went into effect January 1. The lawsuits were filed in federal courts in California, Georgia, Virginia and Washington state. The companies said the defendants include some of the nation's most notorious large-scale spammers. The Internet providers--collectively with tens of millions of subscribers--said they shared information, resources and investigative information to identify some of the defendants. Dozens of those named in the lawsuits, however, were identified only as "John Doe" defendants who were accused of e-mailing unwanted pitches for prescription drugs, herbal potions and weight loss plans. The "can spam" legislation requires unsolicited e-mails to include a mechanism so recipients could indicate they did not want future mass mailings. The law also prohibits senders of unsolicited commercial e-mail from disguising their identity by using a false return address or misleading subject line, and it prohibits senders from harvesting addresses off Websites.

Category 33.2 *Spam, spim, spit & splogs*

2004-03-15 **mobile cell phone spam control Federal Communications Commission**

NIPC/DHS

March 11, Washington Post — FCC sets sights on mobile phone spam.

The Federal Communications Commission (FCC) today took its first steps toward banning spam that targets mobile phones and other wireless devices. The FCC said it will ask the public to submit comments on the best ways to prevent the growth of mobile phone spam, a problem that is still uncommon in the United States though experts agree that it--along with instant messaging spam--is getting worse. The commission is required to develop the rules because of a recently enacted federal law that tries to stop the expanding spam problem. Signed into law by President Bush last December, the Can-Spam Act mostly targets e-mail spam but recognizes that cellphones and other wireless devices are prime targets for unsolicited advertising. The law gives the FCC less than a year to draft rules to allow consumers to prevent spammers from contacting them on their wireless devices. The commission also is seeking public comment on whether commercial messages should be clearly labeled and whether mobile phone service providers have to get authorization from their customers before sending them commercial messages.

Category 33.2 *Spam, spim, spit & splogs*

2004-03-19 **spam commerical Websites block AOL privacy strict**

NewsScan

SHOULD PEOPLE BE BLOCKED FROM REPLYING TO SPAM?

To defeat spammers, America Online blocks the ability of its members to visit Web sites promoted by bulk e-mailers. Most spammer messages include links that lead to Internet sites, but AOL members who now attempt to visit a blocked Web page receive an error message saying simply that a connection to the page could not be made. The result: less business for spammers. But Washington attorney Paul M. Smith, a specialist in Internet and media law, warns: "There is a service to AOL members by doing this, but there's some trade-off... because some people want to go to those sites." AOL is the first — and so far the only — Internet service provider to cut off access to commerce Web sites advertised by spam. Cindy Cohn of the Electronic Frontier Foundation calls the AOL strategy "paternalistic," even if well-intentioned. (Washington Post 19 Mar 2004)

Category 33.2 *Spam, spim, spit & splogs*

2004-03-22 **anti-spam struggle ISPs consumer corporate problem**

NewsScan

ISPs STRUGGLE TO FIND FIX FOR SPAM

Unless you've been hibernating the last six months, you know that spam not only is a consumer headache — it's turning into a corporate nightmare. U.S. companies spend an estimated $1 billion a year in extra security, human resources and lost productivity thanks to this cyber-plague, which comprises anywhere between 50-90% of all e-mail. Despite universal agreement on the problem, major ISPs have not been successful in devising a coordinated approach to fight it, relying instead on lawsuits that at best will be only marginally successful at stemming the flow. Yahoo reportedly is moving toward implementing a DomainKeys system that's used to verify the identity of an e-mail sender, while AOL has recently begun testing a DNS-based system called Sender Policy Framework (SPF). Meanwhile, Microsoft has developed its own system called Caller ID for E-mail and several other efforts, such as the Trusted E-Mail Open Standard, are also available. Experts agree that the balkanization of ISP efforts to deal with spam will delay any final solution, and they're looking to the IETF (Internet Engineering Task Force) to come up with a solution that incorporates the best features of these disparate systems. "Sooner or later, we are going to see what is going to be a compromise proposal that includes elements from the more workable proposals being put forward — DomainKeys and SPF, for example," says the CTO for Outblaze, an e-mail service provider. (CNet News.com 22 Mar 2004)

Category 33.2 *Spam, spim, spit & splogs*

2004-03-30 **anti-spam AOL sweepstakes spam victims rewarded**

NewsScan

AOL UNVEILS SPAM VICTIM SWEEPSTAKES

America Online is launching a sweepstakes program that will award victims of spam various assets seized from spammers. The top prize is a 2002 Porsche Boxster S, purchased with the proceeds from a lawsuit settled with a spammer — one of five antispam lawsuits that AOL filed in federal court last year. AOL executive VP and general counsel Randall Boe says the company sees the sweepstakes program as a "great way to teach spammers a lesson, and reward our members for their continued use of the 'Report Spam' button." The sweepstakes started at 5:00 a.m. this morning and will run till 11:59 p.m. eastern time on April 8th. Details can be found at AOL.com. (Internet News 30 Mar 2004)

Category 33.2 *Spam, spim, spit & splogs*

2004-04-01 **spam unsolicited commercial e-mail law enforcement**

NewsScan

EU'S PROBLEMS ENFORCING ANTI-SPAM MEASURES

The European Union has again ordered eight of its members to enact privacy legislation governing spam and cookies. Since the initial warning was sent in November, only Sweden has enacted the legislation, while Belgium, Germany, Greece, France, Luxembourg, the Netherlands, Portugal and Finland have not. The EU inability to enforce its own regulations makes it more difficult to get other countries to join the fight against spam and other undesirable Internet activities. (Los Angeles Times 1 Apr 2004)

Category 33.2 *Spam, spim, spit & splogs*

2004-04-06 **anti-spam laws Australia penalties spamming**

NewsScan

AUSTRALIAN JUNK E-MAIL LAWS TAKE EFFECT

Hard-core spammers will be the main target when Australia's communications watchdog begins to enforce anti-spam legislation beginning this Saturday. While penalties of $1.1 million a day will be reserved for prolific spammers, most complaints about spamming will be treated with a simple phone call, according to the Australian Communications Authority. The ACA's focus will be on compliance, says Anti-Spam team manager Anthony Wing. "We are really targeting, in the first instance, the hard-core spammers. As long as people are trying to comply in the first instance, if we get a complaint it will result in a phone call." Wing says reducing the amount of spam that hits Australia's borders is a "longer program" that requires international co-operation. (The Age 6 Apr 2004)

Category 33.2 *Spam, spim, spit & splogs*

2004-04-08 **anti-spam dot mail domain white list certified spam free**

NewsScan

ANTI-SPAM GROUP PROMOTES DOT-MAIL DOMAIN

Anti-spam organization Spamhaus is proposing a new "dot-mail" domain that would act as a "white list," guaranteeing that all mail sent from it would be spam-free. Companies with dot-mail addresses would be required to ask e-mail recipients for their permission to send mail as well as a confirmation upon receipt. Spamhaus has offered to review all dot-mail applicants to ensure that they are legitimate, but would charge a hefty fee of $2,000 to do so. One big uncertainty is whether ICANN will approve the new domain, which is under consideration along with dot-tel, dot-travel and dot-xxx, among others. E-mail marketers have expressed interest in the idea, although there's concern over how it would be managed. "There doesn't seem to be any process built in for how to get yourself one of these dot-mail names if they don't choose to give it to you," says a Direct Marketing Association spokesman. The biggest hurdle, however, will be convincing the major ISPs to go along, says Al DiGuido, CEO of bulk e-mailer Bigfoot Interactive. "This idea is stillborn until that happens. Unless Yahoo, MSN or AOL gets behind them, it's going to be a real uphill battle." (Washington Post 8 Apr 2004)

Category 33.2 *Spam, spim, spit & splogs*

2004-04-14 **spam junk e-mail explicit labeling Federal Trade Commission FTC**

NewsScan

FTC DEMANDS EXPLICIT LABELING OF EXPLICIT SPAM

If you can't stop them, label them. The Federal Trade Commission is requiring pornspam e-mail messages to have an explicit warning on the subject line so that Internet users can easily filter them out. Beginning the 19th of next month, such messages will have to bear a label reading "SEXUALLY-EXPLICIT:" and the messages themselves will be prohibited from containing graphic material. This new federal standard will supersede state laws requiring such labels as "ADV:ADULT" for pornspam. (Reuters/USA Today 14 Apr 2004)

Category 33.2 *Spam, spim, spit & splogs*

2004-04-28 **anti spam ISPs tackle Yahoo Microsoft AOL**

NewsScan

ISP HEAVYWEIGHTS TACKLE SPAM

America Online, Microsoft and Yahoo are joining together in an effort to vanquish spam, and are calling for technical changes in the way that e-mail is routed through cyberspace to make it easier to identify the true sender and content of messages. "We are talking about working on ways to change the dynamics of the e-mail system to make it easier to determine what is fraudulent," says MSN VP Brian Arbogast. The companies say they haven't yet discussed exactly what the standards should be, but have agreed they want to include other competitors in their discussions. "Working together, we will have better information about who are the kingpins that are sending the largest volume of spam to our users," says an AOL spokesman. (New York Times 28 Apr 2003)

Category 33.2 *Spam, spim, spit & splogs*

2004-04-29 **spam spammers criminal charges California junk e-mail illegal CAN-SPAM Act**

NewsScan

FOUR SPAMMERS FACE CRIMINAL CHARGES

Four California men face criminal charges for sending millions of junk e-mail messages, becoming the first spammers to be charged under the recently enacted federal CAN-SPAM Act. Christopher Chung, Mark Sadek and Daniel and James Lin are accused of secretly hijacking proxy servers -- systems that relay e-mail from any point on the Internet -- owned by unsuspecting businesses such as Ford Motor Co., Unisys and Amoco, and government agencies, including the Administrative Office of the U.S. Courts and the U.S. Army Information Center. The use of proxy servers is a favorite trick among spammers to disguise their identity. "This has been a problem that's plagued the Net for years, and the fact that corporations and government agencies still have open mail servers is scandalous," says one security consultant. "Somebody dropped the ball." If convicted, the men face up to five years in prison for violating the anti-spam law, as well as up to 20 years for mail fraud for distributing an allegedly fraudulent weight loss skin patch. The group also sent spam mail hawking male organ enlargement pills and Viagra. Terence Berg, the assistant U.S. attorney handling the case, warns that this lawsuit is a harbinger of more to come: "This is just a start. There will be many more prosecutions like this. The government is determined to do something about the flood of spam that is polluting the Internet." (Detroit Free Press/SiliconValley.com 29 Apr 2004)

Category 33.2 *Spam, spim, spit & splogs*

2004-04-30 **US new anti-spam law CAN-SPAM act charge**

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1578981,00.asp

April 30, Associated Press — U.S. Charges four under new anti-spam law.

Federal authorities say they managed to pierce the murky underworld of Internet spam e-mails, filing the first criminal charges under the government's new "can spam" legislation. Court documents in the landmark case in Detroit, MI, describe a nearly inscrutable puzzle of corporate identities, bank accounts and electronic storefronts in one alleged spam operation. At one point, investigators said, packages were sometimes delivered to a restaurant, where a greeter accepted them and passed them along to one defendant. Officials at the Federal Trade Commission told U.S. postal investigators they had received more than 10,000 complaints about unwanted e-mails sent by the defendants. Court records identified the defendants as Daniel J. Lin, James J. Lin, Mark M. Sadek and Christopher Chung of West Bloomfield, MI. They were accused of disguising their identities in hundreds of thousands of sales pitches for fraudulent weight-loss products and delivering e-mails by bouncing messages through unprotected relay computers on the Internet. The "can spam" legislation, which went into effect January 1, requires unsolicited e-mails to include a mechanism so recipients can indicate they do not want future mass mailings.

Category 33.2 *Spam, spim, spit & splogs*

2004-05-14 **spam club fighting forum gatecrash Spamhaus techniques IRC DDoS**

DHS IAIP Daily; http://www.theregister.co.uk/2004/05/14/spam_club/

May 14, The Register — Spam fighters infiltrate spam clubs.

Spam fighters are gaining vital clues in the battle to keep in-boxes clean of junk mail by infiltrating spammer clubs. Online spammer forums like the Pro Bulk Club the Bulk Club and bulkmails.org have been gatecrashed by activists from organizations like Spamhaus. Steve Linford of Spamhaus said spammers know this already but they don't know who amongst their number is working for the other side. In theory invitation to the members-only forums of these sites is only by invitation and only to individuals who have a proven track record in spamming. Apart from playing with the paranoia of spammers, the undercover investigation cast light on the latest spammer techniques. Instead of using open mail relays or unscrupulous hosts, spammers are using compromised machines to get their junk mail out. Viruses such as My-Doom and Bagle surrender the control of infected machines to hackers. This expanding network of infected, zombie machines can be used either for spam distribution or as platforms for DDoS attacks, such as those that many online bookies have suffered in recent months. Trade in machines for DDoS attacks normally happens in more in more anonymous IRC channels but spammers are tapping into the same resource.

Category 33.2 *Spam, spim, spit & splogs*

2004-05-20 **businesses acquisitions spam anti-spam**

DHS IAIP Daily; http://www.technewsworld.com/story/technology/33910.html

May 20, TechNewsWorld — Symantec acquires Brightmail.

Symantec has signed an agreement to acquire Brightmail, a maker of anti-spam technology, in a cash transaction valued at approximately $370 million. The acquisition, conditional upon customary regulatory approval, is expected to close by early July. It is too early to estimate the impact of intangibles on GAAP results from this transaction. As such, Symantec intends to discuss the impact, if any, on GAAP and non-GAAP results at some point in the future.

Category 33.2 *Spam, spim, spit & splogs*

2004-05-31 **crime fighting detective spam anti-spam money trail legislation Slam-Spam**

NewsScan

DETECTIVES FOLLOW THE MONEY TRAIL TO TACKLE SPAM

It seems like spammers have been working overtime since the federal antispam legislation took effect Jan.1, and the government is now turning away from technical fixes offered by software engineers in favor of private investigators' expertise to boost their efforts to stem the deluge of unsolicited e-mail. In an unusual arrangement, the Direct Marketing Association has paid $500,000 to hire 15 investigators to work alongside the FBI agents and other government officials in a program known as Project Slam-Spam. The project has built a case against 50 spammers, mostly by
following the money trail and relying on informants. "Spammers are more than willing to rat each other out," says Microsoft investigator Sterling McBride. "The most useful information is who pays for various aspects of the spam operation," says attorney David Bateman, who represents Microsoft
in spam cases. "To spam, you need four or five things -- a hosting service, a domain name, mailing software, mailing lists and so on. Each one you have to purchase from someone." Microsoft has filed 53 civil cases against spammers in the last 15 months, based on the work of its investigation
team. "The real key is trying to figure out how to connect the virtual world" with "someone you can hold responsible for this," says McBride. Once you've nailed that down, "you can use all the tools of a normal investigation." (New York Times 31 May 2004)

Category 33.2 *Spam, spim, spit & splogs*

2004-06-16 **spammer anti-spam conversion crusader Internet law obedience**

NewsScan

FROM SPAMMER ANTI-SPAM CRUSADER

Sued in March by Yahoo for sending millions of unsolicited commercial messages using Yahoo servers, Canadian spam king Eric Head now says he's renounced spamming and will spend his time drumming in a rock band -- and warning children of the evil possibilities of the Internet: "I urge everyone who is involved in the commercial bulk e-mail business to cease all operations unless and until they are completely compliant with the requirements of the new United States anti-spam laws." (AP/USA Today 16 Jun 2004)

Category 33.2 *Spam, spim, spit & splogs*

2004-06-16 **bulk junk fax rules rescind Federal Trade Commission business productivity time**

NewsScan

MOVE TO RESCIND BURDENSOME JUNK FAX RULES

The chairman of a House subcommittee on telecommunications is introducing a bill to rescind FCC regulations requiring senders of commercial faxes to get prior written approval from recipients. Rep. Fred Upton (R, MI) says his proposed bill is "common-sense regulatory relief" for businesses and associations that have been overburdened with paperwork since the regulations took effect. The bill has been endorsed by the full committee's senior Democrat, John Dingell of Michigan. Newspaper publisher Cheryl Kaechele, testifying on behalf of the National Newspaper Association, told the subcommittee: "Our typical customers are small businesses. They would far prefer to have us send them information by fax than to spend their precious minutes on the telephone or in personal sales calls." And Walt McDonald of the National Association of Realtors testified that the inconvenience of requiring written permission from potential clients before sending a fax "would be a giant step backwards in a business where good customer service depends on quick turnaround."

Category 33.2 *Spam, spim, spit & splogs*

2004-06-17 **Federal Trade Commission FTC do-not-e-mail list fail**

NewsScan

FTC SAYS NO TO DO-NOT-E-MAIL LIST

The Federal Trade Commission has decided that a "do not e-mail list" modeled after the popular "do not call list" would be completely ineffective -- and might actually have an effect just the opposite of the one intended (since it could be used by spammers to find legitimate e-mail addresses and send more spam). Senator Charles E. Schumer (D., NY) is critical of the FTC's decision and insists that a do-not-e-mail list "is the best thing we have and they ought to try it." But the FTC points out that Britain's ban of unsolicited e-mail resulted in an increase, rather than a decrease, in the amount of spam sent, and John R. Levine, the chairman of an organization called the Anti-Spam Research Group, says adamantly: "A do-not-spam list of individual addresses is unworkable."(New York Times 16 Jun 2004)

Category 33.2 *Spam, spim, spit & splogs*

2004-06-22 **e-mail service providers unite Internet zombie spam computers**

NewsScan

AOL, YAHOO, MSN AND EARTHLINK JOIN TO FIGHT THE ZOMBIES

The country's four largest providers of e-mail service have united in a war to defeat the "zombies" -- personal computers that have been surreptitiously invaded by spammers, who then use them to send spam and other messages without the knowledge of the PC owners. The Anti-Spam Technical Alliance, which includes AOL, Yahoo, MSN and Earthlink, is urging all Internet providers to police their networks more aggressively and to cut service away from zombie machines. There may be hundreds of thousands of zombie PCs around the world, accounting for as much as 40% of all spam that is generated. (Washington Post 22 Jun 2004)

Category 33.2 *Spam, spim, spit & splogs*

2004-06-24 **AOL employee lawsuit spam e-mail address theft**

NewsScan

AOL EMPLOYEE BUSTED FOR STEALING E-MAIL ADDRESSES

Jason Smathers, a 24-year-old employee of America Online, has been charged with stealing the e-mail addresses of 92 million AOL customers and selling them to spammers. Under a new federal anti-spam law, he faces the prospect of as many as five years in prison plus a fine of $250,000. The stolen information includes not only e-mail addresses but also telephone numbers, ZIP codes and the type of credit card the customers use (though not the actual credit card numbers, which are kept by AOL in a separate database). The company says: "We deeply regret what has taken place and are thoroughly reviewing and strengthening our internal procedures as a result of this investigation and arrest."(New York Times 24 Jun 2004)

Category 33.2 *Spam, spim, spit & splogs*

2004-07-07 **United Nations UN spam junk unsolicited e-mail legislation**

NewsScan

UN SEEKS SPAM MANDATE

The United Nations aims to bring the international junk email "epidemic" under control within two years by standardizing anti-spam legislation around the world. Representatives from 60 countries are in Australia attending a meeting hosted by the International Telecommunications
Union (ITU). The goal is to develop examples of anti-spam legislation that governments can adopt to make cross-border cooperation easier. (The Australian 7 Jul 2004) Recd from John Lamp

---

Category 33.2 *Spam, spim, spit & splogs*

2004-07-20 **spam anti-spam lawsuit New York settlement spammer**

NewsScan

NEW YORK ACCEPTS $40K TO SETTLE SPAM CASE

New York has accepted $40,000 (plus $10,000 in fees) to settle a lawsuit against a marketer charged with sending unsolicited and deceptive bulk e-mail. New York Attorney General Eliot Spitzer said the marketer, Scott Richter, and his company, OptInRealBig.com, have been held "to a new standard of accountability in their delivery of e-mails. If he does not fulfill these standards, he will find himself back in court, facing greater penalties." Scott Richter's father (who is also his lawyer) says the settlement basically involved a "no harm, no foul" situation from Richter's standpoint, and that the NY attorney general's acceptance of $50,000 -- after initially talking about $20 million in damages -- "speaks for itself." Neither Scott Richter nor his company admitted any wrongdoing in the settlement. (AP/San Jose Mercury News 20 Jul 2004)

Category 33.2 *Spam, spim, spit & splogs*

2004-07-27 **spam survey consumer view purchase bargain**

NewsScan

WHO WOULD HAVE GUESSED IT: SOME PEOPLE LIKE SPAM!

A Yahoo survey of Internet users found that one out of five U.S. residents admit to buying products from spammers, and one out of three make some kind of response to spam (such as by asking to removed from the list, by insulting the spammer, etc.). In defense of spam, a 30-year-old
computer-book author in Los Angeles says, "Spam can be useful. One person's spam is another person's bargain." Others seize on occasional deals they find -- a practice strongly discouraged by Laura Atkins, president of the anti-spam organization called SpamCon Foundation, who points out: "These spam-reading consumers are perpetuating the problem." (USA Today 27 Jul 2004)

Category 33.2 *Spam, spim, spit & splogs*

2004-08-04 **wireless device spam anti-spam Federal Trade Commission rules**

NewsScan

FCC MOVES TO PROTECT WIRELESS DEVICES FROM SPAM

The Federal Communications Commission (FCC) is issuing new rules prohibiting marketers from sending commercial electronic messages to wireless technology users who haven't given them explicit permission to do so. The agency is also urging the industry to develop technologies to prevent spam from overwhelming wireless devices the way it now bedevils the Internet. FCC chairman Michael K. Powell says, "By prohibiting all commercial messages to wireless phones and PDAs absent affirmative consent from the consumer, Americans can now use their wireless devices freely, without being bothered by unwanted and annoying messages." (Washington Post 4 Aug 2004)

Category 33.2 *Spam, spim, spit & splogs*

2004-08-04 **wireless mobile device cell phone spam regulator wrath Federal Communications Commission FCC**

DHS IAIP Daily;
http://news.com.com/Wireless+spam+draws+regulators%27+wrath/ 2100−1028_3−5296649.html?tag=nefd.top

August 04, CNET News.com — Wireless spam draws regulators' wrath.

The Federal Communications Commission (FCC) on Wednesday, August 4, said that commercial e-mail messages to cell phones or handheld computers would not be permitted unless the recipient had asked to receive the correspondence in advance. But the FCC's decision not to restrict unsolicited text messages sent through mechanisms like SMS, which stands for short message service, creates a potentially huge regulatory loophole affecting tens of millions of Americans. Wireless providers often charge a few pennies per text message received. Verizon Wireless subscribers exchanged 2.3 billion text messages last quarter, up from 2.1 billion during the previous quarter. Cingular Wireless reported 1.4 billion text messages were sent during its last quarter. The FCC's rules permit mobile providers to register their Internet domain names in a master database that spammers are supposed to honor. That database will include only domain names like attwireless.com and t-mobileusa.com, and not individual e-mail addresses of subscribers.

Category 33.2 *Spam, spim, spit & splogs*

2004-08-13 **Federal Trade Commission FTC CAN-SPAM spam definition junk unsolicited commercial e-mail**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/26907−1.html

August 13, Government Computer News — FTC proposes definitions for spam.

The Federal Trade Commission (FTC), as the primary enforcer of the CAN-SPAM Act, was required by Congress to define the criteria for determining the primary purpose of an e-mail. If the primary purpose is commercial, the e-mail is subject to the act. CAN-SPAM, which went into effect January 1, prohibits unsolicited commercial e-mail from using misleading subject lines or phony "from" addresses, and requires them to include a valid postal address and a working e-mail address for opting out of future messages. In a notice of proposed rulemaking published Friday, August 13, in the Federal Register, FTC proposed three criteria for different types of messages. The three proposed criteria are based on a single principle: "Determining the primary purpose of an e-mail message must focus on what the message's recipient would reasonably interpret the primary purpose to be. " FTC is accepting public comment on the proposal through September 13. Electronic comments should be submitted through the online form available at https://secure.commentwork.

Category 33.2 *Spam, spim, spit & splogs*

2004-08-13 **spam anti-spam unsolicited junk unwanted e-mail government OECD Organization Economic Cooperation Development**

NewsScan

OECD SETS TWO-YEAR DEADLINE TO CUT SPAM

The OECD said last week it has set up a task force to coordinate the fight by government, business and the public against unsolicited email messages, or spam. It has given the new group two years to study spam and develop a counter strategy. The Organization for Economic Cooperation and Development said in a statement the task force would improve the way work on key aspects of the problem was focused and would improve coordination between various bodies looking at the issue. Key objectives included coordinating international policy, encouraging best practice in industry and business, promoting new technical defenses, informing consumers, and facilitating cross-border law enforcement. (The Age, 13 Aug 2004) rec'd from John Lamp, Deakin U.

Category 33.2 *Spam, spim, spit & splogs*

2004-08-19 **DNA Chung-Kwei Teiresias algorithm spam identification application 96.56% success Thomas J. Watson Center New York**

DHS IAIP Daily; http://www.newscientist.com/news/news.jsp?id=ns99996292

August 19, New Scientist — DNA technique protects against 'evil' e-mails.

A technique originally designed to analyze DNA sequences is the latest weapon in the war against spam. The algorithm, named Chung-Kwei, is based on the Teiresias algorithm, developed by the bioinformatics research group at the Thomas J. Watson Research Center in New York. Instead of chains of characters representing DNA sequences, the research group fed the algorithm 65,000 examples of known spam. Teiresias identified six million recurring patterns in this collection. Each pattern represented a common sequence of letters and numbers that had appeared in more than one unsolicited message. The researchers then ran a collection of known non-spam through the same process, and removed the patterns that occurred in both groups. Incoming e-mail was given a score based on how many spam patterns it had. The Chung-Kwei correctly identified 64,665 of 66,697 test messages as being spam or 96.56 percent. Its rate of misidentifying genuine email as spam was just one in 6000 messages.

Category 33.2 *Spam, spim, spit & splogs*

2004-08-25 **spammers cyber criminals arrest John Ashcroft Attorney General noisy trial**

NewsScan

SOME VICTORIES AGAINST SPAMMERS AND OTHER ONLINE CRIMINALS

Attorney General John Ashcroft will announce today that federal and state law enforcement agencies have arrested or charged dozens of people for crimes related to spam, identity theft, online credit card fraud, and other criminal uses of computers and networks. Much of the funding for the
operation came from the Direct Marketing Association, whose former president says: "We felt that the key to the new law was enforcement. We want spammers to realize that spam is not a free game for them and that they face real penalties if they continue." Steve Linford, director of the U.K.-based
anti-spam organization called Spamhaus Project, is cautiously optimistic: "Spammers believe that they will never be caught. If they [law enforcement officials] get 10, 20, 30 well-known spammers, the rest of the spam community will start to notice. Any spammers who can be made to give up because they think the F.B.I. is getting too close is very good for us." On the other hand, Linford fears that a victory in one place just sets up a new challenge somewhere else: "Next year and the year after we are going to see Russia as the main spam problem." (New York Times 25 Aug 2004)

Category 33.2 *Spam, spim, spit & splogs*

2004-08-25 **spam arrests charges law enforcement trials junk e-mail identity theft scams**

NYT http://www.nytimes.com/2004/08/25/technology/25spam.html?th

In late August 2004, dozens of people in the US were arrested and charged with crimes for sending junk e-mail, identity theft and other computer-mediated crimes. Federal and state law enforcement agencies and prosecutors cooperated in a nation-wide sweep. Operation Slam Spam involved support from industry groups such as the Direct Marketing Association and was coordinated by the non-profit National Cyber-Forensics and Training Alliance in Pittsburgh. Analysts commented that if spammers were shut down in the USA, overseas spammers, especially in Russia, would fill in the gap and continue increasing the volume of junk e-mail.

Category 33.2 *Spam, spim, spit & splogs*

2004-08-25 **spam export US CAN-SPAM Act statistics study survey**

NewsScan

U.S. LARGEST EXPORTER OF SPAM

The United States is the largest global source of spam, producing more than two of every five messages, a report by security firm Sophos shows. Sophos found about 43% of all spam originated in the United States. The next largest source was South Korea, with 15%, and China and Hong Kong,
accounting for a combined 12% per cent. The report suggests that a U.S. law known as CAN-SPAM that took effect in January has done little to curb the flood on unwanted messages that some see as a threat to the Internet. Chris Kraft, senior security analyst at Sophos, says the results indicate little
overall change from a similar survey in February for the United States. (The Australian 25 Aug 2004) rec'd from John Lamp, Deakin U.

Category 33.2 *Spam, spim, spit & splogs*

2004-09-08 **anti-spam technology subverted SPF Sender Policy Framework authentication MX Logic**

NewsScan

SPAMMERS TAKE ADVANTAGE OF SENDER VERIFICATION PROTOCOL

A new study by MX Logic indicates that about 16% of spam mail senders are using a protocol known as Sender Policy Framework (SPF), which has been touted as a spam-blocking tool, thanks to its sender authentication capabilities. "Authentication (with SPF) by itself is not a spam cure-all.
SPF -- as it relates to having an impact on spam -- will hurt only those who spoof domains. You are still going to need content filtering to see if the message was unsolicited," says MX CTO Scott Chasin. Chasin maintains that SPF is only part of the answer to the spam problem: "SPF is great at
combating fraud such as phishing. Phishing attacks are all about spoofing someone's domain name." Chasin says rather than relying on SPF to cut spam, ISPs should be looking into services that could provide subscribers with some kind of measure of the e-mail sender's reputation by certifying some servers as belonging to "good" e-mail senders. "The e-mail filters could then let through legitimate e-mail. It would be 'guilty until proven innocent,'" says Chasin. (CNet News.com 8 Sep 2004)

Category 33.2 *Spam, spim, spit & splogs*

2004-09-17 **e-mail junk unsolicited spammer arrest hunt search bounty Federal Trade Commission FTC America Online AOL objections**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/articles/A27220−2004Sep 16.html

September 17, Washington Post — Cash bounties for spammers win limited FTC backing.

The Federal Trade Commission (FTC), on Thursday, September 16, gave limited endorsement to offering cash rewards to people who help track down e-mail spammers, suggesting that such bounties might work but in fewer circumstances than had been pushed by some anti-spam activists. Congress asked the FTC to study two possible techniques as part of the first federal anti-spam law passed late last year. In June, the FTC recommended against the first technique, a do-not-spam registry, saying it would not work and might lead to more spam. The notion of bounties drew particular credence when it was pushed by Lawrence Lessig, a Stanford University law professor and one of the country's foremost thinkers on cyberspace law and policy. But the major Internet providers, who have their own spam-fighting operations, counseled the FTC against the idea. An America Online Inc. spokesperson, Nicholas J. Graham, said the use of bounty hunters can create its own set of legal problems that could complicate prosecutions. The commission estimates that rewards would need to be in the range of $100,000 to $250,000, which Congress would need to fund because those amounts are unlikely to be covered by damages won in court.

Category 33.2 *Spam, spim, spit & splogs*

2004-11-02 **politics e-mail spam election campaign Democrats Republicans candidates**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A18746-2004Nov2.html

POLITICAL E-MAIL SMACKS OF SPAM

An online survey of 1,000 U.S. Internet users indicates that unsolicited e-mail supporting both the Bush and Kerry presidential campaigns were common in the past few weeks, and about 20% of recipients said the messages may have affected their votes. "The cat's out of the bag," says Anne Bonaparte, president of MailFrontier, which commissioned the study. "E-mail is a powerful communications tool and it has vulnerabilities that are being exploited by people who have a point to make." Engaging in political spam does entail the risk of backlash, however, says Jonah Seiger, cofounder of Connections Media. "Spam is a tactic of snake oil salesmen. I don't see an advantage for a group or a candidate associating themselves with this technique." Meanwhile, Larry Purpuro, president of Republican online consulting group RightClick Strategies disagrees: "In the 2004 election, political e-mail is a tactical nuclear weapon. It is to a large extent under the radar screen, but its ability to target and to penetrate the attention of individuals makes it an extremely effective communications tool." Spam advocating a political position is free speech, protected by the First Amendment, and is not considered illegal under the law. (Washington Post 2 Nov 2004)

Category 33.2 Spam, spim, spit & splogs

2004-11-04 **antispam first spam felony conviction junk unsolicited e-mail America Online AOL**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/articles/A24546−2004Nov 4.html?nav=headlines

November 04, Associated Press — Two guilty in first felony spam conviction.

A brother and sister who sent junk e-mail to millions of America Online (AOL) customers were convicted Wednesday, November 3, in the nation's first felony prosecution of Internet spam distributors. Jurors recommended that Jeremy Jaynes, 30, be sentenced to nine years in prison and fined Jessica DeGroot, 28, $7,500 after convicting them of three counts each of sending e-mails with fraudulent and untraceable routing information. Prosecutor Russell McGuire said Jaynes amassed a net wealth of $24 million peddling worthless products like a "FedEx refund processor," a "penny stock picker" and an Internet history eraser. Virginia, where AOL is based, prosecuted the case under a law that took effect last year which bars people from sending bulk e-mail that is unsolicited and masks its origin. "Spam is a nuisance to millions of Americans, but it is also a major problem for businesses large and small because the thousands of unwanted e-mails create havoc as they attempt to conduct business," Attorney General Jerry W. Kilgore said.

Category 33.2 Spam, spim, spit & splogs

2004-11-05 **spam law regulation advertisign CAN-SPAM**

Washington Post; MSNBC http://www.msnbc.msn.com/id/6411616/

Microsoft's Steve Ballmer ignited a fuse when he sent out a long letter to millions of recipients advertising his company's products and criticizing Linux.

Anti-spam activists accused the company of using e-mail addresses without permission -- in other words, of spamming. Some lawyers specializing in details of antispam laws in the USA criticized the e-mail for failing to include clear and conspicuous instructions on how to be dropped from the mailing list.

Category 33.2 Spam, spim, spit & splogs

2004-11-09 **SPIT VoIP voice over IP spam Osterman**

NewsScan; http://www.usatoday.com/tech/news/2004-11-09-spit_x.htm

SPITTING MAD AT SPAM

Spam over Internet telephony, known as SPIT, will become commonplace as more people make phone calls over the Internet. Internet researcher Michael Osterman warns that Web-based phone systems attacked by spam will "trash voice-mail systems," and explains: "You can easily delete 100 spam text messages. But try to weed through a voice-mail system filled with 100 unsolicited pitches. That's a pain." Spam is already appearing frequently on instant messages, cell phones, and blogs, and one executive of an Internet service provider admits: "As everything gets connected, there are more ways to spam consumers. Spam is everywhere." (USA Today 9 Nov 2004)

Category 33.2 Spam, spim, spit & splogs

2004-11-18 **e-mail spam Bill Gates Microsoft volume filtering**

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/10213910.htm

BILL GATES GETS MILLION OF E-MAILS A DAY

Think you've got spam? Microsoft chairman Bill Gates "literally receives 4 million pieces of e-mail per day, most of it spam," says CEO Steve Ballmer, who notes that the company uses special technology to filter spam intended for Gates. In addition, there are several Microsoft employees who provide human screening. "Literally, there's a whole department almost that takes care of it." (AP/SiliconValley.com 18 Nov 2004)

Category 33.2 *Spam, spim, spit & splogs*

2004-11-30 **spam Lycos response flooding bandwidth saturation counterattack information warfare Denning lawsuit screensaver**

NewsScan; http://www.usatoday.com/tech/products/2004-11-30-lycos-attack-spam_x.htm?csp=34

CYBERSPACE ACTIVISM

The German-based Web portal Lycos Europe is offering a screensaver program that chokes spam servers by flooding them with junk traffic. The company argues that what it's doing is perfectly legal, but former FCC chief technologist David Farber comments: "You don't stop a bad thing by being bad yourself. The idea of somebody coming and hitting you and you hitting back, you both end up very hurt. It just aggravates an already serious problem." And noted computer security expert Dorothy Denning, a professor of defense analysis at the Navy Postgraduate School, points out that cyberspace activism of the kind offered by Lycos Europe is likely to have only minimal impact on spam because "the cost of adding extra bandwidth may be worth the reward" that spammers get from their activities. She adds: "The interesting question is whether or not that company [an anti-spam activist company] might be liable under some law, and would probably be liable, certainly, at least under a lawsuit by the spammers." (AP 30 Nov 2004)

Category 33.2 *Spam, spim, spit & splogs*

2004-12-20 **spam judgement federal judge RICO Iowa racketeering damages**

NewsScan; http://online.wsj.com/article/0

JUDGE SLAMS SPAMMERS WITH $1-BILLION JUDGMENT

A federal judge in Iowa has awarded a small ISP more than $1 billion in damages in what's believed to be the largest judgment ever against spammers. The case was brought by Robert Kramer, whose company provides e-mail service to about 5,000 customers, and who filed suit after his inbound mail servers were jammed with as many as 10 million spam-mails a day in 2000. Citing federal racketeering laws (RICO) and the Iowa Ongoing Criminal Conduct Act, U.S. District Judge Charles R. Wolle ordered AMP Dollar Savings of Mesa, Ariz., to pay $720 million; Cash Link Systems of Miami, Fla., $360 million; and TEI Marketing Group, also of Florida, $140,000. "It's definitely a victory for all of us that open up our e-mail and find lewd and malicious and fraudulent e-mail in our boxes every day," said Kramer, who is unlikely to ever collect on the judgments. (AP/Wall Street Journal 20 Dec 2004)

Category 33.2 *Spam, spim, spit & splogs*

2004-12-28 **America Online AOL report spam decline 2004 legislation CAN SPAM act**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/articles/A30433−2004Dec 27.html

December 28, Washington Post — America Online reports decline in spam in the past year.

America Online (AOL) said Monday, December 27, that it has seen a substantial decline in unsolicited e-mails this year, though some anti-spam experts said the company may be the only Internet provider experiencing such a drop-off. The average number of so-called spam e-mails that AOL blocked daily dropped from a peak of 2.4 billion in 2003 to 1.2 billion late this year. AOL credited anti-spam legislation, such as the federal Can-Spam law, as well as its own spam-filtering software tools, for the decline. AOL remains the largest Internet service provider, with 29 million subscribers worldwide. But an anti-spam expert said AOL's apparent success may not mean that the rest of the Internet is seeing fewer bulk e-mail spam. John Levine, chairman of the Anti-Spam Research Group said, "There are a lot of spammers who specialize in AOL" because the company has such a large subscriber base. Levine said some bulk e-mailers may have backed down from assailing AOL subscribers as a result of the company's aggressive legal actions against spammers. Other Internet providers reported that they have not seen much change in the volume of spam traffic on their networks.

Category 33.2 *Spam, spim, spit & splogs*

2005-01-11 **adult e-mails CAN-SPAM ACT FTC memberships**

EDUPAGE; http://www.wired.com/news/politics/0,1283,66240,00.html

ADULT E-MAILS SHUT DOWN BY CAN-SPAM ACT

The Federal Trade Commission (FTC) has won an injunction against six companies accused of sending thousands of spam messages that failed to meet the requirements of the CAN-SPAM Act. According to the FTC's complaint, the companies sent e-mail that directs recipients to adult Web sites but did not include the phrase "sexually explicit" in the subject line, as required by the antispam law. The e-mails also did not provide opt-out functions to recipients and falsely promised free memberships with the Web sites involved. The temporary injunction issued by a court in Las Vegas marks the first time the requirements of the CAN-SPAM Act regarding adult content have been used. The FTC will ask the court to make the injunction permanent. In addition, those who operate the Web sites that benefit from unlawful spam can be held accountable under the CAN-SPAM law.

Category 33.2 *Spam, spim, spit & splogs*

2005-01-12 **CAN-SPAM spam porn FTC injunction Federal Trade Commission junk e-mail liability prosecution injunction**

NewsScan; http://apnews.excite.com/article/20050112/D87II6A80.html

FTC SHUTS DOWN X-RATED SPAMMERS

The Federal Trade Commission has won a preliminary injunction against six companies accused of profiting from sexually explicit junk e-mail. The injunction, granted by U.S. District Court Judge Philip M. Pro, will last the duration of the FTC's civil suit against the companies. The case marks the first time the FTC has taken action under a rule included in the last years "Can Spam" Act that requires a label identifying sexually explicit e-mail in the subject line. The law also holds liable Web site operators who benefit from fraudulent pornographic spam. "It's not just the people who push the buttons to send spam" who are liable," notes FTC marketing practices division director Eileen Harrington. Named in the FTC complaint are Global Net Solutions, Open Space Enterprises, Southlake Group and WTFRC Inc., all of Nevada; Global Net Ventures of London; and Wedlake Ltd., which is based in Riga, Latvia. (AP 12 Jan 2005)

Category 33.2 *Spam, spim, spit & splogs*

2005-01-14 **Texas notorious spammers lawsuit PayPerAction Leadplex state federal**

EDUPAGE; http://news.com.com/2100-1030_3-5536356.html

TEXAS TARGETS NOTORIOUS SPAMMERS

The attorney general of Texas has filed a civil lawsuit against two individuals believed to be responsible for millions of illegal e-mail solicitations. Ryan Samuel Pitylak, a student at the University of Texas, and Mark Stephen Trotter of California operate two companies, PayPerAction and Leadplex. Spamhaus.org, a watchdog group that monitors spam, has identified the two companies as being among the top five spam operations worldwide. Prosecutors allege that the e-mails sent by the two companies violate state and federal laws, including the CAN-SPAM Act, by including misleading subject lines and fraudulent information in the body of the messages. The defendants, who are also accused of violating Texas trade practices, face millions of dollars in fines, though no criminal charges were filed against them. An attorney for the defendants said his clients' businesses are in full compliance with all applicable laws, including the CAN-SPAM Act. CNET, 14 January 2005

Category 33.2 *Spam, spim, spit & splogs*

2005-02-04 **new spamming technique Internet service provide ISP computer exploitation spammer technique sophistication**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/articles/A61901−2005Feb 3.html

NEW SPAMMING TECHNIQUE USES ISP COMPUTERS.

An advanced spamming technique could push the volume of unwanted e-mail to new heights in coming months, straining the integrity of the online communication system, according to several top experts who monitor the activity of spam gangs around the world. Illegal bulk-mailers have been able to deploy massive blasts of spam by routing it through the computers of their Internet service providers (ISPs), rather than sending it directly from individual machines, the experts said. The result is that "blacklists" of known spamming computers -- which other network operators rely upon to block mail from those machines -- are no longer effective. To block spam coming directly from an ISP's computers, all mail from that ISP would be have to be blocked, which would cripple electronic communication. The new method of attack reflects the evolving sophistication and efficiency of top spamming groups, a community of people who support each other by trading intelligence, products and services. Some ISPs have been able to make dents in the amount of spam reaching the inboxes of computer users, but spam traffic over the Internet continues to rise and to exact steep costs on network operators, businesses and consumers.

Category 33.2 *Spam, spim, spit & splogs*

2005-02-04 **blacklists ISP Internet service provider open spam relay e-mail technique cost estimates**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A61901-2005Feb3.html

SPAMMERS TRY A NEW TACK

Tired of being blocked by "blacklists," spammers are turning to a new technique -- routing it directly through the computers of their Internet service providers, rather than sending it from individual machines. The result poses a dilemma: to block spam coming directly from an ISP's servers would mean blocking all its mail, crippling the system. "From what we've seen, the volumes of this type of spam are going up dramatically," says Steve Linford, who heads up the Spamhaus Project. "We're really looking at a bleak thing" if ISPs don't quickly deploy countermeasures, he adds. Such measures could include more aggressive monitoring and limiting how much mail is being sent from individual machines on their networks. In addition, ISPs should beef up efforts to authenticate mail they pass on through their own computers, says Linford. A study released yesterday estimates that deleting spam costs nearly $22 billion per year in lost productivity, based on a survey of 1,000 adults who said they spend about three minutes per day trashing spam when they check their e-mail. (Washington Post 4 Feb 2005)

Category 33.2 *Spam, spim, spit & splogs*

2005-02-09 **wireless domain spam free Federal Communications Commission FCC regulations working list disclosure**

DHS IAIP Daily; http://www.pcworld.com/news/article/0,aid,119620,00.asp

LIST OF WIRELESS DOMAINS THAT CANNOT RECEIVE SPAM.

The U.S. Federal Communications Commission (FCC) took a major step this week toward fighting unwanted e-mail messages sent to wireless phones and pagers by publishing a list of wireless mail domain names. The FCC, which published the list late Monday, February 7, has ruled that starting in early March, it will be illegal to send most commercial messages to users of wireless phones with addresses that include any of the published domain names. Wireless spam, still limited in the U.S., has generated significant customer complaints in other countries including Japan and India. Senders who violate the FCC rules and send commercial e-mail to the wireless mail domains on the list face fines of up to $11,000 per violation. Scott Chasin, chief technology officer at MX Logic, an antispam software vendor said that the FCC list has one potential downside--it provides spammers with a working list of wireless mail domains. The list is available at: http://www.fcc.gov/cgb/policy/DomainNameDownload.html

---

Category 33.2 *Spam, spim, spit & splogs*

2005-02-09 **Microsoft Pfizer Viagra lawsuit suit spam e-mail scam**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A12618-2005Feb9.html

MICROSOFT AND PFIZER CAMPAIGN AGAINST SPAM

Microsoft and drug manufacturer Pfizer yesterday filed 17 lawsuits against various alleged spammers and Web-site operators that push fraudulent versions of drugs (especially Viagra). This is the first time an Internet service provider (Microsoft's MSN) has joined a major retailer to attack the entire supply chain of online scams. Pfizer attorney Marc Brotman says that one-fourth of all spam is related to pharmaceuticals, and that Pfizer suggested that it and Microsoft pool the two firms' investigative resources. (Washington Post 9 Feb 2005)

Category 33.2 *Spam, spim, spit & splogs*

2005-02-21 **instant messaging spim statistics**

NewsScan; http://www.pewinternet.org/PPF/p/1052/pipcomments.asp

BATTLING THE SPIM-MEISTERS

Almost one in three instant-messaging users in the U.S. have received some kind of "spim" (unsolicited commercial instant messages), according to a survey by the Pew Internet & American Life Project. Results indicate that users age 30 and younger are more likely to get spimmed, compared with the next older age cohort (31-49). Other than the age discrepancy, however, no other demographic trends were discernible, says Pew: "Instant message users in all income brackets and in all racial and ethnic groups are equally likely to receive spim. Somewhat surprisingly, broadband users at home are no more likely than dialup users to receive spim, even though, presumably, those with always-on broadband connections keep their instant message programs running for longer periods of time than dialup users." The survey found that 52 million Americans -- 42% of the online population -- use instant messaging, and among the 30- and-under age group, it's 66%. (Pew Internet & American Life Project 21 Feb 2005)

Category 33.2 *Spam, spim, spit & splogs*

2005-02-21 **spim arrest New York instant messaging MySpace.com extortion**

NewsScan; http://news.com.com/U.S.+makes+first+arrest+for+spim/2100-7355_3-5584574.html

FIRST SPIMMER ARREST

An 18-year-old New York teenager has become the first person to be arrested on suspicion of spimming. Anthony Greco allegedly sent 1.5 million messages hawking pornography and mortgages to users of MySpace.com's IM system, and was arrested in a sting operation in the Los Angeles Airport last Wednesday following an extortion attempt on his part. Greco believed he was flying to LA to seal a deal with the president of MySpace.com, whom Greco had threatened with publicizing his spim techniques if he were not granted an exclusive marketing arrangement that would have legitimized his spimming activities. Assistant U.S. Attorney Brian Hoffstadt says that while Greco's case marks the first criminal prosecution of instant message spamming, there may well be more to come: "We're just beginning to get the tip of the iceberg. This could be a new wave as online communities start up." (CNet News.com 21 Feb 2005)

Category 33.2 *Spam, spim, spit & splogs*

2005-02-23 **denial of service DoS spam blocker court appearance e-mail notice critical information reliability delivery**

RISKS; 23 75
http://news.lp.findlaw.com/andrews/pl/med/20050223/20050223barnes.html

SPAM-BLOCKER CAUSES MISSED COURT DATE

"A plaintiff's attorney in a wrongful-death lawsuit, who missed a court date because his firm's spam blocking software automatically sidetracked the court's e-mail notice, has narrowly escaped being sanctioned for failing to appear at the scheduled status conference…."

In a follow-up analysis, Joseph Brennan pointed out that such a sequence would require a number of errors. Either the lawfirm's spam software was set wrong and discarded blocked e-mail OR it diverted spam to a spam folder but the lawyer didn't look at the spam folder OR the spam-blocker bounced the "spam" but the court officers failed to note the bounce message and therefore did not follow up on the problem. In any case, Brennan was pretty sure there were human errors involved.

[MK adds: there is no specification for required delivery in any of the RFCs defining SMTP. No one should ever assume that e-mail has been delivered to its intended recipient without proof of such delievery.]

Category 33.2 *Spam, spim, spit & splogs*

2005-04-01 **spammer bankruptcy protection anti-spam law Microsoft lawsuit litigation**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4400335.stm

SPAMMER FILES FOR BANKRUPTCY PROTECTION

Scott Richter, proprietor of one of the world's best known spamming operations, said the company has been forced to file for bankruptcy protection. OptInRealBig.com has been the target of several lawsuits for violating antispam laws, including one lawsuit filed by Microsoft, which is seeking $46 million in damages. Spamhaus, an organization that monitors junk e-mail globally, ranks OptInRealBig.com third on its list of spam operations around the globe. The company is alleged to have sent billions of e-mail messages that appeared to come from hijacked return addresses, including those of the Kuwait Ministries of Communication and Finance, the Seoul Municipal Boramae Hospital, and the Virginia Community College System. In its announcement, OptInRealBig.com said that the ongoing lawsuits and possible damages have made it impossible for the company to "still run a viable business." An attorney for OptInRealBig.com said the company expects ultimately to prevail. BBC, 1 April 2005

Category 33.2 *Spam, spim, spit & splogs*

2005-05-09 **SPEWS spam prevention early warning system anti-spam Telewest customers e-mail address hijack zombies**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4528927.stm

ANTISPAM BLACKLIST TARGETS 900,000

Officials at the Spam Prevention Early Warning System (SPEWS) have placed e-mail addresses of 900,000 Telewest customers on its blacklist, saying that computers using those addresses may have been hijacked and used for sending spam. Many organizations use the SPEWS blacklists as e-mail filters--anything coming from an address on the list is blocked. Telewest acknowledged that some subscribers of its Blueyonder broadband service have had their computers compromised by computer viruses and turned into e-mail zombies. Company officials said they are working to contact those users with suspiciously high volumes of e-mail traffic to help them clean their machines. "As you can imagine," said a statement from the company, "[it] is a time-consuming task." Matt Peachey of antispam software firm Ironport said he doubts all of the blocked computers have in fact been turned into spam zombies by hackers. Peachey accused SPEWS of casting too wide a net in its blacklisting. BBC, 9 May 2005

Category 33.2 *Spam, spim, spit & splogs*

2005-05-09 **anti-spam Bayesian filters probabilitic methods countermeasures unsolicited commercial e-mail**

RISKS 23 88

SPAMMERS STRIVE FOR ORIGINALITY TO DECEIVE ANTI-SPAM FILTERS

Dan Wallach reported on his detailed analysis of how spammers are defeating sophisticated anti-spam filters: they are using attributes of normal mail and avoiding obvious characteristics of spam.

>Recently, I've gotten a number of spams that have perfect spelling and vanilla plain text (as opposed to the insane HTML ov3rki!! Variety). If you look at the mail headers, there's some evidence of zombie machines being used to transmit the spam (i.e., received lines not matching up to the From or Sender line) but otherwise the headers are quite clean. For the message in front of me right now, the user agent is even listed as Mozilla on Linux. DSPAM has a clever feature where it will tell you what factors in the message it used to make its decision. In this case, DSPAM latched onto the User-Agent string and other Mozilla-esque headers as having a very low probability of being spam. This outweighted a few strings that otherwise should have tipped it off (e.g., "credit history" or "secure, private").<

He concluded,

>In some sense, this is exactly what Paul Graham predicted would eventually happen in "A Plan For Spam". My hope is that I can eventually untrain DSPAM of its love for Mozilla headers; we'll see how well it does. My fear is that there will always be an avenue of attack for a "contrarian spammer" who engineers spam to be unlike all the other spams out there.<

Category 33.2 *Spam, spim, spit & splogs*

2005-05-12 **Boston spammer ring Internet Spam Gang Websites shut down court order civil suit**

DHS IAIP Daily;
http://www.boston.com/business/technology/articles/2005/05/12/judge_orders_spammers_websites_shut/

JUDGE ORDERS SPAMMERS' WEBSITES SHUT

A Massachusetts state Superior Court judge Wednesday, May 11, issued an emergency order to shut down dozens of Websites, as Massachusetts investigators working with Microsoft Corp. moved against what they described as a Boston-based ring of Internet spammers responsible for one of the world's most prolific spam operations. In a civil suit filed with the court Wednesday, state Attorney General Tom Reilly accused Leo Kuvayev and six other defendants with violating state and federal consumer protection laws by masterminding a global network of spammers who have sent hundreds of millions of e-mail messages directing recipients to Websites with names like oemcd.biz or genericpharmacies.biz. The messages, and the Websites, seek to lure consumers into buying low-interest mortgage loans, pirated software, knockoffs of designer watches, pornography, and counterfeit drugs of prescription brand names. Massachusetts and Microsoft officials said the spammers, whom they dubbed the "Internet Spam Gang," unleashed the largest volume of e-mail they've seen from one group. State officials have not brought criminal charges against the seven defendants.

Category 33.2 *Spam, spim, spit & splogs*

2005-07-07 **spammer Smith Rizler federal judge Burnsville Internet Xpress Pharmacy Direct drugs spam FBI court contempt jailed**

DHS IAIP Daily; http://www.vnunet.com/vnunet/news/2139427/spam−supremo−smith −sued

SUSPECTED SPAMMER SMITH SEIZED

Suspected spammer Christopher Smith, nicknamed the Rizler was arrested at a Minneapolis, MN airport shortly after stepping off a flight from the Dominican Republic, where he had been operating since a U.S. federal judge in May shut down his companies, Burnsville Internet and Xpress Pharmacy Direct, and ordered him to stop selling drugs online. Smith had since set up similar operations in the Dominican Republic, through which he is alleged to have sent more than a billion spam emails either to AOL email addresses or through AOL email accounts. The FBI claims that Smith has already made about $18 million this year. Federal authorities raided Xpress Pharmacy and Smith's home on 10 May, seizing his passport and $4.2m in assets, including a $1.1m house and luxury cars worth $1.8m. At the same time the FBI closed down his 85-employee company. Investigators concluded that Smith had been selling medicines to customers without proper prescriptions, and selling drugs without a licence. The U.S. Attorney's office claims that Smith had broken court orders and is recommending that he be held in criminal contempt and jailed for six months.

Category 33.2 *Spam, spim, spit & splogs*

2005-07-27 **anti-spam content filtering censorship political bias**

RISKS 23 95

ARE SOME ANTI-SPAM SERVICES CENSORING MAIL FOR POLITICAL REASONS?

Pete Klammer voiced concern over possible interference in the political process by corporations running anti-spam services.

>In the run-up to the 2004 election, I found activist messages about (against) Arnold Schwarzenegger were being screened by ACM's e-mail screening service controlled by Postini. I was only able to verify this, and retrieve my messages, because I had chosen the "quarantine" option, and checked the quarantine area soon enough, before the messages were permanently expunged.

Now we hear that messages regarding the Downing Street memos have been blocked from Comcast.net customers (one of the largest high-speed cable internet providers in the U.S.), based on content of the message -- a URL -- rather than subject line or sender address or domain.

The potential for (mis)information manipulation by large and powerful corporations is frightening, particularly as U.S. Law exempts them from "common carriage" legal requirements. We would never (I hope!) stand for our telephone company to redirect our flight-reservation phone call to a different airline "partner" company; why must we tolerate such distortion on the Internet?<

* * *

In a a follow-up response in RISKS 23.96, Craig A. Finseth expressed skepticism about Klammer's hypothesis: "Probably because you asked them to: Postini is an anti-spam service which provides mechanisms for you to control what is filtered (as well as a heck of a lot of stuff that they do for you). My ISP uses it and offers me full control over the amount of filtering done, including complete disabling."

Category 33.2 *Spam, spim, spit & splogs*

2005-08-04 **spam anti-spam efforts litigation ruling University of Texas White Buffalo Ventures student e-mail addresses CAN-SPAM Act**

EDUPAGE; http://insidehighered.com/news/2005/08/04/ut

COURT UPHOLDS UNIVERSITY BLOCK ON SPAMMER

A federal appeals court ruled in favor of the University of Texas (UT) in its dispute with White Buffalo Ventures over thousands of spam e-mails sent by the company to students of the institution. In 2003, White Buffalo, which operates an online dating service geared toward UT students, began sending thousands of messages to student e-mail addresses it had obtained through public records. After receiving many complaints from students, the university blocked White Buffalo's e-mails, a move the company said infringed on its First Amendment rights and its rights under the CAN-SPAM Act. A federal judge disagreed with White Buffalo, and the current ruling supports that decision. The three-judge panel of the appeals court found that the institution is within its rights to place restrictions on commercial speech if such restrictions can be shown to legitimately benefit constituents--in this case, UT's students. Observers noted that the court's rejection of White Buffalo's CAN-SPAM argument is important in that it presents a significant roadblock to organizations that would try to use the law to make it easier, rather than more difficult, to send unsolicited e-mail. Inside Higher Ed, 4 August 2005

Category 33.2 *Spam, spim, spit & splogs*

2005-08-10 **spam spammer Microsoft settlement Scott Richter New York**

EDUPAGE; http://www.nytimes.com/2005/08/10/technology/10spam.html

TOP SPAMMER SCOTT RICHTER SETTLES ON $7M PENALTY TO MICROSOFT

Microsoft has reached a settlement with Scott Richter, a man once described as one of the top three spammers in the world. Efforts by Microsoft and New York Attorney General Eliot Spitzer in 2003 resulted in the collection of 8,000 e-mail messages containing 40,000 fraudulent statements sent by Richter's company, OptInRealBig. Richter earlier agreed to pay New York State $50,000; under the new settlement, Richter will pay Microsoft $7 million. According to Bradford L. Smith, chief counsel for the software giant, $5 million would be used to "increase our Internet enforcement efforts and expand technical and investigative support to help law enforcement address computer-related crimes," while another $1 million will be spent on improving computer access for the poor in New York State. The settlement also requires Richter to comply with state and federal laws governing e-mail and to submit to oversight of his company's operations for three years. New York Times, 10 August 2005 (registration req'd)

Category 33.2 *Spam, spim, spit & splogs*

2005-10-13 **TechWorld spammer United States Sophos percent worldwide**

DHS IAIP Daily;
http://www.techworld.com/security/news/index.cfm?NewsID=4573

U.S. STILL WORLD'S TOP SPAMMER

Despite anti-spam laws the United States is still the world's top spammer. According to the latest report by Sophos, the US is still number one with 26 percent of all worldwide spam. However, the figure has been falling over the years. According to Graham Cluley, senior technology consultant for Sophos, "It has been lowering for awhile for a number of reasons. The anti-spam task forces and the authorities and the ISPs in North America are getting much better at putting into practice methods that are lowering the amount of spam."

Category 33.2 *Spam, spim, spit & splogs*

2005-10-25 **spam plague PC users Security holiday shoppers viruses IM hackers viruses**

DHS IAIP Daily; http://www.usatoday.com/tech/news/computersecurity/2005−
10−2
5−holiday−spamalanche_x.htm

PROJECTED INCREASE IN SPAM, SPIM & SPLOGS WILL PLAGUE PC USERS

Internet security experts are warning consumers of a wave of unwanted commercial e-mail in the weeks leading up to Thanksgiving, when the amount of spam could double as marketers try to reach holiday shoppers. The increase in spam is also due to the fact that more viruses are being spread by instant-messaging (IM) services that infect PCs and then turn them into zombies - machines that are remotely controlled by hackers to spread spam and more viruses. According to Andrew Lochart, director of product marketing at e-mail security company Postini, attacks on IM services increased 350 percent, to 541, in the second quarter from the previous quarter. Spammers are resorting to IM attacks because consumers use software to defend PCs from e-mail-based viruses, and "there isn't much in terms of anti-virus software for IM," he says. In addition, spammers are sending more e-mail in shorter bursts to overwhelm spam defenses. Blogs have also been penetrated by spammers to create "splogs," which are fake blogs with ads. According to Blake Rhodes, CEO of blog search engine IceRocket.com, about ten percent of the blogs created each day are considered splogs.

Category 33.2 *Spam, spim, spit & splogs*

2005-10-26 **spam spim splog spam-blogs fraud search engine distortion hacking GOOGLE**

RISKS; http://tinyurl.com/9498r 24 09

SPAM, SPIM, SPIT AND NOW -- SPLOGS!

Spam, long the scourge of email users, rapidly has become the bane of bloggers too.

Spammers have created millions of Web logs to promote everything from gambling Web sites to pornography. The spam blogs -- known as "splogs" -- often contain gibberish, and are full of links to other Web sites spammers are trying to promote. Because search engines like those of Google Inc., Microsoft Corp. And Yahoo Inc. Base their rankings of Web sites, in part, on how many other Web sites link to them, the splogs can help artificially inflate a site's popularity. Some of the phony blogs also carry advertisements, which generate a few cents for the splog's owner each time they are clicked on.

The phony blogs are a particular problem for Google, Microsoft and Yahoo because each offers not only a Web search engine focused on providing the most relevant results for users but also a service to let bloggers create blogs.

Just this past weekend, Google's popular blog-creation tool, Blogger, was targeted in an apparently coordinated effort to create more than 13,000 splogs, the search giant said. The splogs were laced with popular keywords so that they would appear prominently in blog searches, and several bloggers complained online that that the splogs were gumming up searches for legitimate sites….

[Excerpt from David Kesmodel's article in Wall Street Journal provided by Monty Solomon]

Category 33.2 *Spam, spim, spit & splogs*

2005-10-27 **zombie spammer Microsoft Internet Safety hunt junk e-mail CAN-SPAM FTC**

DHS IAIP Daily;
http://www.securitypipeline.com/news/172901034;jsessionid=Y2YXYNET4ZPCEQSNDBCSKH0CJUMEKJVN

MICROSOFT HUNTS FOR ZOMBIE SPAMMERS

Microsoft is investigating 13 spam operations it believes sent millions of junk mail messages through a single PC that the company purposefully set up as a "zombie," the company said Thursday, October 27. Tim Cranton, the director of Microsoft's Internet Safety division said, "By inserting ourselves in the spammers' path and looking upstream, we have been able to see things we have never been able to see before." The action was coordinated in conjunction with the Federal Trade Commission (FTC) and Consumer Action, a San Francisco-based advocacy group, to identify spammers. Spam operators working in the U.S. could be prosecuted under the federal CAN-SPAM Act. Cranton said, "Hopefully, we'll be able to turn over the results of our investigation for criminal prosecution under CAN-SPAM…We need to take a few more steps, but in the next two to three months, I think we can name these spammers." A new federal Website can be accessed for consumers to access information on protecting their PCs. Website: http://onguardonline.gov/index.html

---

Category 33.2 *Spam, spim, spit & splogs*

2005-11-23 **lawsuit litigation anti-spam Verizon Wireless unsolicited text messages**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1892707,00.asp

VERIZON WIRELESS SUES ANOTHER SPAMMER

Unwanted text messages from a Florida-based travel company were sent recently to 98,000 Verizon Wireless customers, according to a new lawsuit filed by the operator. Even though cell phone spam is still relatively limited, it's nonetheless forcing operators to get a handle on it since their subscribers often pay a fee for each incoming message. "Electronic attacks upon the Verizon Wireless interstate text messaging network will continue; indeed the latest attack was just weeks ago," Verizon attorneys wrote in the suit filed Monday, November 21, in a U.S. District Court in New Jersey. In this particular case, Verizon Wireless alleges that Passport Holidays LLC, of Ormond Beach, FL, sent unsolicited text messages to about 98,000 Verizon Wireless subscribers in the latter part of October. The lawsuit accuses Passport Holidays of using an automated dialer to send the text messages to phones in three East Coast area codes.

Category 33.2 *Spam, spim, spit & splogs*

2005-11-28 **FTC report spam e-mail filters improving anti-spam**

DHS IAIP Daily; http://today.reuters.com/news/NewsArticle.aspx?type=internetNews&storyID=2005−11−28T211837Z_01_SPI876594_RTRUKOC_0_US−SPAM.xml

FEDERAL TRADE COMMISSION: SPAM E-MAIL FILTERS GETTING BETTER

E-mail spammers are aggressive as ever but Internet providers are getting better at blocking junk messages before they reach users' inboxes, according to a U.S. Federal Trade Commission (FTC) study released on Monday, November 28. The FTC found that spammers continue to "scrape" e-mail addresses from the Web using automated programs that look for the telltale "@" sign. But up to 96 percent of those messages were blocked by the two Web-based e-mail providers used by the FTC in its test. The FTC did not say which providers it used in its study. "This encouraging result suggests that anti-spam technologies may be dramatically reducing the burden of spam on consumers," the report said. The FTC noted that Internet providers still must bear the burden of filtering out those messages. FTC Press Release: http://www.ftc.gov/opa/2005/11/spam3.htm FTC Spam study: http://www.ftc.gov/opa/2005/11/spamharvest.pdf

---

Category 33.2 *Spam, spim, spit & splogs*

2005-12-21 **CAN-SPAM Act legislation law FTC report Congress effectiveness legal action content filtering junk e-mail education recommendations**

EDUPAGE; http://www.theregister.co.uk/2005/12/21/can-spam/

FTC SAYS CAN-SPAM WORKING

The Federal Trade Commission reported to Congress on the effectiveness of the CAN-SPAM Act, concluding that legal action against spammers and improved e-mail filtering have reduced the amount of junk e-mail reaching consumers. The agency has filed 21 lawsuits under CAN-SPAM. Recommendations include passing new laws to help regulators trace spammers and sellers outside the United States, better user education on spam prevention, and continued improvement in filtering tools and techniques.

Category 33.2 *Spam, spim, spit & splogs*

2006-01-05 **spam anti-spam litigation judgment CAUCE Iowa ISP Florida spammer**

DHS IAIP Daily; http://www.press− citizen.com/apps/pbcs.dll/article?AID=/2006 0105/NEWS01/601050310/1079 23

IOWA COMPANY WINS $11 BILLION SPAM JUDGMENT

A Clinton, IA-based Internet service provider was awarded an $11.2 billion judgment against a Florida man for sending millions of unsolicited e-mails advertising mortgage and debt consolidation services. The lawsuit, filed in 2003 by CIS Internet Services owner Robert Kramer III, also prompted earlier judgments against companies in Florida and Arizona worth more than one billion. The most recent judgment was issued Friday, December 23, against James McCalla of Florida, who is also barred from accessing the Internet for three years. The lawsuit claimed that McCalla sent more than 280 million illegal spam e-mails into CIS's network, which provides Internet connections in Eastern Iowa and parts of Illinois. Kramer's lawsuit initially named numerous defendants, many of whom were dropped from the lawsuit the last couple years. John Mozena, co-founder and vice president of Coalition Against Unsolicited Commercial E-mail (CAUCE), said Kramer's lawsuit will likely not solve the spamming problem. He said, "There have been regulatory actions and even criminal actions against spammers, but it has not made much of a dent in the total volume of spam we see...Spam is still roughly two-thirds of all e-mail on the Internet."

Category 33.2 *Spam, spim, spit & splogs*

2006-01-13 **anti-spyware coalition ASC group guidelines**

DHS IAIP Daily; http://www.theregister.co.uk/2006/01/13/anti_spyware/ 23

ANTI-SPYWARE GROUP DEFINES DETECTION GUIDELINES

The Anti-Spyware Coalition (ASC), an alliance of software companies, security firms and consumer organizations, has agreed a set of guidelines on detecting invasive finalized spyware. The final draft of the ASC's "risk-modeling description" aims to give an objective criteria on whether a program is malign. A draft of this description was thrown open for public comment in October and the final version that's emerged is essentially an expanded and polished version. The group defines spyware and other potentially unwanted technologies as deployed without appropriate user consent and/or implemented in ways that impair user control over: material changes that affect their user experience, privacy, or system security; use of their system resources, including what programs are installed on their computers; and/or collection, use, and distribution of their personal or other sensitive information. In addition, ASC finalized the list of speakers for its first public meeting which is due to take place on Thursday, February 9, at the Hyatt Capitol Hill in Washington, DC. Federal Trade Commission (FTC) Chairman Deborah Platt Majoras will keynote at the single day event, which will also feature federal regulators, and top state technology and law enforcement officials.

Category 33.2 *Spam, spim, spit & splogs*

2006-01-24 **Bill Gates spam predictor inaccurate anti-spam solution**

DHS IAIP Daily; http://www.techweb.com/wire/security/177103408;jsessionid=F3 33FC31KIRIQQSNDBGCKH0CJUMEKJVN 23

BILL GATES' SPAM PREDICTION MISSES TARGET.

On January 24, 2004, Bill Gates told a group at the World Economic Forum that "two years from now, spam will be solved." During the talk, Gates pinned his prediction on the creation of an authentication scheme to verify senders' identities, as well as the hope that some kind of micropayment structure could be created for levying fees on e-mail. "We have a long way to go before we solve the spam problem," said Scott Chasin, the chief technology officer for Denver, CO-based e-mail security firm MXlogic. Neither of the proposals Gates mentioned two years ago have made much headway. Although Microsoft uses its own Sender ID authentication protocol for the company's Web-based Hotmail service, neither Sender ID nor the competing DomainKeys from Yahoo have anything like broad acceptance by ISPs or enterprises. And the micropayment concept for e-mail is as dead now as it was two years ago. Microsoft may take the position that "solving" the spam problem means containing spam with filtering technology, Chasin said, but even using that definition, spam remains a huge problem.

Category 33.2 *Spam, spim, spit & splogs*

2006-01-30 **study small businesses four times more spam**

DHS IAIP Daily; http://www.smallbizpipeline.com/showArticle.jhtml?articleID=177105260 23

SMALL BUSINESSES GET FOUR TIMES THE SPAM OF LARGER ENTERPRISES.

Small companies were sent almost 50 spam e-mails per day per user in 2005, up from 36 in 2004. This represents four times the number that employees at large companies were sent daily on average last year (12 per user per day in 2005 versus three in 2004). This is according to an annual report by Postini, a provider of message management solutions. The reason for this is that smaller businesses are more prevalent in targeted industries such as publishing, advertising, legal, and real estate, according to Andrew Lochart, senior director of marketing at Postini. "These are industries where you have 100 percent white collar workers whose e-mail addresses are very well known in the world," said Lochart. Another theory is that spammers may presume that larger companies are able to afford strong anti-spam measures, and may not try to infiltrate them as frequently, said Lochart. "What makes it a problem, regardless of why, is that smaller companies are the ones who have fewer defenses in place," said Lochart. "There are no large dedicated IT staffs in place, or large budgets for technology, so it's a double whammy." Postini original press release: http://www.postini.com/news_events/pr/pr013006_tr.php Postini's Annual Message Management and Threat Report: http://www.postini.com/whitepapers/?WPID=36

Category 33.2 *Spam, spim, spit & splogs*

2006-03-28 **MIT 2006 Spam Conference e-mail problems security antispam CAN-SPAM**

EDUPAGE; http://news.com.com/2100-7348_3-6055171.html 23

MIT CONFERENCE ADDRESSES E-MAIL PROBLEMS

Attendees at the 2006 Spam Conference at MIT agreed that filters and other technologies designed to prevent spam from reaching its intended targets merely address the symptoms without doing anything about the underlying problem. Many were similarly dismissive of proposals to charge a fee to senders of e-mail, saying that such an approach runs counter to the fundamental tenets of the Internet. Phil Raymond of Vanquish Labs compared a fee system to having first class and cattle cars on a train, suggesting that "some of [the cattle] cars will be left behind completely." Presenters at the conference instead urged adoption of economic incentives that would encourage users to be good e-mail citizens. Raymond, for example, proposed a system under which bulk e-mailers would be required to post a bond, against which recipients of those e-mails could make claims if they deemed messages to be spam. Opinions were mixed, however, about the CAN-SPAM Act. Jon Praed of the Internet Law Group said the legislation has done little to discourage spammers while placing new burdens on legitimate e-mail marketers. In contrast, Aaron Kornblum, a member of Microsoft's antispam legal team, said the law was the basis for 70 civil lawsuits that Microsoft has filed against spammers since January 1, 2004.

Category 33.2 *Spam, spim, spit & splogs*

2006-03-30 **spam spamming trick tactic filter evasion joe-job**

DHS IAIP Daily; http://www.theregister.co.uk/2006/03/30/joe_job_twist/ 23

JOE-JOB SPAMMERS SHIFT TACTICS TO EVADE FILTERS.

Spammers are applying a new twist to joe-jobbing -- a trick used to get around e-mail filters. Instead of forging the sender's e-mail, as done in conventional joe-jobbing, address spammers are deliberately sending their messages to an invalid e-mail address at a high profile company using a forged "From" address at a target company. Because of this, the IP address and the e-mail domain address now match and the junk e-mail message may be able to bypass e-mail filters.

Category 33.2 *Spam, spim, spit & splogs*

2006-04-21 **China to overtake US spam source**

DHS IAIP Daily; http://www.channelregister.co.uk/2006/04/21/spam_relay_hotlist/ 23

CHINA POISED TO PINCH U.S. SPAM CROWN.

China is closing in on the U.S. at the top of a league of spam relaying countries. According to statistics from security firm Sophos, China originated 21.9 percent of the junk mail messages captured in its spam traps compared to 23.1 percent for the U.S. Two years ago, the U.S. accounted for half of all spam sent in the world, a figure that has now dropped to less than a quarter, thanks to crackdowns against spammers and better information sharing among ISPs.

Category 33.2 *Spam, spim, spit & splogs*

2006-05-04 **spammer spam do-not-spam addresses Blue Security Blue Frog**

DHS IAIP Daily; http://www.smh.com.au/news/breaking/spammer−identifies−do −not−spam−addresses/2006/05/04/1146335837392.html 23

SPAMMER IDENTIFIES 'DO NOT SPAM' ADDRESSES.

One spammer has managed to identify e-mail addresses on Blue Security's Blue Frog "do-not-spam" list, taking advantage of an obvious flaw with such lists and prompting critics to wonder what took so long. The lists are generally encrypted so spammers can't mine them for new addresses. However, John Levine, co-author of Fighting Spam for Dummies, said spammers merely have to run their lists, see what's been removed and compare that with the original to find out the addresses on the "do-not-spam" lists.

33.3 Authorization, access controls

Category 33.3 *Authorization, access controls*

2003-02-24 **authorization confidentiality privacy control data leakage**

NewsScan

MICROSOFT PUTS A LOCK ON CORPORATE COMMUNICATIONS
Alarming organizations that encourage employee whistle-blowing on corporations engaged in wrongdoing, Microsoft has developed new technology called Windows Rights Management Services, which lets a company restrict which of its employees may access, download, print, or forward "company-sensitive" e-mail or Web material. Based on the XrML programming language, the software was created within Microsoft's Trustworthy Computing initiative focused on improving the security and privacy of information. But corporate accountability watchdogs are appalled. Joanne Royce of the nonprofit Government Accountability Project says, "It sounds to me like just another way to restrict the free flow of information. In a way it sounds like it won't hinder whistleblowers per se, because they won't even get to see this stuff." Michael Kohn of the National Whistleblower Center in Washington, D.C., calls the new technology "ludicrous" and warns, "You create a whole secret society within a corporation. Anyone who is within that circle is unlikely to be a whistleblower." (AP/USA Today 21 Feb 2003)

Category 33.3 *Authorization, access controls*

2004-01-14 **insider threat industrial espionage Voltaire**

NIPC/DHS; http://www.gcn.com/vol1_no1/daily−updates/24622−1.html

January 12, Government Computer News — Intelligence community seeks protection from inside threats.

A team of companies is building a tool to help the intelligence community keep tabs behind its firewalls. The Voltaire system will integrate existing technology to identify suspicious activity by insiders with legitimate access to sensitive information. Voltaire is intended to make it easier for agencies to share sensitive and classified information by providing a tool to enforce access policy and prevent misuse. The goal of Voltaire is to detect and stop the kind of activity that FBI turncoat Robert Hanssen got away with for years. Hanssen gathered and sold information about FBI counterintelligence activities by browsing through computer files to which he had access. Although he had no legitimate need to see much of the information, investigators found he was able to access it over a period of years without raising any flags. A demonstration version of Voltaire is expected to be ready for testing by summer. Feedback from intelligence agencies will then be implemented into a final product.

Category 33.3 *Authorization, access controls*

2004-01-26 **NIST IT security draft report guidelines safeguards standards advice risk management**

DHS/IAIP Update

January 23, Federal Computer Week — NIST releases telnet, IT security drafts.

Federal agencies desiring to minimize work disruptions from outside intrusions can begin with simple safeguards, such as preventing unauthorized users from using the telnet protocol to gain access to a server, according to officials at the National Institute of Standards and Technology (NIST). Draft documents on computer security released Thursday, January 22, by the NIST give an example of how unauthorized telnet users simply identify themselves as a guest to gain access to sensitive government files. The Risk Management Guide for Information Technology Systems suggests that disabling telnet is about a 10-hour procedure. Practical advice in the 58-page document includes other ways that agencies can develop standards for safeguarding sensitive but unclassified information in federal computer systems. As applied to information systems, the guide says, risk management is a responsibility of executive managers to be shared with technical managers, and not a technical manager's sole responsibility. Engineering Principles for Information Technology Security, a 33-page document also released this week, offers an overview of accepted principles and practices for security information technology systems. Additional information can be found on the NIST Website:
http://csrc.nist.gov/publications/drafts.html

Category 33.3 *Authorization, access controls*

2005-04-20 **identification authentication I&A encryption secure logon design failure control customer information passwords userIDs**

RISKS 23 85

SEVERAL US BANKS STILL REFUSE HTTPS FOR LOGON PAGES

Brad Hill noted a serious lapse of risk management in several banks' online systems:

>I was actually rather shocked to find that U.S. Bank (http://www.usbank.com/), Chase (http://www.chase.com) and Bank of America (http://www.bankofamerica.com) all still *force* users to enter their login and password on an insecure page. This exposes account holders to a great risk of their credentials being stolen. The login forms on their genuine home pages are submitted to a secure site, as they claim. The problem is that you need security *before* you enter your data. If DNS, a router or a proxy server anywhere along the path to their server were compromised, the login page could be substituted for one that submits to another site or injected with JavaScript that sends info elsewhere, asynchronously, before it goes to the real destination. Without an SSL certificate chain there is no way to verify that the insecure page with the form came from a trusted source and no way short of exhaustive code inspection to tell where the form data is actually going.

BankOne, Wells Fargo, Citi, Washington Mutual, Bank of the West, Key Bank and Sun Trust all offer SSL versions of their login page, but for some reason, U.S. Bank, BofA and Chase redirect to an insecure site or return an error when trying to connect with SSL. You *can't* log in securely, even if you try. The existence of this kind of obvious and fundamental security mistake after all the publicity about this category of attack (note that all these banks *do* have a user education page on phishing/fraud prevention!) is definitely something to keep in mind when choosing a bank.<

33.4 Risk analysis & management

Category 33.4 *Risk analysis & management*

2005-04-05 **risk management perception publicity public relations comments explanation clarity taking responsibility stupidity blame**

RISKS 23 83

RISK MANAGEMENT: GOOD VS STUPID RESPONSES TO DISASTERS

Michael "Streaky" Bacon published an excellent analysis of good vs stupid public response to disasters or near disasters:

Air disasters receive widespread press coverage. Crashes often cause people to cancel bookings with the affected airline. The share price often dips, sometimes severely, in the aftermath of an air accident.

This is also true for many other major incidents involving corporations (i.e., not 'natural' causes).

One thing often stands between a 'crisis of confidence' and 'business as usual', and that is the credibility of the organisation's spokespeople.

On 3 April, a Phuket Air 747 was twice forced by passenger action to abort a take-off from the UAE when fuel was seen flowing from the wing over an engine as the plane accelerated down the runway. A UK-based spokesman for the airline told the media that no-one had been in any danger and claimed that passengers had "panicked". He is also reported to have said that passengers were not qualified to judge what was safe or not. He said that the wing tanks had been "over-filled".

Whilst I do not comment upon the accuracy or otherwise of the spokesman's comments, I will comment on their advisability and I do suggest that this is not a good way to manage risk.

It is reported that many passengers have now refused to fly any further with the airline.

A contrast in risk management is provided by one British airline that suffered two 'incidents' with the same type of aircraft some nine years apart. In the first, the aircraft crashed with tragic loss of life following the (erroneous) shutdown of one engine and loss of power on the other (faulty) engine during an emergency landing. The Chairman of the airline was interviewed at the scene and with tears in his eyes promised to find out what had happened and to take every possible step to prevent its recurrence. The share price was not much affected, neither were bookings. The second incident concerned the loss of oil pressure in both engines shortly after take-off - leading to the shut-down of both engines and a successful 'dead-stick' landing. The loss of oil was caused by a maintenance failure. The airline put the 'Director of Engineering' (or similar title) in front of the media, and he attempted to explain away the incident as a problem with their maintenance company. It was reported at the time that passengers subsequently canceled bookings and the stock price fell.

The 'what', the 'way' and the 'how' of the Chairman were believable, those of the Director were not.

The RISK is in getting the wrong person to say the wrong thing. Effective crisis management involves the right thing by the right person at the right time in the right way to the right people.

[The first case is that of a British Midland 737-400 (RISKS-11.42). PGN]

Category 33.4 *Risk analysis & management*

2005-04-07 **credit card loss company agent training awareness confidentiality breach policy procedure stupidity identity theft**

RISKS 23 84

NO PROBLEM! BANK OF AMERICA AGENT REVEALS PERSONAL DETAILS TO FINDER OF LOST VISA CARD

When Caskey L. Dickson's wife reported a lost VISA card that she found, the Band of America agent on the support line cheerfully informed her -- without her asking -- of the owner's home phone number and billing address plus the fact that the card had not been reported stolen.

Despite the honest lady's protests that she did not need to know these things, the agent flippantly dismissed her concerns about identity theft with "Oh, that's not a problem."

Category 33.4 *Risk analysis & management*

2005-05-01 **risk management legacy systems denial of service failure software quality assurance replacement system failure**

RISKS; http://www.cio.com/archive/050105/comair.html 23 87

COMAIR EXECUTIVES DELAYED REPLACING LEGACY SYSTEM THAT FAILED

Stephanie Overby, writing in CIO magazine, analyzed the COMAIR disaster of December 2004. "[T]he legacy system [for managing flight crews] failed, bringing down the entire airline, canceling or delaying 3,900 flights, and stranding nearly 200,000 passengers. The network crash cost Comair and its parent company, Delta Air Lines, $20 million, damaged the airline's reputation and prompted an investigation by the Department of Transportation."

The details were as follows:

"As it turned out, the crew management application, unbeknownst to anyone at Comair, could process only a set number of changes—32,000 per month—before shutting down. And that's exactly what happened. On Christmas Eve, all the rescheduling necessitated by the bad weather forced the system to crash. As a result, Comair had to cancel all 1,100 of its flights on Christmas Day, stranding tens of thousands of passengers heading home for the holidays. It had to cancel nearly 90 percent of its flights on Dec. 26, stranding more. There was no backup system. It took a full day for the vendor to fix the software. But Comair was not able to operate a full schedule until Dec. 29."

All of this trouble could have been avoided had the warnings dating back to 1997 been heeded about the need to upgrade the then-11-year-old system, which was running on outdated hardware. The rest of the article goes into extensive detail about the management failures responsible for the debacle.

Category 33.4 *Risk analysis & management*

2005-09-11 **emergency management communications frequency bands risk analysis vulnerability politicians stupid pronouncements lack experience naïve elementary mistakes denial of service DoS vulnerability bandwidth saturation jamming disaster**

RISKS 24 04

POLITICIANS USUALLY AMATEURS AT EMERGENCY MANAGEMENT

It is sad that politicians start to believe that they know how to solve technical problems. One such sad case was Rudy Giuliani's pronouncement today that a single frequency (then frequency band) for all emergency services would make things work better. Now I am hardly the world's leading expert on radio frequency spectrum allocation, but I do have some small amount of experience in understanding radio communications and emergency response, and I was startled, well not all that startled, perhaps bemused at the lack of understanding displayed by people who are not risk management professionals. Of course it seems that a lot of political folks think that they can do as good a job as risk management professionals, and likely that is why we are in such a sad state as a nation state at handling emergencies. I haven't done a complete assessment of the suggestion, but here are some initial thoughts.

The idea is that communications will work better if everyone can talk to each other and therefore a single frequency band would allow them to do so and improve emergency communications. Sounds sensible, however…

1) It means that in order to disrupt ALL emergency communications I only need to jam one frequency band.

2) Different natural and artificial phenomena interfere with RF communications in different frequency bands, so by using a relatively limited portion of the available bandwidth, there is a guarantee that in some places no communications will work.

3) If I want to listen into your communications, it makes it a lot easier if I know the frequencies being used, and if everyone has to talk to each other, then anyone can listen to everyone else. Encryption won't solve this of course for the same reason.

4) If there is a big emergency and everyone is on a small subset of the bands available, there will be a lot of interference, reducing communications effectiveness.

5) Certain weather and other human induced conditions wipe out portions of the frequency band for periods of time, making ALL communications fail simultaneously (see 1 above).

6) Interference between jurisdictions means that dispatchers in one jurisdiction might end up talking over those of their neighbors, causing confusion and more traffic problems as well as increasing the potential for phony messages going on the air.

You all get the idea by now. Of course the last assessment I did that involved a radio communications system for a local government was several weeks back, and we were a bit concerned that they only had 3 redundant ways to communicate via RF - Car radios that talk to towers in redundant locations - hand-held radios on a different frequency range that could talk to the towers, the cars, and each other independently of the other tower system, and cellular telephones that they could use when the other systems failed. They also reported problems of interference on rare occasions with the frequencies used by neighboring jurisdictions (see 6 above), but only in certain locations where they could communicate over quite a long distance because of weather-related signal bounces off of clouds.

Different frequency bands are used for different things for good reasons, and there are good reasons that a single frequency band for emergency response would be a bad thing. Perhaps we should put Rudy in charge of FEMA and see if things get better or worse… after all, the last political appointee there with no expertise in emergency management worked out so well…

[By Fred Cohen]

Category 33.4 Risk analysis & management

2006-03-21 **business data center lack risk management plan study**

DHS IAIP Daily; http://www.securitypipeline.com/news/183701727 23

MANY DATA CENTERS STILL HAVE NO RISK MANAGEMENT PLAN.

Business technology managers are facing tough challenges as data centers grow larger and more complex. More than 75 percent of all companies have experienced a business disruption in the past five years, including 20 percent who say the disruption had a serious impact on the business, according to a recent survey of data center managers. Despite the critical nature of data center operations to business, nearly 17 percent reported they have no risk management plan, and less than 5 percent have plans that address viruses and security breaches. The results, which were announced Tuesday, March 21, at the Data Center World conference in Atlanta, are part of survey of nearly 200 members of AFCOM, a leading association for data center managers. Some of the predictions: Within the next five years, one out of every four data centers will experience a serious disruption; by 2015, the talent pool of qualified senior-level technical and management data center professionals will shrink by 45 percent; and over the next five years, power failures and limits on power availability will halt data center operations at more than 90 percent of companies.

34 Net filters, monitoring (technologies)

Category 34 *Net filters, monitoring (technologies)*

1997-01-17 **Web monitoring filtering**

PA News

CyberGuard introduced their Webtrack package to create audit records of where employees surf to on the World Wide Web. Employers have expressed concern about the amount of time that employees can waste by surfing the Net without discipline.

Category 34 *Net filters, monitoring (technologies)*

1997-01-23 **Spam**

RISKS 18 79

Filtering to refuse junk e-mail can lead to problems when the filters contain misspellings. Legitimate sources of e-mail can then be rejected because of similarities to the offending domain names.

Category 34 *Net filters, monitoring (technologies)*

1997-03-25 **spam filter**

EDUPAGE

An enraged programmer from California has developed software called Dead Bolt that allows victims of spam to pool their blacklists and thus improve anti-spam filtering. Critics charge that the system may be vulnerable to abuse if innocent people's addresses are fraudulently added to the list of spammers.

Category 34 *Net filters, monitoring (technologies)*

1997-03-25 **appropriate use censorship**

PR Newswire

WebAware, Inc. announced its new WebPrints product, which allows parents and corporate supervisors to see exactly which Web pages have been browsed by the users they supervise. See <www.webaware.birmingham.mi.us> for details. The product would appear to work only if the users being audited are unaware that they can empty their cache of images at the click of a button. By July, the URLs listed in the Yahoo directory were inoperative.

Category 34 *Net filters, monitoring (technologies)*

1997-03-27 **pornography filters**

EDUPAGE, AP

Filtering technology is still relatively crude, with amusing false positives and the possibility that objectionable Web sites can evade restrictions by avoiding key words used by the filters.

Category 34 *Net filters, monitoring (technologies)*

1997-06-26 **censorship decency children online CDA**

PR Newswire

The Children's Partnership announced its publication _The Parents' Guide to the Information Superhighway: Rules and Tools for Families Online._ See <http://www.childrenspartnership.org>. According to their press release, "The _Parents' Guide_ provides strategies and tips for parents to use to help their children benefit from computer technologies and online resources, while helping to ensure that their children will be safe while exploring the Information Superhighway. The guide includes age-specific tips for online activities as well as listings of blocking device software."

Category 34 *Net filters, monitoring (technologies)*

1997-06-30 **censorship pornography filter**

AP

Calvin Woodward of the Associated Press investigated the effectiveness of computerized smut filter programs. A test of Cyber Patrol, a popular tool for parental controls, showed inconsistent results when tested with requests including words such as "personal," anything but "ducks" ending in -"ucks," words containing "sex" (although the subtlety was improved, with Anne Sexton's work and geographical place names being passed through), and spotty results in the "health" and "sex education" areas. Experts continue to warn that no programmatic filter can replace parental involvement with their children's Web surfing.

Category 34 *Net filters, monitoring (technologies)*

1997-07-25 **Web vandalism**

PA News

Allied Domecq, British makers of Barking Frog "alcopop" (alcoholic beverages that can hook children into alcohol dependency) offered its young victims the opportunity to build their own mini-Web-sites on its own Web site. Although the company normally screens such personal pages, it missed one in which someone posted references to the Devil and advice on how to masturbate. Embarrassed by these references (but not by selling alchol to kids), the company pulled this feature from its Web site.

Category 34 *Net filters, monitoring (technologies)*

1997-07-30 **pornography ISP**

AP

CompuServe announced new regulations that would require its 5.4 million customers to register for access to "adult" materials online. Confirmation of such registration will be mailed to the account holders.

Category 34 *Net filters, monitoring (technologies)*

1997-08-17 **Internet pornography games**

AP

Parents and residents of Dunblane, Scotland as well as many others were shocked and disgusted when a warped user of Virgin Net, a London ISP, created and distributed a computer game where players gained points by killing children. The ISP terminated the account of the creator of this disgusting exercise as soon as it was brought to their attention.

Category 34 *Net filters, monitoring (technologies)*

1997-08-27 **e-mail filter children education Internet**

Newsbytes

A new consortium began providing e-mail for children in September. Called "WhoWhere?", the consortium includes The Lightspan Partnership and Computers for Education. Because most schools cannot provide one computer for each child, WhoWhere stores its e-mail centrally. Children access their e-mail from any terminal or computer. The service includes e-mail filtering to protect the children against inappropriate content. See <http://www.whowhere.com> for more information.

Category 34 *Net filters, monitoring (technologies)*

1997-09-11 **pornography filter**

DPA

In Darmstadt, Germany, US scientist James Ze Wang presented Internet pornography filtering software based on pattern recognition of images. Porno-Blocker should be available soon with support from Stanford University, which owns commercial rights to Dr Wang's invention.

Category 34 *Net filters, monitoring (technologies)*

1997-10-05 **pornography statistics appropriate use policy**

EDUPAGE, OTC

According to the EDUPAGE editors, "A study conducted by Digital Detective Services found that one in four corporate computers investigated contained pornographic files, including some cases of child porn. The study was based on 150 investigations over an 11-month period. (Investor's Business Daily 3 Oct 97)" The firm, based in Falls Church, VA, also reported that many small and medium firms have no formal policies on Internet use. Relying on self-policing does not work.

Category 34 *Net filters, monitoring (technologies)*

1997-10-26 **anti-spam proxy server**

EDUPAGE

Lucent Technologies announced the Personalized Web Assistant as an anti-spam system that filters out unwanted commercial e-mail. Lucent said they might offer the product to ISPs as a value-added feature for e-mail users.

Category 34 *Net filters, monitoring (technologies)*

1998-01-04 **Internet monitor audit trail parents children**

AP

The new NetSnitch software that came on to the market in August, unlike net-filtering software, doesn't stop children from accessing different parts of the Internet. The product keeps an audit trail so that parents can evaluate how much time their children are spending on the Internet and list the web sites that the kids have visited. Ideally, the software would be used openly by parents, not inserted on children's computers in secret.

Category 34 *Net filters, monitoring (technologies)*

1998-01-20 **censorship Web filters free speech law PICS**

EDUPAGE

The ACLU criticized the World Wide Web Consortium (W3C) for its Platform for Internet Content Selection (PICS) standard, saying that, "The W3C is taking on a quasi-governmental role, and to the extent that the standards it adopts become the basic standards of the Internet, it will have more influence than most national governments will have. These are not mere technical standards that engineers should be establishing. This platform raises fundamental questions about free speech, and that debate should occur in public."

Category 34 *Net filters, monitoring (technologies)*

1998-01-22 **obscenity filter quality assurance QA data diddling hostile**

RISKS 19 56

Ross Johnson of the University of Canberra reported that Cybersitter Internet filtering software deleted the character string "NUDE" from his source files even though the characters in question actually occurred over a line break and despite intervening characters. They were part of the code
#define one 1 /* foo menu */
#define two 2 /* bar baz */
which therefore appeared as
#define one 1 /* foo */
fine two 2 /* bar baz */
much to the annoyance of the (non-coprolalic) programmer.

Category 34 *Net filters, monitoring (technologies)*

1998-02-10 **filtering legislation law regulation libraries schools**

EDUPAGE

John McCain (R., AZ) introduced a bill requiring schools and other recipients of federal money must use filtering software to prevent children from accessing indecent material. Cosponsors were Hollings (D., SC), Murray (D., WA), and Coats (R., IN).

Category 34 *Net filters, monitoring (technologies)*

1998-02-22 **filtering censorship QA**

EDUPAGE

According to EDUPAGE: <<The magazine Sky & Telescope says that the use of filtering software programs has prevented some schools from accessing Sky Online (http://www.skypub.com) because of the site's use of the word "naked," as in the expression "the naked eye." (Sky & Telescope Mar 98)>>

Category 34 *Net filters, monitoring (technologies)*

1998-07-28 **filtering Internet Web schools acceptable use policy**

EDUPAGE

Quality Education Data of Denver, CO released a study showing that 39% of the primary and secondary schools they studied with Internet connections filtered their students' access to the Net. About 80% had acceptable-use policies in place.

Category 34 *Net filters, monitoring (technologies)*

1998-10-28 **criminal hacker reverse engineering cryptanalysis censorware**

New York Times
http://www.nytimes.com/techweb/TW_Teen_Group_Distributes_New_Net_Filter_Crack.html

The Peacefire group of anti-censorware hackers decrypted the master password used to safeguard the list of forbidden sites in the Cyber Patrol Internet filtering program. Peacefire created a program to disable the filtering software; the 2000 downloads of that "crack" in a few days indicated the level of interest by young people in beating their parents' and their schools or libraries' efforts to restrict access to the Net. Learning Company immediately issued a patch to interfere with the crack.

Category 34 *Net filters, monitoring (technologies)*

1998-11-11 **hate speech filter censor software**

Wired
http://www.wired.com/news/print_version/email/member/culture/story/16197.html

The Learning Company, makers of the porn-filtering software CyberPatrol, worked with the Anti-Defamation League to create and release HateFilter, a similar tool for blocking access to hate-mongering sites. The ADL national chairman said, "We are engaged in a full-blown battle against high-tech hate. Bigots are seducing our children with online messages presented in full-color animation with music and video.... Parents should be able to protect their children from hate by keeping bigotry and prejudice out of their homes." Naturally, there were protests (including the usual use of the phrase "slippery slope") from anti-censorship organizations and from some of the blocked sites. The American Family Association, in particular, was blocked by CyberPatrol lists in June 1998 because of its homophobic content — which it stoutly defended as legitimate points of view, not hate-speech. Some critics pointed out that the new filter was not the first of its kind; the Church of Scientology developed filters for its members to prevent them from reaching Web sites critical of the CoS.

Category 34 *Net filters, monitoring (technologies)*

1999-01-26 **censorship filtering parental controls restrictions porn**

TechWeb

The RuleSpace Company announced a new pornography filter using the Intelligent Content Recognition Technology they claimed would make more reasonable distinctions about the content of sites using words such as "breast." The company said it opposed the use of filtering software in public schools and libraries and aimed its product at parents.

Category 34 *Net filters, monitoring (technologies)*

1999-04-06 **pornography cryptography encryption communications**

Business Wire

In an ugly development, pornography sites are providing strong encryption for their wares, making it difficult for investigators searching for evidence on data storage devices to accumulate evidence of illegal activity such as the use of child pornography. Encrypted porn is also impossible for filtering software to identify. The availability of NovaStor on the Web means that people can encrypt and decrypt files freely using the "Secret Service" function that simulates a safe using the company's DataSAFE software.

Category 34 *Net filters, monitoring (technologies)*

1999-04-08 **filter censorship restriction pornography lists keywords**

New York Times

Cybersitter and Clickchoice, makers of censorware, that favorite bugaboo of prepubescents everywhere, got into a legal battle over dirty words. Cybersitter accused Clickchoice of reverse engineering its proprietary list of filthy keywords and said it was considering a lawsuit. This situation may be fallout from the widespread cracking of censorware Naughty-Naughty lists; Cybersitter, in particular, was cracked in 1997 by Bennett Haselton, founder of the anti-censorware group Peacefire. The Index Verborum Prohibitorum was posted all over the Net within days, no doubt to the delight of the same prepubescents who didn't like the original product.

Category 34 *Net filters, monitoring (technologies)*

1999-09-25 **Web Internet ISP censorship rating pornography**

New York Times, Guardian (London)

The Internet Content Rating Association (ICRA) will try to create the first world standard based on RSACi, a rating system developed by the Recreational Software Advisory Council (www.rsac.org), a non-profit body in the United States. At a private meeting in Paris in mid-April, the major worldwide ISPs discussed how to help parents, schools and employers filter out objectionable materials more effectively than current methods. At present, the voluntary rating systems have managed to classify only about 1% of the world's sites; the new initiative would include better standards and more widespread publicity to encourage users to put pressure on providers to rate their sites. In addition, plans included spot checks to verify accuracy of the ratings.

Category 34 *Net filters, monitoring (technologies)*

2000-07-20 **workplace monitoring surveillance controls civil liberties employees employers covert law proposal legislation**

NewsScan,

A group of bipartisan lawmakers . . . introduced legislation that would require companies to disclose their workplace monitoring activities to employees when they are hired, and to update them on an annual basis. Under the bill, employers could still secretly monitor an employee if there is "reasonable" suspicion that illegal activity is taking place, but workers could not be routinely monitored without their knowledge. The American Management Association reports that 45% of companies with 1,000 or more employees snoop on workers in some way, but Sen. Charles Schumer (D-NY), a co-sponsor of the bill, says the figure is closer to 75%. "We would never stand for it if an employer steamed open an employee's mail, read it and put it back," says Schumer. "It is the same thing with an employee's e-mail." The bill has attracted a wide range of supporters, from the left-leaning American Civil Liberties Union to the conservative Eagle Forum. (MSNBC 20 Jul 2000)

34.1 Net filters

Category 34.1 *Net filters*

1996-12-20 **net filter censorship legal extortion bullying**

Netly News http://cgi.pathfinder.com/netly/editorial/0,1012,453,00.html

In July 1996, Declan McCullagh and Brock Meeks, authors of the aggressively confrontational and always interesting "Cyberwire Dispatch," revealed the hidden political agenda of Solid Oaks Software, makers of the CyberSitter net filter. Seems the lightly-encrypted list of forbidden sites included not only pornography purveyors but also the Web page for the National Organization of Women, the International Gay and Lesbian Human Rights Commission, and even of sites critical of CyberSitter and Solid Oaks. In December 1996, McCullagh reported on the responses of Brian Milburn, President of Solid Oak Software. In quick succession, he and his lawyers
* accused the writers of decompiling his copyrighted software in violation of the Solid Oak copyright and threatened criminal prosecution (never materialized);
* demanded that several Web sites critical of their product be shut down and the Web site managers expelled from their ISPs.
Think twice about what kind of automated controls you choose to put on your computers. You may be filtering more than you thought you would.

Category 34.1 *Net filters*

2000-01-29 **censorware filtering error**

RISKS 20 77

Some censorware (Internet filtering software) in libraries blocked access to the Superbowl XXXIV Web site because of the "XXX" string.

Category 34.1 *Net filters*

2000-03-16 **pornography libraries access children censorship filtering monitoring audit trail debate argument study research**

NewsBytes

In the endless debate between supporters and opponents of Internet filtering (censorware) to prevent kids from seeing pornography, the extreme right-wing Family Research Council endorsed a study by David Burt (Dangerous Access, 2000 Edition: Uncovering Internet Pornography in America's Libraries) claiming to show that children do in fact access pornography on public library computers. The official position of the American Library Association (ALA) is that very few children access pornography on library computers (the ALA's director has said that "only one child out of a trillion billion might use library computers to seek out pornography" — this despite objections from some working librarians who have come to dread helping users of their terminals for fear of confrontation with various forms of nastiness online. On the other hand, to put things in perspective, the FRC supports homophobia, opposes abortion, objects to First Amendment protection for art museum exhibits, argues that a woman's place is in the home, and describes feminism as having an "unrealized and ironic relationship to the cheapening of life and the value of womanhood, the growth of an overbearing government, and the decline in family and marital stability."

Category 34.1 *Net filters*

2000-09-21 **filtering censorware proprietary formats standards communications interoperability market dominance**

RISKS 21 06

Richard Schroeppel commented on the accommodation to aggressive censorware (e.g., using ** to modify words that might get a document bounced silently by filters) and asked readers to think about the implications of allowing policy-setters to destroy communications without notice based on proprietary standards such as secret lists of banned words or requirements for use of specific formats such as Adobe Acrobat PDF or Microsoft Office files.

Category 34.1 *Net filters*

2000-09-22 **censorware pornography filtering photographs images algorithm**

InformationWeek

Content Technologies announced a new pornography filter called Pornsweeper. the product looks at every incoming e-mail and attachment and differentiates likely candidates for rejection by the presence of too much "skin tone" compared with other colors in the image. Users determine the cutoff point.

Category 34.1 *Net filters*

2000-12-08 **censorware false positive incompetence stupidity**

RISKS, http://sethf.com/anticensorware/smartfilter/gotalist.php 21 14

In another spectacular demonstration of the importance of reverse engineering to expose incompetence, someone cracked the blacklist used by the SmartFilter censorware and discovered that several serious information security resources were erroneously blocked because they are classified in the "criminal skills" group: comp.risks, comp.dcom.telecom, comp.org.cpsr.announce, comp.org.eff.news, comp.protocols.tcp-ip, comp.security.announce and several others.

Category 34.1 *Net filters*

2001-06-06 **censorware content filtering algorithms heuristics errors false positives QA quality assurance design flaw e-mail blocking**

RISKS 21 47

Dan Birchall found that his e-mail newsletter was rejected by some censorware products, apparently because the phrase "sizzling summer" was determined to be indicative of pornography. Birchall suggested, "A better method might combine heuristics with the scoring capability in some mail server software (I'm personally familiar with Exim), incrementing or decrementing a counter based on the occurrence of given words or phrases, with actions depending on the final value of the counter. Thus, if "sizzling" is a +1 word, "video" a +2 word, and "sex" a +3 word, a threshold of 3, 4 or 5 might be used for blocking."

Category 34.1 *Net filters*

2001-06-10 **censorware content filtering algorithms heuristics errors false positives QA quality assurance design flaw e-mail blocking**

RISKS 21 47

Lauren Weinstein, moderator of the PRIVACY Forum, tracked down the reason a censorware content filter blocked his respected publication on a particular site: his quotation of the day included a reference to the movie, "I Love You, Alice B. Toklas!" Unfortunately, the ScanMail filter spotted the "I Love You" and apparently classified the message as a worm or virus. A disgusted Weinstein added, "With such a level of "stone club" analysis at work, one can only imagine what other innocent e-mail is being injected, inspected, detected, infected, neglected, and selected by the "sophisticated" algorithms of filtering programs to be flagged, reviewed, dropped, banned, burned, or trashed."

Category 34.1 *Net filters*

2001-06-27 **censorware e-mail filter algorithm false positive crude gross heuristics pattern matching**

RISKS 21 50

Jurjen N.E. Bos contributed yet another e-mail filter failure to RISKS:

"The IACR (International organisation of Cryptology Research) has someone on its Board of Directors named Don Beaver. The direct result of this is that the recent IACR newsletter (a 34K document full of relevant news on the cryptologic community) was rejected by our company firewall, because his name was in there too many times. It also contained other "dirty" words, such as LaTeX, hardcore, and so on. Our IT department told me that the message would *not* have been rejected if it was split in two, since the number of dirty words would have been halved. . . ."

Category 34.1 *Net filters*

2001-07-25 **censorship content filtering parental control technology V-chip television**

NewsScan

FIVE YEARS AFTER INTRODUCTION, V-CHIP GETS VERY LITTLE USE
The so-called V-chip devices, which have been installed in new TV sets since 1996 (when President Clinton urged Congress to make them mandatory so that parents could "assume more personal responsibility for their children's upbringing"), are used by only 7% of all parents. The Kaiser Family Foundation said the reason the V-chip is used so little is that the TV networks have little interest in promoting it (since programs from those same networks be blocked by the device). (New York Times 25 Jul 2001)
http://partners.nytimes.com/2001/07/25/arts/television/25CHIP.htm

---

Category 34.1 *Net filters*

2001-10-23 **content filtering censorship labeling voluntary children parental guidance**

NewsScan

AOL, YAHOO, MSN BACK NET FILTERING SYSTEM
The Internet Content Rating Association, supported by AOL, Yahoo, and MSN, will use a rating system in which Web operators would label their sites if they have potentially objectionable material (such as nudity or gambling), so that parents can approve or disapprove each category for access by the children. An executive of the Association says that the value of a voluntary self-labeling system is that it's "about choice--not censorship--on the Internet. We believe that good corporate citizenship and tools that help parents made good decisions is a much better alternative than government regulation." (AP/Washington Post 23 Oct 2001)
http://www.washingtonpost.com/wp-dyn/articles/A37920-2001Oct23.html

---

Category 34.1 *Net filters*

2002-01-23 **censorware content filtering antispam algorithm simplistic false positive availability**

RISKS 21 90

MS-Outlook's "adult content filter" assumes that the phrase "over 18" automatically and inevitably means that an e-mail message is pornographic spam. Outlook therefore rejected an issue of Microsoft's own e-mail MSDN Flash newsletter because it contained the phrase "provides over[space]180 hours of content in three technical conferences."

Category 34.1 *Net filters*

2002-04-11 **intellectual property law proposals censorship censorware libraries content filtering**

RISKS 22 03

Marc Rotenberg published a thoughtful essay in RISKS celebrating the 50th anniversary of the publication of Ray Bradbury's novel, _Fahrenheit 451_, drawing parallels between the nightmarish world of the novel and some of the trends he sees in the USA today. In the novel, all written language is banned; in today's America, "Already software filters have been turned on controversial ideas and unpopular organizations. And new copyright techniques will digitally incinerate recorded words that might otherwise be widely available."

Category 34.1 *Net filters*

2002-12-11 **content filtering pornography study research libraries**

NewsScan

A LITTLE BIT OF ANTI-PORN FILTERING CAN GO A LONG WAY
"A little bit of filtering is O.K., but more isn't necessarily better," says Vicky Rideout, vice president of the Henry J. Kaiser Family Foundation, which conducted a study showing that when anti-pornography Internet filtering software is set at a low level of restriction, it's just as effective as when it is set a high level, and is far less likely to prevent searchers from reaching bona fide health sites. But some observers, such as Judith F. Krug of the American Library Association, think that filters are such blunt instruments that they should not be used at all in public institutions: "Filters are just fine for parents to use at home. They are not appropriate for institutions that might be the only place where kids can get this information." The filtering programs generally block any references to sex-related terms; examples given by the report include such subjects as safe sex, condoms, abortion, jock itch, gay, and lesbian. (New York Times 11 Dec 2002)

Category 34.1 *Net filters*

2003-04-07 **pornographic sites blocked Pakistan**

NewsScan

PAKISTAN FILTERS 1800 SITES TO BLOCK PORNOGRAPHY
On the order of the Pakistani government, Pakistan Telecommunications is blocking at least 1800 Web sites described as pornographic. Hafiz Muhammed Taqi, a religious leader in that country, says: "This is one good move on the part of the present government. The young generation should be saved from sinking neck-deep in the filth of pornography and vulgarity;" however, Web software engineer Farhan Parpia, skeptical of the effectiveness of such filters, note that "curbing porn sites is as difficult as blocking the wind. You block one, and dozens more come up like mushrooms." (AP/USA Today 7 Apr 2003)

Category 34.1 *Net filters*

2003-06-24 **pronography child library block pornographic sites web**

NewsScan

COURT UPHOLDS LAW REQUIRING SOFTWARE FILTERS IN LIBRARIES
The U.S. Supreme Court, in a 6-3 opinion, has upheld provisions in the Children's Internet Protection Act that require public libraries to install anti-pornography software filters, if those libraries are to receive federal grants and subsidies. All nine justices agreed that there was no constitutional problem in a decision to restrict children's access to pornographic material, and that software filters are blunt instruments that inevitably block more material than the statute contemplates; still, the majority did not view this over-blocking as an infringement of the First Amendment rights of adult library patrons. To the argument that adults might be embarrassed by having to ask librarians to unblock pornographic sites for their viewing, Chief Justice Rehnquist wrote that "the Constitution does not guarantee the right to acquire information at a public library without any risk of embarrassment." (New York Times 24 Jun 2003)

Category 34.1 *Net filters*

2003-07-24 **libraries net filtering FCC CIPA software unblock**

NewsScan

LIBRARIES GET REPRIEVE ON NET FILTER DEADLINE
The Federal Communications Commission said yesterday that libraries will have an extra year to comply with the provisions of the controversial Children's Internet Protection Act (CIPA), which mandates that libraries accepting federal funding must install Internet filtering software. The new deadline is July 1, 2004. Opponents of the Act — including the American Library Association and the American Civil Liberties Union — have challenged CIPA, saying it violates free speech guarantees, but the U.S. Supreme Court ruled June 23 that CIPA did not infringe on First Amendment rights, noting "the ease with which patrons may have the filtering software disabled" by asking a librarian to unblock a particular site. (CNet News.com 24 Jul 2003)

Category 34.1 *Net filters*

2003-11-03 **censorship software bad words profanity misspelling accidental denial-of-service DoS**

RISKS 23 1

Another victim of the d__n bad-word filter!

RISKS contributor Adam Abrams could not register as a user on an e-commerce Website because his e-mail address was flagged as containing profanity. Abrams had to ring up customer service reps at collectorcartraderonline.com in order to complete his registration. Abrams speculates which string in his e-mail address, "adamabrams@shaw(dot)ca," was red flagged. "Could it be "bra"?" he asks. "rams?" "No, it was "dam"," he concludes. A misspelled bad word had caused the problem--Abrams complains against being "punished for other people's illeteracy"!

Category 34.1 *Net filters*

2003-12-11 **spam-filtering software free nonprofits Mailshell Inc. www.stopspamtoday.org**

NewsScan

FREE SPAM-FILTERING SOFTWARE FOR NONPROFITS
Mailshell Inc., maker of anti-spam software, is offering nonprofits and charities a holiday gift — free one-year subscriptions to its $30 software product. "Nonprofits can't necessarily avail themselves of cutting-edge technologies," says Mailshell marketing VP Eytan Urbas. "These are people who are working hard, a lot of them don't make a lot of money, for things they believe in. It feels like the right thing to do to support that." To avail themselves of Mailshell's offer, nonprofits with a 501(c)(3) designation should sign up by Friday at www.stopspamtoday.org. (AP 11 Dec 2003)

Category 34.1 *Net filters*

2003-12-15 **censorship filtering e-mail security politics**

RISKS 23 9

AOL now filtering based on whether they like embedded URLs

Contributor Stever Robbins discovered that AOL was blocking all e-mail with the URL of moveon.org, a political Website that criticizes President George W. Bush's policies. He fears the risk in such silent censorship is that "AOL can decide they don't like a particular URL, for instance, of a topic or candidate or public opinion poll that they disapprove of, and voila -- several million people now can't even be told about that page! "

Category 34.1 *Net filters*

2004-02-24 **pornography indecendy automated filtering false positives failure**

RISKS; http://www.mercurynews.com/mld/mercurynews/business/8026783.htm 23 20

SENDING E-MAIL CAN BE A STRUGGLE IF YOUR NAME HAS A 4- LETTER WORD

Drew Dean summarized a story in the _San Jose Mercury News_ by Mike Cassidy: >A Scottish gentleman named Craig C*ckburn (generally pronounced Coburn) had all too difficult a time receiving his e-mail. It turns out that Mr. C*ckburn's job title is "senior IT application speci*list", which also has problems due to the word "speci*list" containing the substring "ci*lis" (when used as a proper noun, a Vi*gra competitor). Not new, but increasingly painful for many people.<

Category 34.1 *Net filters*

2004-05-27 **movie censorship filtering DVD player**

http://www.nytimes.com/2004/05/27/technology/circuits/27stat.html?ex=1400990400&en=7f1caf6facfff153&ei=5007&partner=USERLAND

AUTOMATED CENSORSHIP

The RCA DRC232N DVD player includes ClearPlay technology that blocks out violence, sexual language, nudity, crude language, cursing, profanity, ethnic slurs, references to drug use and "vain or irreverent reference to G-d or a deity" — automatically. The scene-skipping software is based on profiles downloaded to the player; the profiles are defined by the human operators at ClearPlay. Investigation of the pattern of censorship reveals that the standards of the censors are "wildly inconsistent" (in the words of the New York Times' David Pogue). Pogue points out that "ClearPlay's most ridiculous assumption, however, is that excising only the split second of central violence somehow makes the overall scene less traumatic." In general, reports Pogue, the system seems remarkably tolerant of violence, for all its claims to transform movies for family viewing.

Category 34.1 *Net filters*

2006-05-30 **spam filter censorship obscenity algorithm words blocking denial-of-service availability e-mail**

RISKS 24 30

COMPUTER C*CK-UP FINDS E-R-E-C-T-I-O-N HARD TO HANDLE

Yet another example of the perils of simple-minded content filtering:

>Two e-mail messages objecting to a home extension failed to reach a council planning department because their computer system blocked the word "e-r-e-c-t-i-o-n". Commercial lawyer Ray Kennedy, from Middleton, Greater Manchester, claims he sent three e-mails to Rochdale council complaining about his neighbour's plans. But the first two messages failed to reach the planning department because the software on the town hall's computer system deemed them offensive. When his third e-mail, containing the same word, somehow squeezed through, it was too late. A planning officer told Mr Kennedy that his next-door neighbour's proposals had already been given the go ahead.<

[Abstract by Nick Rothwill edited by Peter G. Neumann to reduce likelihood of blocking of the entire issue of RISKS]

[MK adds: another issue is that naïve users are increasingly unware that the technical specifications for e-mail do not include guaranteed delivery. If delivery matters to you, CHECK FOR IT. Why didn't Mr Kennedy write a letter if the issue was so important to him?]

34.2 Usage monitoring, audit trails (employees, children)

Category 34.2 *Usage monitoring, audit trails (employees, children)*

2000-01-21 **privacy monitoring employer employee alert awareness expectation**

NewsScan, TechWeb http://www.techweb.com/wire/story/TWB20000121S0014

The newest version of Investigator, the software made by WinWhatWhere that's used by some companies to monitor employees' every keystroke, will add an optional banner alerting users to the presence of the system and telling them they are consenting to its use by operating the computer. Previous versions had been difficult to detect, leading some privacy advocates to complain about its sneaky intrusiveness. "I heard a lot of concerns about the invisibility of the program," says WinWhatWhere president Richard Eaton. "It had a splash screen that was just momentary, but this requires the user to acknowledge the message by clicking on a button before it goes away." (TechWeb 21 Jan 2000)

Category 34.2 *Usage monitoring, audit trails (employees, children)*

2000-02-11 **civil lawsuit seizure evidence disk drives subpoena investigation employees home computers protests labor action**

POLITECH, World Socialist Web Site
http://www.wsws.org/articles/2000/feb2000/nwa-f11.shtml

In February, Northwest Airlines succeeded in getting a subpoena allowing their investigators to seize computers from the homes of 21 named employees whom the company accused of organizing and staging a "sick-out" that forced cancellation of many flights. Investigators copied data from hard drives, including private e-mail, and also searched computers at the offices of Teamsters Union Local 2000 in Bloomington, MN. Many advocates of free speech protested the action.

Category 34.2 *Usage monitoring, audit trails (employees, children)*

2000-04-18 **Internet filtering monitoring hardware**

NewsScan, CNet http://news.cnet.com/news/0-1004-200-1713007.html

Juniper Networks is shipping a new processor called Internet Processor II, a souped-up version of an earlier filtering technology that scans data flowing through a network to detect suspicious traffic. The Internet Processor II is capable of filtering 20 million packets of data a second, compared with older security software that could handle only 200,000 data packets per second. The older software slowed networks down so much that ISPs were reluctant to implement it. (News.com 18 Apr 2000)

Category 34.2 *Usage monitoring, audit trails (employees, children)*

2000-11-10 **privacy censorship monitoring lawsuit judgement decision education school records parents children teachers faculty staff**

NewsScan

A New Hampshire judge has ruled that, since computers in schools are not for personal use but "as an integral part of the education curriculum," Internet history logs showing what sites are visited by students, faculty, and staff are public information open to inspection by any parent or parents willing to pay the cost of copying the information to disk after editing it to eliminate names and passwords of individual users. (New York Times 10 Nov 2000)
http://partners.nytimes.com/2000/11/10/technology/10CYBERLAW.html

---

Category 34.2 *Usage monitoring, audit trails (employees, children)*

2001-02-23 **privacy children censorware**

NewsScan

FILTERING FIRM ABANDONS PLANS TO SELL DATA ON KIDS
Under heavy pressure from privacy groups, the company N2H2, a maker of the "Bess" Internet filtering software, has decided to stop selling marketing research companies its "Class Clicks" list that reports the Web usage patterns of school children. The Bess software is used by 14 million students in the U.S. Company executive Allen Goldblatt says that no personally identifiable data on children were ever collected or sold and that "we never would, never have, and never will jeopardize anyone's privacy." Although characterizing the controversy as "a distraction for us," Goldblatt added: "I think any time you have a great public debate about privacy issues, ... this is a good thing." (AP/USA Today 23 Feb 2001)
http://www.usatoday.com/life/cyber/tech/2001-02-23-kids-privacy.htm

---

Category 34.2 *Usage monitoring, audit trails (employees, children)*

2001-04-01 **privacy Web cookies usage monitoring lawsuit judgement**

NewsScan

FEDERAL COURT RULES IN FAVOR OF COOKIES
U.S. District Court Judge Naomi Reice Buchwald has dismissed a class-action suit against online advertiser DoubleClick accusing that company of privacy-related violations of three federal laws. The judge concluded that DoubleClick had not violated those laws through its use of "cookies" (techniques for automatically tracking the movements of Web surfers), and ruled that Web sites could be considered DoubleClick's real "users" and could therefore give consent to monitoring of the transactions with individual customers who visited those cites. Privacy expert Paul Schwartz of Brooklyn Law School offers a different view: "The court said the Web site is the 'user' of the electronic service and can give consent to DoubleClick. So what are the individual consumers, chopped liver?" (New York Times 6 Apr 2001)
http://www.nytimes.com/2001/04/06/technology/06CYBERLAW.html

Category 34.2 *Usage monitoring, audit trails (employees, children)*

2001-06-12 **information gathering data mining investigation audit scanning workplace privacy forensics investigation police law enforcement management policy**

NewsScan

NEW CORPORATE SOFTWARE SEARCHES EVERYWHERE -- EVEN PERSONAL HARD DRIVES
New productivity software from AltaVista will allow companies to collect data from anywhere in the organization: including not only corporate networks but also individual e-mail accounts and employee PCs. The software is able to search through more than 200 different computer applications and recognize 30 different languages. Privacy advocates are worried. Attorney Gregg Williams says: "This could open a real Pandora's Box. There are some private things on office computers that you really don't want to know about." And Richard Smith of the Privacy Foundation says the software is "really dangerous" and warns that it "would hurt both companies and their employees by damaging morale." But Dana Gardner of the Aberdeen Group has little use for such concerns: "For every person that gets a little embarrassed because some personal information gets passed around the office, there are going to be more people who are able to find important information that helps them close a sale with an important customer or build a better mousetrap." (AP/Washington Post 12 Jun 2001)
http://washingtonpost.com/wp-dyn/business/latestap/A54075-2001Jun12.html

---

Category 34.2 *Usage monitoring, audit trails (employees, children)*

2001-12-11 **Internet instand-messaging chat monitoring logging audit trail parental supervision children**

NewsScan

NEW SOFTWARE SPIES ON INSTANT MESSAGING
New software from Ascentive Inc. enables parents to record their children's instant-messaging chats just like a VCR records a television program, allowing the PC owner to view frequent screen shots of actual conversations and to search and view IM logs for certain words. ChatWatch, a feature included in Ascentive's BeAware PC monitoring software, is more effective than filtering, says Ascentive CEO Adam Schram: "Filters give you too many false positives and negatives -- they block breast-cancer sites but not all porn sites." Instant messaging has soared in popularity over the past few years, with IM use up 34% at work and 28% at home this year. (Wall Street Journal 11 Dec 2001)
http://interactive.wsj.com/articles/SB1008016926590752280.htm (sub req'd)

Category 34.2 *Usage monitoring, audit trails (employees, children)*

2002-02-17 **surveillance technology spyware logging audit trail employee privacy keystroke logging pornography appropriate use policy**

NewsScan

THE CASE OF THE HORRIFIED SPY
The man who conceived and wrote the software thinks of himself as a privacy lover and says that what his program does is "horrifying": "Every time I add a feature into it, usually it's something that I've fought for a long time." But he's sold more than 200,000 copies of his $99 downloadable Investigator software, which can read every e-mail message, instant message and document someone sends and receives, and will take pictures from a Web cam, save screen shots, and read keystrokes in numerous languages. The program is hidden on the target's computer, as are the files containing the information it gathers. Ari Schwartz of the Center for Democracy and Technology concedes that the surveillance technology is a valuable tool in fighting fraud or child pornography, but thinks that companies need to resist using it too readily because "we think morally there are some very large issues" raised when employers track the personal habits of their workers. (AP/San Jose Mercury News 17 Feb 2002)
http://www.siliconvalley.com/mld/siliconvalley/2693278.htm

Category 34.2 *Usage monitoring, audit trails (employees, children)*

2002-04-12 **privacy monitoring corporate policy instant messaging**

NewsScan

COMPANIES START TRACKING WORKERS' INSTANT MESSAGES
Employees have known for several years that their bosses are keeping an eye on their telephone and e-mail habits, but new technology now makes it possible to monitor instant messaging exchanges as well. Privacy advocates say they know of no major instances where employees have been disciplined for IM abuse, but that it's probably just a matter of time. As of last year, only 20% of all IM accounts belonged to business users, but that percentage is expected to rise to 50% by 2004, according to the Radicati Group. Meanwhile, some companies have reported more diligent workers after they installed e-mail monitoring software on their corporate systems. "It changed the employee behavior. Their productivity went up," says one marketing director. "They were a little bit more careful with their communication. It will be the same with IM," she predicts. (AP 12 Apr 2002)
http://apnews.excite.com/article/20020412/D7IRHP780.html

Category 34.2 *Usage monitoring, audit trails (employees, children)*

2002-11-11 **software piracy copyright infringement usage monitoring peer-to-peer P2P**

NewsScan

COLLEGES URGED NOT TO MONITOR PEER-TO-PEER SHARING
The Electronic Privacy Information Center (EPIC), a Washington-based nonprofit organization that promotes freedom of speech on the Internet, is attacking letters recently written by the recording industry asking college officials to monitor Web use at their institutions for copyright violations made through peer-to-peer sharing of music or video files by members of the academic community. EPIC is criticizing those letters for trying to shift the burden of content enforcement to academic institutions which have scarce resources for such purposes, and is warning against a network "arms race" between file sharers and copyright enforcers. The group thinks colleges should avoid adopting a "confrontational role with respect to these technologies," because all it would do would be to harm the network's overall performance. (IDG News Service 11 Nov 2002)
http://www.idg.com.hk/cw/readstory.asp?aid=20021111002

Category 34.2 *Usage monitoring, audit trails (employees, children)*

2002-12-10 **surfer content filtering work appropriate use wasting time**

NewsScan

SURFERS: WHAT COULD THEY BE THINKING?
A study by Aaron Schatz has found that the top ten search terms used on Lycos Net this year have been: 1, Dragonball (the Japanese cartoon); 2, Kazaa (the music and video file-swapping service); 3, tattoos (that's right — tattoos); 4, Britney Spears, the pop singer who, oops, did it again; 5, Morpheus (file-swapping); 6, NFL, the National Football League; 7, IRS; 8, Halloween; 9, Christmas; and 10, Pamela Anderson, the actress and, uh, celebrity icon. Schatz says, "No matter how the news ebbs and flows, people still use the Internet for entertainment." So we see. There just doesn't appear to be that big a demand for information on the origins of the First World War. (USA Today 10 Dec 2002)

Category 34.2 *Usage monitoring, audit trails (employees, children)*

2002-12-17 **forensic investigation employee background**

NewsScan

COMPUTER FORENSICS TARGETS DISGRUNTLED EMPLOYEES

"There's a growing acknowledgment among executives that insiders can do more damage than the smartest outside hacker," says a Manhattan systems administrator. With that in mind, computer forensics software is targeting employee habits and behavior in an effort to stop corporate crime before it happens. Products like Savvydata's RedAlert collect, consolidate and analyze employee information to determine an individual's threat to the organization, based on what files employees accessed, the contents of their e-mails, and which company policies they violated. That information can then be combined with RedAlert's subscription-based Intelligent Information Dossier service, which allows corporate IT folks to research workers' criminal histories, credit information, financial asset details, friends and associates. Some IT workers think RedAlert goes too far: "RedAlert totally freaked me out," says a systems administrator for a Wall Street firm. "I understand why you'd need something like this if you are the CIA, but for standard biz use? I just don't think I'd work at a company that used these sorts of tools." Meanwhile, other products such as EnCase Enterprise Edition scour the network to see if any workers possess "unauthorized information" in order to prevent problems such as fraud, future lawsuits and other issues. (Wired.com 13 Dec 2002)

Category 34.2 *Usage monitoring, audit trails (employees, children)*

2003-01-21 **employee monitoring data theft prevention privacy simulations**

NewsScan

NEW WAY TO FOIL DATA THIEVES
Researchers at the State University of New York at Buffalo are developing software that tracks and analyzes how each computer user performs his or her routine tasks, such as opening files, sending e-mail or searching archives, to create individual profiles. The "user-level anomaly detection" software then alerts network administrators if a worker's behavior deviates from his or her profile so that they can monitor that employee's activities more aggressively. "The ultimate goal is to detect intrusions or violations occurring on the fly," says head researcher Shambhu Upadhyaya. "There are systems that try to do this in real time, but the problem is it results in too many false alarms." Some rival computer-security products also feature user profiling, but it's based on huge amounts of data flowing through entire networks. Upadhyaya says such detection systems are usually 60% to 80% reliable, whereas simulation tests indicate the new software would be up to 94% accurate. One information specialist says, "Other intrusion techniques require something like looking at audit logs after the damage has already occurred. The advantages offered by this approach is an intruder with malicious intent can be identified very early and a system operator can contain the damage, repair it in real time and shut out the intruder. This means that systems that have been attacked by an intruder maliciously might not necessarily be brought down." (Wired.com 20 Jan 2003)

Category 34.2 *Usage monitoring, audit trails (employees, children)*

2003-02-20 **content filtering monitoring university college student network bandwidth file-swapping P2P peer-to-peer copyright intellectual property infringement violation piracy**

NewsScan

TECHNOLOGY TARGETS P2P PIRATES
A new technology, provided by Audible Magic, has been tracking file-swapping traffic on the University of Wyoming's network for the past several months, quietly noting every trade of an Avril Lavigne song or a "Friends" episode. The technology isn't yet blocking file trades, but that could come next, say university administrators who complain their networks are sometimes overwhelmed with file-swapping activity. "I don't really want to be looking that closely at what people are doing, and you'd probably just as soon not have me looking either," says a University of Wyoming network specialist who's helping to manage the Audible Magic project. "But it's getting to be the only way to control our bandwidth." Audible's technology goes beyond the conventional port-blocking and digital rights management efforts now used to control file-swapping. It allows a network operator to see exactly what files are being transferred by creating a copy of all the traffic flowing on a network, identifying those bits that are using FTP (file transfer protocol) or Gnutella technology, and then re-creating those files to identify them. The resulting reports give university network administrators a good look at what students are trading and in what quantities, and future steps could include selectively blocking such trades. "We believe that what this does is transform network devices to be content-intelligent," says Audible CEO Vance Ikezoye. "That will be important. You can't just say, 'Let's block peer-to-peer.'" (CNet News.com 20 Feb 2003)
http://news.com.com/2100-1023-985027.html

Category 34.2 *Usage monitoring, audit trails (employees, children)*

2003-04-08 **computers monitor work habits Queen's University**

NewsScan

COMPUTERS TO WATCH YOU WHILE YOU WORK
With today's computer users increasingly overloaded by a combination of e-mail, instant messages and phone calls, researchers at the Human Media Lab at Queen's University in Ontario are designing technology that will enable a PC to gauge their user's attention level and sort out which messages and phone calls are important. "Today's digital lifestyle has the unfortunate side effect of bombarding people with messages from many devices all the time, regardless of whether they're willing, or able, to respond," says Human Media Lab director Dr. Roel Vertegaal. "We now need computers that sense when we are busy, when we are available for interruption, and know when to wait their turn — just as we do with human-to-human interaction." Techniques used to evaluate PC users' availability include an eye contact sensor that enables the PC to determine whether the user is present and whether he or she is looking at the screen. (BBC News 8 Apr 2003)

Category 34.2 *Usage monitoring, audit trails (employees, children)*

2003-06-17 **big brother company monitoring e-mail employees**

NewsScan

BIG BROTHER AT THE OFFICE
More than three out of four of the nation's largest companies monitor employee e-mails, Internet connections and computer files, because bosses are worried that their employees, instead of working, will use the Internet for pornography, online shopping, or Internet gambling. George Walls, a union president in Milwaukee, says that companies "are far more aggressive than they ever have been in the past. Virtually every minute of every day they can tell what you are doing. With all the monitoring, it is turning into an electronic sweatshop." Lisa Ellington, a call center worker, finds the situation "kind of insulting," and explains: "I am a good employee and don't have any reason to be stressed out by this. But it is human nature. You tense up. I pay bills, buy children's school clothes or order flowers. I know a lot of people did Christmas shopping. It gives you time to multitask and take care of things." (Milwaukee Journal Sentinenal/SJMN 17 Jun 2003)

Category 34.2 *Usage monitoring, audit trails (employees, children)*

2005-01-25 **privacy remote keylogger monitoring surveillance workplace forensic evidence data archives pornography appropriate use**

NewsScan; http://news.bbc.co.uk/1/hi/technology/4188747.stm

SOFTWARE WATCHES WHILE YOU WORK

Security firm 3ami and storage specialist BridgeHead Software have teamed up to create a network security system that can log computer keystroke activity, store it and retrieve the files within minutes. The developers say the system represents a breakthrough in the way data is monitored and stored, but privacy advocates worry that such monitoring not only is overly intrusive but can be damaging to employees' morale. However, 3ami managing director Tim Ellsmore counters: "That is not the case. It is not about replacing dialogue but there are issues that you can talk through but you still need proof. People need to recognize that you are using a PC as a representative of a company and that employers have a legal requirement to store data." The software was developed in response to the Freedom of Information Act's requirement for companies to store all data for a specified period of time, and is designed to monitor the downloading of pornography, the use of inappropriate language and the copying of applications for personal use. It also potentially could enable employers to track stolen files and identify whether they'd been e-mailed to a third party, copied, printed, deleted or saved to a CD, floppy disk, memory stick or flash card. (BBC News 25 Jan 2005)

Category 34.2 *Usage monitoring, audit trails (employees, children)*

2005-08-09 **computer tampering policy violation student punishment school lawsuit litigation Pennsylvania**

EDUPAGE; http://www.wired.com/news/technology/0,1282,68480,00.html8/

STUDENTS FACE PUNISHMENT FOR COMPUTER TAMPERING

Thirteen high school students in the Kutztown Area School District in Pennsylvania face felony charges of tampering with computers after defeating security measures on laptops issued to them by the school district. The laptops included Internet filters and an application that allowed district administrators to see what students did with the computers. The 13 used administrator passwords--which, for unknown reasons, were taped to the backs of the computers--to override the filters and download software such as iChat that the district policy forbids. The students also modified the monitoring program so that they could see what the administrators did with their computers. The students and their parents argued that the felony charges are unwarranted, but, according to the district, students and parents signed acceptable use policies that clearly state what activities are not allowed and that warn of legal consequences if the policy is violated. The students continued to violate district policies for use of the computers even after detentions, suspensions, and other punishments, according to the district. Only then did school officials contact the police. Wired News, 9 August 2005

---

35 DNS conflicts, trademark violations (Net, Web)

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1997-02-12 **Internet DNS domain names**

AP

In February, the International Ad Hoc Committee proposed seven new top-level domains:
.store — businesses offering goods,
.info — information services
.nom — personal sites
.firm — businesses or firms
.web — entities emphasizing the World Wide Web
.arts — cultural groups
.rec — recreational or entertainment activities.

These proposals were greeted with expressions of horror and outrage by members of the Association for Interactive Media and the Open Internet Congress, whose heated press release termed the proposals "an attempted takeover." In a Question and Answer section, the opponents of the IAHC write, "The Internet is likely to break apart on October 15, 1997. That is the date that the coup leaders intend to re-route the Internet to be under their control against the advice of those who keep things running smoothly today. When they rip the essential root servers off the Internet backbone, the entire system may begin to fragment. Your email will be returned and your Web site visitors will be turned away. These organizations have refused to recognize the validity of the registries that ensure that traffic is successfully delivered to .com, .org, and .net addresses. Serious concern has arisen over the possibility of malicious viruses and Trojan Horses being hidden in the software that runs the Internet."

See <http://www.interactivehq.org/oic> for details.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1997-02-20 **Internet DNS domain names**

PA News

Organizations who fail to register domain names that are appropriate for them may be losers on the Net, according to Giles Turnbull of PA News. For example, www.smarties.com has nothing to do with the popular multicolored candy; instead, it posts pornography. Experts urge

---

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1997-02-27 **Internet domain hijackings DNS**

Reuters

As companies recognize the value of the Net, newcomers are finding that their names have been hijacked by speculators who registered obvious domain names in the hope of selling them back to the legitimate users at a high price. Some victims are going to court, charging trademark infringement. Others are paying fees of up to $150,000 to gain control of domain names that they feel they need for their business.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1997-04-20 **Internet DNS domain names**

EDUPAGE

Network Solutions, Inc. proposed that the FCC temporarily take over registration of top-level domain names in the DNS until a world-wide system can be agreed upon. A few days later the National Science Foundation announced that it is washing its hands of the whole DNS mess and wants the Internet community to manage domain naming any damn way it wants to. In July, reports surfaced that the U.S. Department of Justice was investigating Network Solution Inc. for possible antitrust violations in its monopoly control of the DNS.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1997-05-04 **Internet DNS domain names**

EDUPAGE

Fifty-seven companies signed the DNS management proposals put forth by the International Ad Hoc Committee to define seven new domain names and define 28 new DNS registrars. In addition, 23 other companies indicated their intention to sign. However, unless the agreement is universal, it may lead to confusion in the DNS with disastrous consequences for the Internet.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1997-05-15 **DNS QA Internet domain names**

RISKS 19 15

The Association for Computing Machinery may have forgotten to pay its DNS renewal of $50, or maybe the InterNIC fouled up; but in any case, for a brief period in May the ACM was out of reach of Internet e-mail.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1997-06-03 **Internet trademark**

EDUPAGE

Honors Technologies Inc. of Reston, VA, runs automatic teller machines for about 450 financial institutions. In 1990, it was called Internet, Inc. and registered the word "Internet" as a trademark in the U.S. Now Honors Technology executives are upset by the widespread use of the word "Internet" in banking and has sent lawyers' letters to other companies warning them to stop using that word. The Internet Society protests the whole idea that "Internet" is a valid trademark and wants the registration rescinded.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1997-06-03 **trademark DNS Internet domain names conflict**

EDUPAGE

Microsoft lawyers are huffing and puffing over the registration of a dozen and more DNS entries such as "microsoftnetwork.com" by a college student in California. According to Microsoft, he "is clearly involved in copyright infringement, trademark infringement and unfair trade practices. We will try to contact him and request him to stop. Failing that, we'll send a cease-and-desist letter requesting he stop infringing upon our name."

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1997-06-05 **Internet DNS domain names speculation parasites extortion**

EDUPAGE

Speculation on Internet domain names increased with the announcement of plans to extend the range of top-level domains. One speculator claims to have received 1,800 pre-registrations of specific names at $15 a pop, with $35 more due if he actually gets the name for his anxious clients. In Houston, a company is claimed to have paid $150,000 to buy the rights to "business.com" from the British firm that registered it four years before.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1997-07-08 **Internet DNS domain names speculation parasites extortion**

OTC

William Dutcher reported on the growing traffic in reserved Internet domain names in an article in July. It seems that many larger firms are paying good money to gain control of domain names they want; prices range from a few thousand dollars to a million dollars for "billgates.com". Some speculators have been registering thousands of likely domain names hoping to find victims who will pay for their reserved names. It's difficult to find any redeeming social value in such practices, any more than in the actions of ticket scalpers. These people are equivalent to parasites, taking advantage of an economic niche and exploiting others for no benefit to anyone except themselves.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1997-07-14 **trademark DNS Internet domain names conflict**

OTC

NASA and the FTC both complained to Network Solutions Inc. about the sites "nasa.com" which, they allege, is a violation of The National Aeronautics and Space Act of 1958. This Act, "as amended, clearly prohibits the knowing use of the letters 'NASA' in connection with a product or service 'in a manner reasonably calculated to convey the impression that such product or service has the authorization, support, sponsorship, or endorsement of [NASA]. . . ." when such authorization etc. do not exist. However, some legal experts doubted that the Act would apply to the "nasa.com" site, which included a picture of boxer Evander Holyfield's ear and pointed to a pornographic site but could not be construed as being approved by NASA. Network Solutions responded to the legal pressure by removing the site's DNS entry.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1997-07-17 **Internet DNS domain names corruption hacking diddling**

EDUPAGE

After a competitor of Network Solutions deliberately introduced fraudulent entries into the DNS, corruption spread rapidly throughout the world to other DNS servers. Many addresses in the .com and .net domains were unreachable as a result of the hack and users found their e-mail undeliverable and their Web sites unreachable.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1997-07-25 **Internet DNS domain names corruption hacking diddling**

Inter@ctive Week Online

Eugene Kashpureff filed fraudulent information with InterNIC for its DNS updates in July, forcing domain name servers around the globe to recognize temporary and unauthorized Internet addresses ending in .xxx, .mall, .nic and .per. A few weeks later, he inserted false information that forced people trying to access the Web site of Network Solutions Inc. to end up at Kashpureff's Alternic site. Alternic is fighting NSI's monopoly over the .com, .net, .edu, .gov and .org domains. Kashpureff faced civil suits from NSI for damages and may face criminal charges of computer trespass.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1997-07-29 **Internet DNS domain names law**

Reuters

At the end of July, the Information Technology Association of America brought together parties interested in the Domain Name System to resolve conflicts over expansion of top-level domains. With termination in March 1998 of Network Solutions Inc.'s monopoly on .com, .edu, .net and .org, efforts to control the DNS increased in sharpness and urgency.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1997-08-03 **trademark DNS Internet domain names conflict**

EDUPAGE

In yet another conflict over scarce domain names, an American firm — Prince Sports Group — is protesting the allocation of "prince.com" to a British firm — Prince Plc. A British court refused the US company's plea, but the companies are now in litigation in the USA.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1997-08-11 **DNS spoof fraud vulnerability**

WebWeek http://www.webweek.com:80/current/infrastructure/19970811-secure.html

Two weeks after Eugene Kashpureff contaminated the DNS by inserting fraudulent pointers to his own AlterNIC site, he claimed to be working with victim Network Solutions Inc. to improve DNS server software to prevent future similar attacks, which may have succeeded because of free access to a "helpful hints" field that can trick a server into associating a requested address with some other, unauthorized address on the Net. The IETF continued its work on a news secure a DNS which would include encrypted authentication for all DNS server updates, including controls over the "helpful hints" field. In November, Kashpureff was arrested by Canadian Immigration officials and handed over to the FBI on a warrant for violations of computer crime statutes.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1997-08-26 **Internet DNS domain names InterNIC availability integrity QA**

RISKS 19 34

When the InterNIC, run by Network Solutions Inc. (Herndon, VA) lost the $50 payment for renewal of a customer's DNS entry, the consequences were unusually public: NASDAQ was off the net for segveral hours on 19 Aug 97.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1997-10-03 **Internet DNS domain names law**

Wired

In response to the efforts by the Geneva-based International Ad Hoc Committee to rationalize top-level domains in the Internet, US House members began considering legislation to force all registration entities to be located in the USA. "American taxpayers, companies, and government built the Internet," said Rep. Chip Pickering (R-Mississippi), chairman of the House Science subcommittee on Basic Research. Speaking at the second domain-name hearing, he said, "This is something uniquely American."

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1997-10-16 **trademark DNS Internet domain names conflict**

EDUPAGE

In Britain, several firms joined in a court case demanding that cybersquatters One In A Million Ltd stop using Internet domain names that violate their trademarks.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1998-02-01 **DNS domain name system law regulation**

EDUPAGE

The Clinton Administration announced a Green Paper outlining how the US government proposes to regulate the DNS. A new non-profit, private corporation would be set up by the end of September 1998 and would regulate registration of domain names. European ISPs and government agencies expressed dismay over private ownership of the high-level domains. In April, the White House announced plans for coordination with the European Union over governance of the Internet.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1998-02-10 **DNS domain name system fraud impersonation**

EDUPAGE

The Educom consortium offered to take responsibility for allocating addresses in the .edu top-level domain when Network Solutions' contract expires in March 1998. The consortium expressed concern about the currently unregulated state of .edu registrations, with fraudulent operations tricking victims by using the spurious credibility of such a domain name.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1998-02-10 **DNS domain name system pornography**

EDUPAGE

The Clinton Administration expressed dismay that a pornographer has registered whitehouse.com and is using that domain name to host a pornographic Web site. The Presidential attorney, Charles F. C. Ruff, wrote, "However distasteful your business may be, we do not challenge your right to pursue it or to exercise your First Amendment rights, but we do challenge your right to use the White House, the president, and the first lady as a marketing device... As your own online disclaimer implicitly acknowledges, the foreseeable result of your use of the White House domain name is that children will access your Web site inadvertently. Your customers will understand such a result is unconscionable, and so, we submit, should you." The pornographer sneered that the government has no trademark on "white house" or related words. [The Lewinsky affair and the Starr report rendered the White House complaints about pornography problematical.]

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1998-03-24 **Internet DNS jurisdiction regulation US government Europe**

EDUPAGE

At the end of March, the Internet Council of Engineers, based in Geneva, filed formal criticism of the US government's proposed regulation of the DNS. In a related development, a US district court judge ruled that all of the funds collected by the InterNIC under the $30 "Intellectual Infrastructure Fee" program had been received illegally. The $45M fund would have been used in part to fund the Next Generation Internet project; however, a group called the American Internet Registrants Association filed suit for class-action status to demand return of all that money to Internet domain-name holders. The action was dismissed in court at the beginning of September.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1998-04-21 **DNS conflicts law court case judgment**

EDUPAGE

In San Francisco, a federal appeals court rejected the view that Internet domain names were not covered by trademark law. The ruling supported the view that it is illegal to use someone else's trademark as an Internet domain name in an attempt to extort payment for giving it back. Score one for the good guys.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1998-06-28 **trademark infringement lawsuit**

EDUPAGE

SyNet sued Microsoft over SyNet's trademark of "Internet Explorer." Curiously, Microsoft lawyers claimed that this name was generic, like "coke." It would be interesting to know how those same lawyers would react if some other company began marketing a Web browser called, say, "Thingummy Corporation's Internet Explorer." In any case, Microsoft settled the lawsuit at the beginning of July — for a cool $5M. 'Course, that's pocket change to Microsoft. Now, does anyone know who owns the name for those neat glass things that cover holes in the wall?

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1998-07-09 **DNS domain name system Europe**

EDUPAGE

European plans for a concerted response to US plans for control of the domain name system collapsed in Brussels in early July.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1998-07-21 **DNS domain name system registrars CORE US**

EDUPAGE

A new group, the Internet Council of Registrars, or CORE, reported in July that it had already registered 40 applications from around the world for new domain names.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1998-08-27 **DNS corruption cache authentication domain name system**

EDUPAGE

DARPA has contracted with Network Associates (working with the Internet Software Consortium) to prevent further recurrence of last year's corruption of the DNS. The plan is to provide cryptographically-strong authentication that would prevent imposters from modifying data in DNS data caches.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1998-10-01 **DNS Internet domain name system US government**

EDUPAGE

Despite its deadline of the end of September, the US government delayed termination of its contract with Network Solutions Inc to control the domain name system. The date of handover to a private corporation, Internet Corporation for Assigned Names and Numbers (ICANN) was pushed back a week. In early October, Network Solutions and the Administration agreed that NS would continue to manage .com addresses until the new non-profit organization was ready to take over. Then in late October, the Commerce Dept. flip-flopped and announced that ICANN was not, in fact, the definitive choice of the Administration.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1999-01-05 **DNS spoofing interception Web site e-mail vulnerability**

PR Newswire

Men & Mice, an Icelandic software developer <http://www.menandmice.com/>, warned of a serious vulnerability of many sites on the Internet. Using their DNS Expert analysis tool, they found that one-third of all the sites on the Internet were vulnerable to DNS spoofing. Using known vulnerabilities, criminals can send e-mail purporting to come from the victimized site, causing potential embarrassment and even legal liability in cases of mail-bombing attacks or widespread spam. Even worse, it would be possible to corrupt DNS tables to redirect connections to pirate sites; one scenario sketched out by the DNS expert Cricket Liu (of Acme Byte and Wire) ran as follows: "To picture the potential damage, envision visiting your bank's web site to transfer funds from one account to another. Unfortunately, the web site seems to be having problems: After entering your account information and PIN, you still can't access your account data. The web site reports a 'temporary failure' and invites you to try again later. What you don't realize is that the web site you see is actually a near-exact replica of your bank's web site — startlingly easy to create — and that you've just sent your account number and PIN to hackers in another part of the world. Though you entered the correct URL, your local name server had been spoofed into believing that the bank's domain name corresponded to the address of a web server run by hackers." On their own Web site, the company posted extensive information about how to combat DNS spoofing. Acme Byte and Wire also posted Cricket Liu's presentation, "Securing Your Name Server" at <http://www.acmebw.com/securing/index.htm>.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1999-02-17 **trademark Web site copyright lawsuit DNS conflict squatters**

THE TIMES; Boston Globe

Jason Drummond, owner of VirtualInternet.net in England, helps companies protect themselves against cybersquatters who register domain names to take advantage of companies just getting started on the Net. Drummond was interviewed by John Kavanagh for The Times of London; he recommended that companies register as many variations on their trademarks as they can think of — with hyphens, underscores, abbreviations, acronyms, even likely misspellings. In another article, Jerry Ackerman wrote in the Boston Globe that some cybersquatters are getting rich on their claims; e.g., Compaq paid U$3.3M for the rights to <altavista.com>. Speculators also watch for mergers attentively. Ackerman wrote, "For example, six days before Exxon Corp. and Mobil Oil Corp. announced merger plans last Dec. 1, and continuing for a week afterward, five speculators - from Japan, South Korea, Singapore, Canada, and the United States - laid claim to 11 Internet addresses that joined the names of the two oil-industry giants."

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1999-02-17 **trademark infringement lawsuit lawyers attorneys Web sites DNS domain name system**

National Post (Canada)

The list of threats corporations attempting to defend what they see as their trademarks against Web sites using a variety of common names and words continued to grow in 1999. Simon Avery, writing in Canada's National Post, included the following cases:

* Playboy Enterprises Inc. and Estee Lauder Inc. sued Excite Inc. for infringing their trademarks in delivering URLs in response to searches by users.
* Archie Comic Book Publications threatened 23-month-old Veronica Sams because they claim that www.veronica.org violates their copyright on the name Veronica.
* Colgate-Palmolive sued the owners of Ajax.org because they were using the name of an ancient Greek hero — and scouring powder.
* Toys `R' Us sued Gus Lopez, owner of Toysrgus.
* Yahoo Inc. sued Yahooka, a guide to marijuana on the Internet.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1999-02-23 **cybersquatters DNS conflict trademark copyright domain name**

AP

In Houston, a federal court ruled in favor of Microsoft in a civil case against two cybersquatters who had registered eleven domains such as "microsoftwindows.com" and "microsoftoffice.com" as well as others such as "AirborneExpress.com", "AlamoRentaCar.com", "AssociatedPress.com" and "TravelersInsurance.com". Although the judge did not assign punitive damages, one of the defendants said through his lawyer that he was quitting the domain-name game.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1999-03-10 **DNS domain name system conflict adminstration**

Data Communications

In early March, the InterNIC of Network Solutions Inc. dropped thousands of entries from its domain name database, leaving those users bereft of their e-mail addresses and Web sites. Customers who were dropped were required to re-register for a fee. Some critics accused the firm of trying to get one last gasp of revenue before the ICANN (Internet Corporation for Assigned Names and Numbers) takes over in September 2000.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1999-04-20 **DNS domain name system allocation restriction licensing**

ZDNN

In April, Network Solutions Inc. lost its monopoly on domain name registration. ICANN, the Internet Corporation for Assigned Names and Numbers, announced five new registrars. The company agreed to make its database available to competitors. For a full of authorized registrars see <http://www.icann.org/registrars/accredited-list.html>.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1999-04-22 **Internet DNS domain name service fraud URL hijacking**

PR Newswire

Someone claiming to be a Portuguese resident called Carlos Pereira registered 25 domain names on the new .NU Domain Ltd domain name server in Britain. The perpetrator set up pornographic Web sites using .NU's quick-and-easy InstantWeb service and hijacked IP connections to legitimate Web sites. The .NU company revoked the perpetrator's accounts.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1999-04-23 **DNS domain name system ownership ISP conflict**

Network World Fusion http://www.nwfusion.com/news/1999/0423domain.html

One of the nastier side-effects of ICANN's monopoly busting decentralization of domain name registrations is that individual registrars could theoretically keep ownership of domain names they issue. Change registrar and you could find that someone else owns your trademarked domain. Such loss of control could be disastrous, forcing companies to change letterhead, business cards, and their entire Web sites. In addition, some ISPs are planning to offer domain-name services bundled into their contracts. Writing in Network World, Sandra Gittlen and Denise Pappalardo urged, "customers should check the fine print of their contracts to make sure that they retain rights to their
online brands if they switch ISPs."

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1999-05-03 **WIPO intellectual property DNS domain name squatters**

New York Times

In early May, the World Intellectual Property Organization (WIPO) of the United Nations proposed to ICANN (the Internet Corporation for Assigned Names and Numbers) that cybersquatting be outlawed. ICANN began evaluating the recommendations at a meeting in Berlin at the end of May.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1999-05-05 **DNS antitrust privacy database competition**

Washington Post

The DoJ began investigating the behavior of Network Solutions, Inc. (NSI), the firm which used to have a monopoly on Internet domain name registrations. The company refused to release their database of existing domains despite pressure from the National Science Foundation, which originally funded the company's operations. NSI also claimed that releasing its database might open the floodgates to junk e-mailers.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1999-05-10 **e-commerce Web Internet libel slander abuse complaints**

The Times (London)

Ian Brodie wrote an interesting article in _The Times_ (London, UK) summarizing some of the problems irritated consumers are causing businesses by creating critical Web sites that attract other people who are, depending on your perspective, angry victims of corporate greed or whining sore-heads who need to get a life. The canonical names for such sites include $1_sucks.com or $1_stinks.com, where $1 is the string variable representing some recognizable version of the exploiter/victim company. Some of the companies have responded with lawsuits; others with attempts to buy the offending DNS registration; and a few with cooperation and attention.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1999-05-24 **cybersquatters domain name registration DNS**

LA Times

A computer club in London, Pictureweb, managed to register 75,000 domain names between February and May 1999 through the ICANN-approved company "Register.com". Some of the club members registered thousands of names.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1999-06-28 **DNS domain name system registration conflict policy charges fees**

New York Times

In June, ICANN was forbidden by the US government to open its planned registration of Internet domain names to competition as several factions squabbled for control and oversight of the process. Critics didn't like ICANN's threat to cut Network Solutions Inc. (NSI) out of the registration business — especially since ICANN had no right to any such decision (it resides with the Dept of Commerce). Others questioned the new organization's right to levy a $1 annual fee on every registered domain.

In July, the test period for other companies offering to provide registration services was extended yet again, this time until 6 Aug 1999.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1999-07-16 **criminal hacker DNS domain name system**

Communications Week International

On 1999-07-01, criminal hackers hijacked Network Solutions Inc.'s Web sites (<networksolutions.com>, <netsol.com> and <thedotcompeople.com>) and rerouted would-be visitors to the CORE (Council of Internet Registrars) Web site — a competing domain-name system registrar. According to David Hotzman, NSI's CTO (Chief Technology Officer), someone made unauthorized template modifications of a host that changed the IP addresses of the NSI domain names. According to an article in _Communications Week International_, "The hack itself was a DNS modification spoof, whereby a person makes a modification to a domain name using NSI's public template interface, yet inserts data for a domain name owned by another party. NSI declined to comment on whether this was the first known attack of its kind, but said it has redesigned the system to protect against similar intrusions in the future."

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1999-07-20 **pornography DNS domain name system registration obscenity**

Washington Post

Network Solutions Inc decided that other registrars would not be limited by the FCC list of seven forbidden words (yes, you know what they are) in domain name registrations.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1999-07-30 **cybersquatting DNS domain name registration trademark infringement law legislation bill proposal**

Wall Street Journal http://interactive.wsj.com/articles/SB933300984173737383.htm

Orrin Hatch (R-UT) and others proposed a law to prevent people from using trademarked names belonging to others when establishing domain names for use on the Net. The bill provided for statutory damages and the right to appeal to the courts for seizure of the offending domain name.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1999-10-05 **DNS ICANN domain name system Web**

TBTF http://tbtf.com/archive/1999-10-05.html

ICANN, NSI and the Department of Commerce came to agreement in October over many elements of the new regime for naming Internet domains. According to Keith Dawson, editor of the always-useful TBTF newsletter (see < http://tbtf.com/archive/1999-10-05.html >), the key issues were as follows (direct quote from TBTF):
- NSI assents to ICANN's authority and agrees to sign a modified Registrar Agreement.
- Commerce takes over operation of the InterNIC.
- The fee NSI charges to competitive registrars drops from $9 to $6.
- NSI agrees in principle to a per-name fee to fund ICANN's operations, provided that NSI does not owe more than $2M under such a program. NSI hands over $1.5M to ICANN immediately.
- NSI continues to run the authoritative root server for at least four years. Even after its eventual transfer to ICANN, Commerce continues to assert policy authority to direct this server. [MK: I wonder what the EU thinks of this provision.]
- NSI must totally separate its registry and registrar functions-. If it accomplishes this within 18 months then it can hold onto the root server for an additional four years.
- NSI effectively gives up the claim that it owns the intellectual property represented by the .com/.org/.net database.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1999-10-13 **trademark infringement translation multilingual DNS domain name lawsuit**

Wired via PointCast News

Lawyers for WhatsHappenin.com sued quepasa.com for trademark infringement, claiming that the Spanish words were unacceptable because they constituted infringement, unfair competition and false advertising. Observers were watching the case with interest because its outcome could affect many sites whose names have the same meaning in various languages.

Category 35 *DNS conflicts, trademark violations (Net, Web)*

1999-10-26 **DNS hijacking search engines pornography criminal hacker**

Computer Currents 17 i20

Web hijacking can occur by copying legitimate Web sites, indexing them with search engines, then redirecting browsers to alternate — often pornographic — pages. The perpetrator can charge advertisers for all the unwilling hits on their sites. One villain who was shut down by the FTC even ran Java applets that disabled the "back" arrow in browsers and deleted the ability to close the browsers. People trapped in porno-hell had to reboot their computers to get out. Experts recommend that everyone keep an eye on the actual URL that appears in their browser window; any discrepancy between the visible URL and the actual URL should alert one to the possibility of fraud. In addition, consider running a personal firewall to block Java applets from unknown or untrustworthy sites.

35.1 Cybersquatting

Category 35.1 Cybersquatting

2000-01-21 **cybersquatting DNS trademark infringement**

NewsScan, San Jose Mercury News
http://www.sjmercury.com/svtech/news/breaking/ap/docs/115878l.htm

Filing suit under a federal anti-"cybersquatting" law passed last year, musician John Tesh, who has a Web site called tesh.com to offer "intelligence for the family," is suing the owners of johntesh.com, charging that their only purpose in registering the site was to trade on his own good name and resell their domain name for a profit. (AP/San Jose Mercury News 21 Jan 2000)

Category 35.1 Cybersquatting

2000-02-22 **trademark DNS domain name system conflict cybersquatting dispute arbitration**

NewsScan

[By mid-February,] Eighty-nine cases [had] been filed with the "cybersquatting" arbitration service run by the World Intellectual Property Organization (WIPO) since its inception in December, and the service has already handed down decisions in favor of the World Wrestling Federation, Stella D'oro Biscuit, and Telstra. Still pending are disputes over dior.org, easyjet.net, world cup2002.com, jpmorgan.org, microsoft.org, alaskaairlines.org and dodialfayed.com. The mandatory dispute resolution system has seen a jump in cases from one filed in December to 60 filed in February. Unless an arbitrated decision is challenged in court, domain name registrars are bound to implement it. (Financial Times 22 Feb 2000)

Category 35.1 Cybersquatting

2000-06-01 **domain name system DNS cybersquatting arbitration WIPO**

NewsScan, Wall Street Journal
http://interactive.wsj.com/articles/SB959810376180166493.htm

Actress Julia Roberts . . . won control of the Internet name www.juliaroberts.com, after an international arbitration panel ruled that an accused cybersquatter had no legitimate interest in that name and registered it in bad faith. The World Intellectual Property Organization, which is one of four designated arbitrators of Internet domain name disputes, cited evidence that the defendant, Russell Boyd, had registered names of several famous movie and sports celebrities, and had even tried to auction the Roberts address on eBay. In reaching its quick decision, the panel is demonstrating its willingness to extend protection to famous individuals, even if they haven't formally registered their names as trademarks. (Wall Street Journal 1 Jun 2000)

Category 35.1 Cybersquatting

2000-11-28 **censorship Web DNS domain name system lawsuit cybersquatting forgery judgement filtering**

NewsScan, Wired http://www.wired.com/news/business/0,1367,40380,00.html

A federal district court in San Jose ruled the. . . [sex.com] domain name must be returned to its original owner, from whom it was transferred six years ago through a forged letter. The successful plaintiff said that the ruling "shows that eventually the little guy an win at a great cost [$500,000]" and added: "I plan to do something not as sick-o as this guy [the defendant]." The judge ordered the defendant to put $25 million in escrow pending a determination of how much the plaintiff had been deprived by the misappropriation of the valuable name. . . . (Wired.com 28 Nov 2000)

Category 35.1 Cybersquatting

2000-12-13 **DNS domain name service trademark copyright conflict**

NewsScan, San Jose Mercury News
http://www.mercurycenter.com/svtech/news/breaking/ap/docs/743090l.htm

The Author's Guild has asked the Internet Corporation for Assigned Names and Numbers (ICANN) to require a British company called Old Barn Studios Ltd. to surrender ownership of domain names it created by appropriating the names of well-known authors, such as R.L. Stine, John Berendt, Charles Frazier, and Thomas L. Friedman. The Guild says: "For authors, whose names and reputations are their most valued stock-in-trade, bringing this proceeding was absolutely necessary. We hope to establish the precedent that in cyberspace, as in traditional venues of trade, authors' names belong to them, not to the first outfit that registers a famous name as a domain name." (AP/San Jose Mercury News 13 Dec 2000)

Category 35.1 *Cybersquatting*

2001-04-04 **cybersquatting lawsuit decision judgement penalty fine pornography**

NewsScan

SEX.COM THIEF MUST PAY $65 MILLION In a record verdict against a cyber-squatter, a federal judge in San Francisco awarded the original owner of the sex.com domain name $65 million for the five years' loss of use he suffered after the address was hijacked by fugitive Stephen Cohen, who now lives in Tijuana. "The number is big, but it is unlikely that I will ever see more than a small fraction," said plaintiff Gary Kremen. Meanwhile, Kremen's site has dropped the hard-core images placed by high-paying porn advertisers, and now uses a text-based dictionary that links to other sex sites by topic. "We have done what we said we were going to do -- reduce the amount of pornography on the site as we transition to more mainstream content," said Kremen. (Los Angeles Times 4 Apr 2001)
http://www.latimes.com/business/20010404/t000028664.html

Category 35.1 *Cybersquatting*

2001-06-04 **cybersquatting DNS domain name system entrepreneurs competition registration**

NewsScan

WHAT'S IN A NAME
When an Internet domain name is not renewed (whether intentionally or by accident), it goes back on the market, and some companies specialize in buying them up and reselling them for other purposes. Ray King of SnapNames says: "The bigger the company, the easier it is. They just lose track of it... Any good name that expires you, can be certain there will be at least a couple hundred people trying to get it." A short, clever name with a good search position at Yahoo is vulnerable to being recaptured for use as an "adult" site. (USA Today 4 Jun 2001)
http://www.usatoday.com/life/cyber/tech/2001-06-04-domain-name-woes.htm

---

Category 35.1 *Cybersquatting*

2001-10-26 **DNS domain name system registration maintenance pornographers cybersquatting**

NewsScan

HOW A KIDS SITE WAS TAKEN OVER BY PORNOGRAPHERS
A Web site offering a math-and-money game for children was turned into a porn site after an employee's departure left VeriSign unable to get paid for the renewal of the site's registration. With the fee unpaid, the domain name was sold to a pornographer, because "they felt we weren't paying our invoices. But we weren't getting any because of confusion over the contact information." The game is now offered at Moneyopolis.com. (New York Times 26 Oct 2001)
http://partners.nytimes.com/2001/10/26/technology/26NET.html

Category 35.1 *Cybersquatting*

2001-11-13 **DNS domain name system cybersquatting extortion pornography**

RISKS 21 76

Malcolm Pack, writing in RISKS, gave a startling explanation of why so many sites have been converted to pornographic content. He suggests, ". . .[The] presence of pr0n on the 'hijacked' site is a blackmail tool, which would explain why so many domain names obviously targeted at children become (apparently inexplicably) pr0n sites. I'd never thought of pr0n as a weapon. . . ."

[Mr Pack uses "pr0n" as a substitute for "porn" presumably to avoid triggering e-mail content filters.]

Dan Fandrich confirmed that extortionists are indeed buying expired domain names and installing porn in order to embarrass former domain owners and extort high repurchase prices. He wrote, ". . . [P]ornographers bought up close to 2000 expired domains . . ., including domains owned by respectable organizations with hundreds of inbound links, such as the TCL Consortium, XIII International AIDS Conference, Evian, Universal ADSL Working Group, and Craig's List. I tracked down the original owners of about 60 of these sites with the most inbound links and warned them of the problem . . . . Five months later, only three of those 60 sites have done anything about their former domains, either buying them back from the extortioners or getting links changed to their new sites."

Mr Fandrich offers some thoughtful advice to anyone thinking about letting a domain name registration lapse: "Some of the former owners I talked to seem to have trouble seeing that their web sites did not stand in isolation, that people outside their organization had links to their web site and others had bookmarks and those links attached to their names were now serving up porn. I got responses to the effect of «We have a new domain name now, so we don't care what happens to the old one.» One certainly takes a RISK in letting one's domain name expire, but when the gamble fails and what must be about the worst case scenario occurs, the indifference I've seen surprised me. I find it hard to believe that so many people have so little respect for their viewers and customers."

Category 35.1 *Cybersquatting*

2002-02-15 **cybersquatting dishonesty Web hijacking political propaganda trickery**

NewsScan

LYING FOR TRUTH

Some unknown person or group has created a Web site called www.reedcollegis.com intended to fool people looking for Reed College (www.reed.edu) and send them an anti-abortion site called www.abortionismurder.com. Reed College chief technology officer Martin H. Ringle says, "We've paid for 'reed.com' and 'reed.org,' and so on, in an effort to pre-empt cybersquatting. But it's impossible to imagine every variation of the name and how it could be used -- although in hindsight, reedcollegis.com was an obvious one." The site abortionismurder.com is maintained by a Florida man, Thomas P.A. Fitch, who denies involvement with or knowledge of the creation of reedcollegis.com, but does admit to owning an address similar to that of the College Board. His aim is to attract college applicants to his anti-abortion site to expose "to the truth" students who are "going to run this country in fifteen years... I'd say our tactics are not dishonest. They're creative, they're on the edge, they're bold. Thank you for the publicity because it's only helping our cause." Sheldon E. Steinbach of the American Council on Education says of use of the name reedcollegis.com to divert unsuspecting surfers from their intended goal: "This is the first instance, to my knowledge, that a university or college name has been hijacked for seemingly a political purpose." (Chronicle of Higher Education 15 Feb 2002) http://chronicle.com/free/2002/02/2002021501t.htm

---

Category 35.1 *Cybersquatting*

2002-05-27 **DNS Domain Name System hijacking pornography**

RISKS 22 10ff

Geoffrey Bent noted in RISKS:

When the US Navy forgot to renew registration on NavyDallas.com - apparently because Network Solutions forgot to send them a renewal notice - it was snapped up by a pornography site. NSI accepted the new registration despite the new owner being identified simply as "Bog". Meanwhile, NavyBoston.com now directs users to an eBay auction site:

http://www.newsbytes.com/news/02/176741.html

Category 35.1 *Cybersquatting*

2002-05-28 **fraud scam URL DNS domain name system misspellings pornography theft investigation pursuit mouse-trapping HTML cybersquatting**

FindLaw Download This; http://news.findlaw.com/ap/ht/1700/5-24-2002/20020524120012_14.html 87

INTERNET SCAM ARTIST FINED $1.9M

In May 2002, John Zuccarini of Andalusia, Pa., was ordered to pay $1.9 million in restitution to victims of his URL-misspelling scam, in which he registered more than 5,500 Web sites with names similar to celebrities and popular organizations such as the Backstreet Boys, Bank of America, Victoria's Secret, and The Wall Street Journal. In particular, Zuccarini registered 15 variations on the name of the Cartoon Network site and 41 versions of Britney Spears' name. The scam worked by forcing accidental visitors into click-through advertisements and disabling their ability to leave the site; sometimes the back and close buttons were inoperative. Another deceptive technique involved a "stealth page" concealed under the task bar, usually at the bottom of the screen. This window activated a timer that popped up yet more ad windows at the beleaguered viewer.

Money came from advertisers who were also being cheated, since most of the clickthroughs were in fact from unwilling victims of the scam. By October 2001, Zuccarini had already been sued by 63 groups in the two years and lost 53 times. He had been subjected to 56 arbitration proceedings and lost rights to about 200 of his misspelled domains, yet he continued to rack up profits using his schemes. The US Federal Trade Commission (FTC) filed a complaint against Zuccarini, "doing business as The Country Walk, JZDesign, RaveClub Berlin, and more than 22 names incorporating the word "Cupcake," including Cupcake Party, Cupcake-Party, Cupcake Parties, Cupcake Patrol, Cupcake Incident, and Cupcake Messenger." Unfortunately, Zuccarini remained at large despite attempts of law enforcement officials to locate him.

Category 35.1 *Cybersquatting*

2002-06-27 **cybersquatting intellectual property extortion domain name system DNS Domain Name System pornography gambling rules dispute registration**

NewsScan

ICANN PROPOSES RULES TO FIGHT CYBERSQUATTING
The Internet Corporation for Assigned Names and Numbers (ICANN) says it's close to adopting new procedures that would make it easier for individuals and businesses to avoid extortion by cybersquatters, and would establish a waiting list for coveted domains that become newly available to the public. The first measure would establish a 30-day grace period for domain name owners to renew their contracts -- a move intended to prevent speculators from swooping in and registering an expiring domain name before the owner has time to renew. "ICANN receives a large number of complaints for inadvertently deleted domains It affects churches, schools, businesses," says an ICANN spokesman. "We get a lot of complaints from people who wake up to find their domain has expired and now has porn on it, or it's linked to a casino site. Then, they'll ask for a ransom to get it back." The waiting-list proposal would allow a bidder to pay a fee to get first dibs on any newly available domain names. That proposal has run into opposition from registrars who say the $28 that VeriSign has proposed charging them for the service is too high. (Reuters/Wired 27 Jun 2002)
http://www.wired.com/news/politics/0,1283,53518,00.html

Category 35.1 *Cybersquatting*

2002-07-30 **cybersquatting DNS Domain Name System conflicts extortion**

NewsScan

WHAT WAS A DOT-COM LAND GRAB, DADDY?
Cybersquatting is virtually (no pun intended) a thing of the past -- and cyber "real estate" is definitely losing value. The number of dot-com, dot-net, and dot-org names has declined by more than 11% in the first five months of this year, and industry analysts are saying that the dot-com land grab is over. This is quite a change from those heady days, not so long ago, when desirable dot-com names could fetch hundreds of thousands of dollars from companies eager to project just the right image to customers. Now, companies like Johnson & Johnson are saying: "It's become clear that we've already registered as many domain names to protect our trademarks as we need. We haven't needed to buy any more this year." So what will cybersquatters do now? One knowledgeable observer of the scene says, "Speculation is gone. The days of hunting out a real business opportunity are here." Maybe the cybersquatters will actually get a real job. That would be nice. (Los Angeles Times 29 Jul 2002)

Category 35.1 *Cybersquatting*

2003-01-06 **DNS Domain Name System cybersquatting fraud theft lawsuit**

NewsScan

SEX.COM RULING COULD OPEN FLOODGATES ON REGISTRY LAWSUITS
A federal appeals court has asked California's Supreme Court to rule on whether Network Solutions Inc., the largest U.S. domain registry, must face a multimillion-dollar damage claim from the rightful owner of the sex.com domain name. The ruling could lead to a flood of lawsuits against domain registries, particularly NSI, from hundreds of people who claim their domain names were also stolen. The current case stems from a lawsuit filed in 1998 by Gary Kremen who registered the sex.com name with NSI in 1994. In October 1995, NSI received a letter purportedly from Kremen asking that the name be reregistered to a company headed by Stephen Cohen. NSI complied without attempting to verify the validity of the request, and then refused to undo the transfer when alerted to the fraud. Meanwhile Cohen, who was using the domain name for a lucrative porn business, fled the country before Kremen's lawsuit against him went to trial in 2001. Kremen, who is now using sex.com for his own porn business, was awarded $65 million in damages from Cohen for fraud (which he'll probably never collect) and is now requesting an additional $30 million from NSI for allowing the fraudulent transfer. (San Francisco Chronicle 4 Jan 2003)

Category 35.1 *Cybersquatting*

2003-02-11 **.gov domain hijacking government Access One Network Northwest AONN**

NIPC/DHS

GSA PULLS SUSPICIOUS .GOV SITE

The General Services Administration (GSA), which runs the .gov registry, pulled the plug on a .gov Web site pending an investigation into the authenticity of the organization that controlled it. Until January 24, the AONN.gov Web site contained information about an agency calling itself the Access One Network Northwest (AONN), a self-described cyberwarfare unit claiming to employ more than 2,000 people and had the support of the U.S. Department of Defense. No federal agency called AONN appears to exist, and no agency with that name is on the official list of organizations maintained by the U.S. National Institute of Standards and Technology. The action could point to the first case of a .gov domain name hijacking. Cybersquatting, or registering a domain to which you may not be entitled, is hardly uncommon among the multitude of .com and .net domains. But there are no known cybersquatting incidents involving a governmental domain, according to the GSA. Claiming credit for the deleted .gov site is a man who calls himself Robert L. Taylor III. Taylor declined to explain how or when he secured a .gov domain for the group, calling AONN's operations "classified." A Pentagon representative said that AONN has no affiliation with the U.S. military and he had no knowledge of the organization. According to the official .gov registration rules, only organizations that appear in an official list of government agencies qualify for a .gov domain—and AONN is not on it. Registering a .gov domain name involves writing an authorization letter, printing it out, and then sending it to the ".GOV Domain Manager" in Reston, Virginia.

Category 35.1 *Cybersquatting*

2003-06-13 **sex.com domain name ownership stephen cohen gary kremen**

NewsScan

S*X.COM RESTORED TO RIGHTFUL OWNER
The U.S. Supreme Court has rejected an appeal from cybersquatter Stephen Cohen, who had hijacked the lucrative s*x.com domain name from its original owner Gary Kremen, putting an end to six years of legal wrangling. The ruling, which upheld a lower court's award of $65 million in damages to Kremen, is viewed by legal experts as a landmark case because it holds domain registrar VeriSign accountable for allowing the ownership transfer to take place, based on a forged letter from Cohen. The case is also expected to set a precedent for treating an Internet address as legal property — a designation disputed by VeriSign, which could face fines of up to $200 million if found liable. Kremen now faces an uphill battle to claim his award, because Cohen is now a fugitive in Mexico. (BBC News 13 Jun 2003)

Category 35.1 *Cybersquatting*

2004-07-07 **DNS squatting Kerry Edwards Websie 2004 Presidential election race**

NewsScan

KERRY EDWARDS: THAT'S A FELLOW IN INDIANAPOLIS

Indianapolis native Kerry Edwards, a 34-year-old bail bondsman, owns the Kerryedwards.com domain, but is willing to sell the name -- for the right price. A Kerry spokesman says: "Our campaign did inquire about KerryEdwards.com, but because of the money they were asking for, we took a pass." Kerry Edwards wanted a five-figure payment. A number of other obvious choices for a campaign Web site (including KerryEdwards04.com, KerryEdwards2004.com, and KerryEdwards-2004.com) are already registered. (Washington Post 7 Jul 2004)

Category 35.1 *Cybersquatting*

2005-01-17 **denial of service DoS domain name system DNS hijacking fraud data integrity authorization**

RISKS; http://www.panix.net/hijack-faq.html 23 69

DON'T PANIX

The DNS entry for the Panix ISP was hijacked in January 2005. Cyrus R. Eyster reported to RISKS on the case and quoted the Panix Website:

Panix's main domain name, panix.com, was hijacked by parties unknown. The registration of the panix.com domain was moved to a company in Australia, the actual DNS records were moved to a company seemingly in the United Kingdom (but with servers in Canada and corporate registration in Delaware), and panix.com's mail was redirected to servers in Canada. None of the systems exploited to perform this hijacking were under Panix's control.

It's not supposed to be possible to transfer a domain name from one registrar to another without notifying both the current registrar and the current domain owner, but that's what seems to have happened.

As the hijacking occurred over the weekend, we had great trouble reaching responsible parties at the other companies involved. The domain was not returned to us until the beginning of the business day in Australia on Monday. None of the companies involved had support numbers that were available over the weekend, or even emergency contact numbers.

Category 35.1 *Cybersquatting*

2005-07-08 **Google Website domain misspelling typo cybersquatting case victory**

EDUPAGE;
http://today.reuters.com/business/newsArticle.aspx?storyID=nN78398318

GOOGLE WINS TYPOSQUATTING CASE

Google has the rights to several misspellings of its domain name, according to a decision by the National Arbitration Forum (NAF). Google had filed a complaint against Sergey Gridasov, a Russian man who had registered domain names of googkle.com, ghoogle.com, gfoogle.com and gooigle.com, saying that he was profiting from Google's name with the domains, which are common mistypings of google.com. Gridasov reportedly used the domains to redirect Web surfers to sites that would download various kinds of malware to their computers. Because Gridasov did not respond to the complaint, the NAF was compelled to accept the allegations in Google's complaint. According to the NAF, Gridasov is not entitled to use the domains, which are confusingly similar to Google's.
Reuters, 8 July 2005

Category 35.1 *Cybersquatting*

2005-07-18 **cyber squatting lawsuits BDC Capital Inc.**

EDUPAGE; http://www.detnews.com/2005/technology/0507/18/0tech-250797.htm

UNIVERSITY CHARGES CYBERSQUATTING

A Minnesota-based company has raised the ire of a number of colleges and universities after registering more than 23,000 URLs, many of which imply a connection to the schools that does not exist. BDC Capital Inc. has registered such URLs as www.universityofmichiganwolverines.com,
which is not affiliated with the University of Michigan at all, and www.uofmgophers.com, which has no connection with the University of Minnesota. Marvin Krislov, general counsel at the University of Michigan, which has sent the company a cease-and-desist order, called the URLs a "pretty clear violation of trademark," noting that reasonable people would likely assume a connection between the site and the institution. A spokesperson from BDC said the company does not believe it has violated any trademarks. He said the company believes that the URLs "represent a significant asset to both BDC and the schools," saying that BDC anticipates a "partnership" with the schools to sell souvenirs and other items. Detroit News, 18 July 2005

35.2 Trademarks vs DNS

Category 35.2 Trademarks vs DNS

2000-01-07 **Web DNS squatting trademark infringement lawsuit**

NewsScan, Reuters, San Jose Mercury News
http://www.sjmercury.com/svtech/news/breaking/merc/docs/000077.htm

Teen Magazine has filed a federal lawsuit charging the operators of pornographic Web site of violating "cybersquatting" laws when it created a pornographic Web site called teenmagazine.com. Teen Magazine's own Web site is called simply teenmag.com. Lynn Lehmkul, an executive of the company that owns the magazine, says, "This is just unconscionable. It would be irresponsible of us not to pursue this matter in every possible way. It has been pretty well documented that people who seek out pornographic sites on the Internet use 'teen' as a search word." (Reuters/San Jose Mercury News 7 Jan 2000)

Category 35.2 Trademarks vs DNS

2000-01-25 **DNS conflict lawsuit infringement art corporation judge trademark**

POLITECH http://slashdot.org/yro/99/12/01/2156208.shtml

In 1994, a group of European artists chose the DNS entry "etoy.com"; their Website went online in Oct 1995 and they proceeded to have fun for the next several years carrying out disrespectful creative acts such as hijacking Playboy pages using fraudulent metatags to get novice Web users onto the etoy.com Web site. The group continued in this jolly way until September 1999, when a company called eToys.com sued the etoy.com group for trademark infringement — even though eToys.com wasn't formed until June 1997 and did not reach the Web until October 1997. On Monday 29 Nov a (computer-illiterate?) judge granted the eToys corporation an injunction that forced etoy.com to shut down its Web site until the end of December 1999. In the intervening months, the unscrupulous business people saw the value of their stock go down thanks to a world-wide campaign of harassment against the litigious corporation, ably led by the (R)TM)ark organization. On 2000-01-25, eToys.com finally dropped its lawsuit.

Category 35.2 Trademarks vs DNS

2000-07-13 **cybersquatter trademark lawsuit domain name system DNS**

NewsScan

The International Olympic Committee, the U.S. Olympic Committee and the Salt Lake Organizing Committee . . . joined together in a lawsuit accusing some 1,800 Web sites of misusing the Olympic name. The suit represents the largest action by far brought under the recently enacted Anticybersquatting Consumer Protection Act. Previously, the largest named about 250 defendants. The IOC says about 50 of the sites have been turned over to the Olympic groups without further legal action. (AP/MSNBC 13 Jul 2000)

Category 35.2 Trademarks vs DNS

2000-10-16 **DNS trademark conflict lawsuit ruling judgement celebrity pornography**

NewsScan

Madonna . . . joined such celebrities as Julia Roberts and Isabelle Adjani in successfully suing a Web entrepreneur who created a site called madonna.com. The World Intellectual Property Organization found that the businessman, who used the site for sexually explicit material, "lacks rights or legitimate interests in the domain name" and that the name "had been registered and used in bad faith." (AP/MSNBC 16 Oct 2000)

Category 35.2 Trademarks vs DNS

2000-12-11 **DNS domain name system obscenity freedom speech lawsuit judgement ruling**

NewsScan, San Jose Mercury News
http://www.mercurycenter.com/svtech/news/breaking/merc/docs/026011.htm

A federal judge has ruled against plaintiffs who relied on First Amendment rights to incorporate obscene or vulgar words in the addresses of the "adult" Web sites. Arguing that Web names are not only to provide addresses but also to communicate the nature of the product, their attorney gave the example: "When you're looking for antiques, the first thing you would put in is antiques.com." (And when you're looking for ...) American Civil Liberties Union attorney agreed that domain names are "more than just signposts," but the position of University of Miami law professor Michael Froomkin is that the judge's ruling prevents individuals from arguing that domain names are simply words in the public domain, that can be used by anyone. (AP/San Jose Mercury News 11 Dec 2000)

Category 35.2 *Trademarks vs DNS*

2001-05-24 **DNS domain name system trademark infringement lawsuit**

NewsScan

UNIVERSITY SUES ADULT SITE FOR USING ITS TRADEMARK [24 May 2001]
The University of North Carolina has filed a $100,000 lawsuit against the adult Web site uncgirls.com, which is registered to Universal Nude College Girls Sites. The suit charges the owners of the site with misappropriating the university's trademark "UNC." A university official said, "We don't want our trademarks diluted, and we don't want the good name of the university to be smirched." In addition monetary damages, the suit demands that the domain name uncgirls.com be transferred to the university. (AP/USA Today 24 May 2001)
http://www.usatoday.com/life/cyber/tech/2001-05-24-unc-adult-site-suit.htm

---

Category 35.2 *Trademarks vs DNS*

2001-08-15 **DNS domain name system registrar name conflict trademarks challenge arbitration**

NewsScan

INTERNET REGISTRAR TO CHALLENGE NAME CLAIMS [15 Aug 2001]
In response to widespread criticism, Afilias -- the company that runs the new ".info" domain -- says it will challenge some of the more shaky claims made on the most desirable names. The situation arose when Afilias allowed businesses to claim their trademarks before registration was opened up to the general public. Many of those claims were made on common dictionary words, with registrants providing little or no trademark documentation. Afilias rules allowed would-be challengers to register their complaints, but charged them $295 to begin the process. Even if they were successful, challengers were refunded only $220 of that fee. More than 25,000 .info names have been claimed since preliminary registration opened July 25, and Afilias exec Roland LaPlante says his company expects to file hundreds of challenges with arbiters at the World Intellectual Property Organization. Some of the names already claimed include books.info, consumers.info and business.info. (AP 15 Aug 2001)
http://news.excite.com/news/ap/010815/00/internet-names-for-grabs

---

Category 35.2 *Trademarks vs DNS*

2002-01-16 **DNS domain name system registrar trademark conflict investigation**

NewsScan

INTERNET REGISTRAR CHALLENGES '.INFO' TRADEMARK CLAIMS [16 Jan 2002]
Afilias, the company responsible for registering ".info" names, is challenging 741 registrations made by people who claimed they owned the trademark on the name. Afilias says it didn't have the time to verify that applicants actually held the trademarks that they claimed. "It would have been too complicated and slow, since there is no unified worldwide database for trademarks," says Phillipp Grabensee, an Afilias board member. "We would have had to check every single brand." Afilias is now attempting to sort through its database and weed out fraudulent applications, referring them directly to an international mediator for resolution. During the two-month period set aside for trademark holders to preregister for their names, 52,245 names were registered, and it's estimated about 20% of those names were fraudulently acquired. "Some people seem to have registered a whole dictionary," says Grabensee. (Handelsblatt/Wall Street Journal 16 Jan 2002)
http://interactive.wsj.com/articles/SB10112144497968880.htm (sub req'd)

Category 35.2 *Trademarks vs DNS*

2002-08-23 **cybersquatting Domain Name System DNS conflict lawsuit settlement**

NewsScan

FORD MOTOR COMPANY SETTLES DISPUTE OVER 'FORDFIELD' DOMAIN NAME
Ford Motor Company has settled its federal lawsuit against, Michael Ouellette, the owner of a T-shirt and grass seed business named Ford Field Inc., which the entrepreneur had registered on the Internet as "fordfield." Ford had charged Ouellette with trademark infringement and cybersquatting, but he insisted that his inspiration for the name had been a public baseball diamond where he used to play ball. (AP/New York Times 22 Aug 2002)

Category 35.2 *Trademarks vs DNS*

2003-06-19 **falwell sites name personal information privacy WIPO**

NewsScan

FALWELL WINS IN BATTLE OVER SITES USING HIS NAME
The Rev. Jerry Falwell has won his battle with an Illinois man who created parody Web sites using Falwell's name. Falwell had lodged a previous complaint about the sites with the World Intellectual Property Organization (WIPO), but WIPO ruled against him. Recently he learned that his own organization had trademarked the name Jerry Falwell several years ago when he was doing a television talk show. When that became known, the Illinois man decided to surrender the site names to Falwell, rather than face a lawsuit. (AP/Atlanta Journal-Constitution 19 Jun 2003)

Category 35.2 *Trademarks vs DNS*

2003-11-06 **Microsoft domain name hotmail.co.uk forgets expires**

NewsScan

OOPS! MICROSOFT DROPS THE BALL ON U.K. HOTMAIL DOMAIN
Microsoft apparently forgot to renew its registration for hotmail.co.uk, sending the domain name back into the pool of available names. It was snapped up immediately by a do-gooder, who then contacted Microsoft to alert it to its oversight and arrange a transfer of ownership back to the software giant. However, these efforts to do the right thing were rebuffed and it was only when The Register contacted the company to inquire about the snafu that the matter was "escalated" to upper-level officials who then sought to work out a deal. By all accounts, hotmail.co.uk will be restored to the Microsoft fold within the next few days. (The Register 6 Nov 2003)

Category 35.2 *Trademarks vs DNS*

2004-04-21 **domain name lawsuit conflict settlement intellectual property**

NewsScan

SEX.COM SAGA CONCLUDES

The lengthy legal battle over the rightful ownership of the "sex.com" domain name has come to a conclusion with VeriSign's agreement to settle for terms that are rumored to be around $10 million. "This shows that the small guy can eventually beat a huge company. Hopefully, this leads to better care, custody and control over people's intellectual property," says Gary Kremen, who originally registered the name but found in 1995 that Network Solutions had turned the rights over to convicted forger Stephen Michael Cohen, who duped the Internet registrar into believing he had purchased it from Kremen. A federal court in 2001 ordered Cohen to pay Kremen $65 million, but Cohen skipped the country and is rumored to be living in Monte Carlo. Kremen then set his sights on VeriSign, which had purchased Network Solutions in 2000 and refused to admit any mistake had been made. The company is embroiled in nine other lawsuits over problems with domain-name registrations, according to the company's most recent annual filing with the SEC. (Los Angeles Times 21 Apr 2004)

35.3 Politics & management of the DNS

Category 35.3 *Politics & management of the DNS*

2000-03-17 **DNS domain name system jurisdiction cybersquatting legal ruling**

NewsScan

A federal court in Virginia has ruled that it has jurisdiction over all of the .com, .edu, .net and .org Internet domain names held in the vast registry of Network Solutions, which until recently held a monopoly over domain name registrations. The decision arose earlier this month as the court presided over the case of Caesars World Inc. vs. Caesars-Palace.com. Domain name disputes can be settled without going to court, via the arbitration procedures set up by ICANN and the World Intellectual Property Organization, but if plaintiffs decide to litigate, this ruling means they must answer to the Virginia federal court. "If you lose, all you lose is the property in Virginia" i.e., the domain name, "and not $10 million in damages for trademark infringement," says an expert on legal jurisdiction, although she notes that the names themselves can be very valuable. (Financial Times 17 Mar 2000

Category 35.3 *Politics & management of the DNS*

2000-06-14 **DNS domain name system registrar invoice bill**

RISKS 20 92

Peter G. Neumann summarized an embarrassing lapse of DNS registration: "J.P. Morgan & Company (worth $21 billion) lost its Internet connectivity on 13 Jun 2000 because they failed to pay their $35 bill from Network Solutions for their jpmorgan.com domain: three bills ignored over six weeks. All of their Net customers were affected. (Last year Microsoft failed to reregister a domain name necessary for Hotmail service, although a computer consultant bailed them out by paying the fee for them.) "

In a follow-up contribution to RISKS, Peter Sleggs reported that he has experienced difficulties with Network Solutions' billings. On occasion, he failed to receive paper invoices for one of the two domains he has registered. In addition, his payments for one of the domain failed to be registered correctly. [Comment by MK: at this point, DNS registration is becoming a critical issue for businesses; perhaps a few good tort lawyers could do some good to encourage DNS registrars to shape up and recognize the importance of their operations.]

Similarly, Arthur J. Byrnes reported in RISKS that Network Solutions Inc. claimed that they would send a snail-mail and e-mail warning 30 days before the renewal deadline; they did neither. He very sensibly wrote, "So, my personal experience makes me wonder where the blame actually lies in these stories. I know that if I worked for a dot.com, I'd be checking all of my employer's domains expiration dates."

Category 35.3 *Politics & management of the DNS*

2000-06-26 **domain name system DNS lawsuit**

NewsScan

ICANN, the Internet nonprofit corporation chosen by the Clinton administration in 1998 to run the Internet's domain name system, . . . [was] sued by Afternic.com, a corporation in New York that claims ICANN has violated its own bylaws by refusing Afternic's application to become a registrar for Internet addresses, and by ignoring repeated requests for a meeting. ICANN, controversial from the start and now low on cash, has never denied an application for a company or group to be a domain name registrar, but has kept some (such as Afternic's) on hold. (New York Times 26 Jun 2000)

Category 35.3 *Politics & management of the DNS*

2000-07-10 **domain name system DNS government approval**

NewsScan, New York Times
http://www.nytimes.com/library/tech/00/07/biztech/articles/10doma.html

The General Accounting Office (GAO), the investigative agency attached to Congress, . . . decided that the Clinton Administration acted within the law when it transferred to a nonprofit organization called the Internet Corporation for Assigned Names and Numbers (ICANN) authority to administer the registration of domain names for the Internet. Since its founding, ICANN has often been charged by critics who accuse it of being secretive and undemocratic. (New York Times 10 Jul 2000)

Category 35.3 *Politics & management of the DNS*

2000-07-17 **domain name system DNS trademark**

NewsScan

ICANN, the global Internet name regulator, . . . approved a plan to expand beyond the seven top level Internet domain names, with the new addresses possibly appearing as early as . . . [2001]. The new names could include .shop, .bank, .travel, .museum and .sex, but no decisions on exactly which names would be added have been reached. Meanwhile, critics of the decision include groups that had lobbied for non-western-alphabet names and current owners of .com names who now must worry about protecting their trademarks by registering new names. (Financial Times 17 Jul 2000)

Category 35.3 *Politics & management of the DNS*

2000-07-23 **policy statement DNS domain name service politics**

RISKS, PFIR http://www.pfir.org/statements/policies 20

Lauren Weinstein and Peter G. Neumann, co-founders of the new group "People for Internet Responsibility" (PFIR, < http://www.pfir.org >) published a manifesto entitled "Statement on Internet Policies, Regulations, and Control." The Executive Summary follows:

>It is increasingly clear that the Internet, as embodied by the World Wide Web and a wide variety of other Net-based services and technologies is rapidly becoming a critical underpinning and foundation to virtually every aspect of our lives, from the very fundamental to the exceedingly mundane. It is likely that few aspects of commerce, education, communications, government, entertainment, or any other facets of our daily existence will be unaffected by this exceedingly rapid change that is sweeping the globe far more rapidly than would have been anticipated only a few years ago.

These global and interconnected developments, unprecedented in human history, suggest that decisions regarding policies, regulation, control, and related Internet activities will be of crucial concern to the *entire* world's population. Consequently, the proper representation of many varied interests regarding such activities must be respected.

It is our belief that the current mechanism for making many key decisions in this regard, as embodied in The Internet Corporation for Assigned Names and Numbers, "ICANN" (http://www.icann.org), is proving to be inadequate to the task at hand. We believe that this is the result primarily of structural and historical factors, not the fault of the individuals directing ICANN's activities, whom we feel have been genuinely attempting to do the best possible job that they could with highly complex, contentious, and thankless tasks.

We are convinced that the Internet's future, and the future of humanity that will be depending upon it to ever increasing degrees, would be best served by consideration being given to the establishment of a new, not-for-profit, voluntary, international organization to coordinate issues of Internet policies and related matters. This organization would be based on a balanced representation of private-sector commercial and non-commercial interests, and public-sector interests including governmental bodies and organizations, educational institutions, and other enterprises.

Although the proposed course of action is expected to be difficult, the risks of inaction are enormous and likely to increase dramatically in the coming years.<

Category 35.3 *Politics & management of the DNS*

2000-10-20 **DNS conflict auction lawsuit**

NewsScan,
ZDNethttp://www.zdnet.com/intweek/stories/news/0,4164,2642661,00.html

A self-described "Internet entrepreneur" . . . filed a class-action lawsuit against Network Solutions Inc. [in October], charging the company with hoarding a stockpile of as many as three million domain names, which NSI plans to offer in a potentially lucrative auction. NSI tried to auction the names in May, but a public outcry forced the company to cancel its plans. If the suit is successful, NSI would have to make the expired domain names available to be registered through its public pool of names, rather than being sold off to the highest bidder. "They are attempting to benefit from a product that is not theirs," . . . [said] Scott Powell, the attorney for plaintiff Stan Smith. (ZDNN 19 Oct 2000)

Category 35.3 Politics & management of the DNS

2000-11-03 **DNS domain name system registration lawsuit defamation fraud scam accusations**

NewsScan, USA Today http://www.usatoday.com/life/cyber/tech/cti760.htm

ICANN SUED FOR DEFAMATION The non-profit Internet Corporation for Assigned Names and Numbers (ICANN) is being sued in U.S. District Court in San Antonio by a start-up company called RegLand, which accuses ICANN of defamation and interference in its business. The company says that when it tried to pre-register new domain names, ICANN defamed it by calling it a "fraud" and a "scam." (Bloomberg/USA Today 2 Nov 2000)

Category 35.3 Politics & management of the DNS

2000-11-09 **DNS domain name registration non-English characters conflicts IETF**

NewsScan, San Jose Mercury News
http://www.mercurycenter.com/svtech/news/breaking/merc/docs/085037.htm,
InfoWorld

In November, VeriSign, the company in charge of dot-com, dot-net, and dot-org Internet domain names . . . began accepting Chinese, Japanese, and Korean characters for those suffixes, an action expected to dramatically accelerate Internet globally. Arabic and other non-English languages will be added later. Doug Wolford, the general manager of Network Solutions Inc., VeriSign's registration arm, said: "There's a whole world out there that has really not been able to use the Web. Hundreds of millions of people have to use English to find their native language Web site. It's an absurdity, an artifact of history long outgrown." (AP/San Jose Mercury News 9 Nov 2000)

However, [t]he Internet Society . . . warned that proceeding with the sale of multilingual domain names will harm the stability of the Internet Domain Name System, and asked that the initiative be postponed until the Internet Engineering Task Force can develop a proposed standard for internationalized domain names. Internet Society VP David Maher admits that it's unusual for the group to issue such a strongly worded statement. "This is very significant... We think this will absolutely hurt the DNS and inevitably lead to conflicts as people claim to have the rights to certain names because of this test bed... Real problems come from the fact that there are conflicting proposals for how internationalized domain names should be handled. This automatically ensures there will be serious problems. It's like different companies selling telephone numbers or seats on the same flight." (Infoworld.com 8 Nov 2000)

Category 35.3 Politics & management of the DNS

2000-11-17 **DNS domain name system additions new opposition criticism costs**

NewsScan, New York Times
http://partners.nytimes.com/2000/11/17/technology/17DOMA.html, San Jose
Mercury News
http://www.mercurycenter.com/svtech/news/breaking/internet/docs/646427l.ht
m

[In November, the] Internet Corporation for Assigned Names and Numbers (ICANN) . . . [announced that it would] add seven new top-level domain names for Internet addresses:.info, .biz, .name, .museum, .aero, museum, and .coop. The first two will be for general use, with biz expected to relieve the pressure for businesses to find a unique name within the popular .com domain, which now has 20 million sites; .pro is intended for professionals, such as doctors and lawyers; .name will be used to designate personal Web sites; .museum will be restricted to museums; .aero for airline groups; and .coop for business cooperatives. ICANN did not give its approval to other domain names that had been proposed to it, including .web, .kids, .xxx, .union, .health, .travel, and .geo. The new names will not be put into effect no sooner than next Spring. (New York Times 17 Nov 2000)

The Geneva-based World Health Organization (WHO) . . . issued a statement expressing strong displeasure at ICANN's decision not to include a top-level domain name designated .health, and stating that the organization will "begin immediately to explore ways of recourse." WHO had proposed creation of a .health domain to be used strictly for sites providing information and services which met the quality standards of WHO and public health organizations, consumer groups, and academic institutions. (Reuters/San Jose Mercury News 17 Nov 2000)

[However, it] turns out that the seven new domain names chosen by ICANN may do little to broaden the possibilities for picking an Internet name. Many of the companies tapped to administer the new names are planning to restrict who can buy them by charging hefty registration fees and vetting those that apply. Neulevel, the company that will be administering the .biz domain, reportedly is planning to charge $2,000 for each domain name and $150 a year to renew it. It's also planning to make the .biz names available only to established companies in an effort to prevent cybersquatting squabbles. Many of the other organizations chosen to run the new domains are thinking about imposing similar restrictions. (BBC News Online 21 Nov 2000)

Category 35.3 *Politics & management of the DNS*

2000-11-30 **DNS domain name system conflicts politics**

NewsScan, Wall Street Journal
http://interactive.wsj.com/articles/SB975524587449438763.htm

VeriSign's recent initiative to register Chinese-language Internet domain names has unleashed a maelstrom of conflict, with a Chinese government affiliate immediately launching its own rival, and incompatible, system. The result could be two separate Internet routing systems, causing major headaches for Chinese-speaking Internet surfers. "The risk is balkanization of the Internet, dividing the Internet up into islands of connectivity," says Pindar Wong, who until recently served as vice chairman of ICANN. "Global connectivity is the most precious aspect of the Internet. Anything that might potentially jeopardize that needs to be considered very carefully." The battle exemplifies Beijing's efforts to both embrace the Internet's development potential while at the same time attempting to control it. Critics say the system operated by the government-affiliated China Internet Network Information Center is as isolating as if China decided it would use its own system of telephone numbers. "It's a classic case of China trying to develop the Internet the way it suits them rather than what suits the rest of the world," says a senior analyst for IDC. (Wall Street Journal 30 Nov 2000)

Category 35.3 *Politics & management of the DNS*

2001-02-05 **DNS domain name system new politics**

NewsScan

ICANN DEFENDS NAME CHOICES
ICANN chairman Vinton Cerf acknowledges that the group may have rejected qualified proposals when it approved seven new domain names last year, but says that the goal "was not to have a contest and pick winners." ICANN purposely kept the pool of new names small, so that it could test whether the additions caused any problems with the overall system. Domain names, he says, have never been added "in the context of the Internet as it exists today. We want to do so without endangering the utility of what has become a global medium for communications and commerce." (AP/Washington Post 8 Feb 2001)
http://washingtonpost.com/wp-dyn/articles/A44287-2001Feb8.html

---

Category 35.3 *Politics & management of the DNS*

2001-07-26 **DNS domain name system ICANN lawsuit lottery**

NewsScan

LAWSUIT CHALLENGES .BIZ 'LOTTERY' [26 Jul 2001]
A class-action lawsuit filed in Los Angeles Superior Court this week alleges that NeuLevel, the operator of the new ".biz" domain, is running an illegal lottery by charging customers just for a chance to register a .biz name. There is no guarantee that a customer will be awarded a desired name, as more than one customer may pay for a chance on the same name. The suit names as co-defendant the Internet Corporation for Assigned Names and Numbers (ICANN) and several registrars, including VeriSign and Register.com, which have been licensed to sell .biz and other Internet domain names to the public. The plaintiffs argue that NeuLevel's "lottery enterprise" is not only illegal, but unfair because it allows those with larger financial resources to increase their odds of getting a name by buying multiple chances. (InteractiveWeek 26 Jul 2001)
http://dailynews.yahoo.com/h/zd/20010726/tc/lawsuit_challenges_dot_biz_lottery__1.html

---

Category 35.3 *Politics & management of the DNS*

2001-11-06 **ICANN DNS domain name service politics election candidates**

NewsScan

ICANN CONSIDERS REDUCING PUBLIC ROLE IN INTERNET MANAGEMENT [6 Nov 2001]
The At-Large Membership Study Committee of ICANN, the nonprofit international organization responsible for developing policies for Internet address assignment and management, is recommending that special fees be charged to members of the public who want to participate as at-large directors in ICANN's decision-making processes. Former Swedish Prime Minister Carl Bildt, who heads the Committee, says that existing and other proposed methods for picking at-large directors are unworkable: "You can have all sorts of visionary schemes but we living in the reality of today. ICANN needs stability. This is not the time for experiment." Last year's at-large elections allowed voting by e-mail, and suffered from technical and administrative difficulties. (AP/San Jose Mercury News 6 Nov 2001)
http://www.siliconvalley.com/docs/news/svfront/043415.htm

Category 35.3 *Politics & management of the DNS*

2001-11-13 **ICANN security DNS domain name service registrars security attacks vulnerability Internet**

NewsScan

ICANN REVIEWS NETWORK SECURITY ISSUES [13 Nov 2001]
Speaking at the annual meeting of the Internet Corporation for Assigned Names and Numbers (ICANN), network security expert Paul Vixie warned: "The Internet is very fragile. It would be very easy for an angry teenager with a $300 computer to create almost unlimited pain for anyone on the Internet and not get caught. We've got to have attention focused on this." Some ICANN critics charge the organization with having ignored security concerns until forced to address them, and Paul-Jean Jouve, president of the network security company Brinx Corp, wrote in a letter: "I am deeply troubled by the complacency of the ICANN leadership on the subject of security. It took worldwide fears to stimulate the dialogue on this issue." (Reuters/New York Times 13 Nov 2001)
http://partners.nytimes.com/reuters/technology/tech-tech-icann-security.html

---

Category 35.3 *Politics & management of the DNS*

2001-11-14 **DNS domain name system international conflict dispute control**

NewsScan

DOMAIN NAME FIGHTS IN NONWESTERN COUNTRIES
Many of the world's Internet users have address suffixes indicating the countries in which they are located (such as ".fr" for France), but often "location" is not really the right word. For example, the ".tj" domain for Tajikistan is actually run out of Fresno, California, and 800 of the 1,000 Web sites are pornographic in nature. Tajik activist Asomiddin Atovev, who works with the Global Internet Project Initiative, sees both the problem and the solution: "The first step is getting control out of the U.S." (Reuters/San Jose Mercury News 14 Nov 2001)
http://www.siliconvalley.com/docs/news/svfront/029080.htm

Category 35.3 *Politics & management of the DNS*

2002-01-21 **DNS domain name system lottery**

NewsScan

REGISTRARS REJECT VERISIGN'S 'PAY-TO-WAIT' PROPOSAL [21 Jan 2002]
Internet domain name registrars overwhelmingly oppose VeriSign's proposal to create a pricey waiting list for registered domain names, calling it too expensive and anti-competitive. VeriSign has suggested charging registrars $40 for first dibs on a registered domain name. A subscriber would be guaranteed first-refusal rights to the name if it becomes available, but would still have to pay even if the current owner decided to renew its subscription. VeriSign said the waiting list would provide a new source of revenue and discourage speculation in domain names by raising the cost. Other registrars complained that instead of solving the cybersquatting problem, the proposal would just shift the action to the waiting list. In addition, some expressed suspicions that VeriSign would use the waiting list to hoard all the best names for itself, but Chuck Gomes, VP of policy and compliance for VeriSign's Global Registry Services, said his company maintained a strict "firewall" between the two sides of the business: "I ensure that day by day we're not advantaging any registrar I understand the mistrust, but it's unwarranted." (Wired.com 21 Jan 2002)
http://www.wired.com/news/business/0,1367,49756,00.html

Category 35.3 *Politics & management of the DNS*

2002-02-25 **DNS domain name system government involvement politics policy model**

NewsScan

ICANN PRESIDENT WANTS MORE GOVERNMENTAL PARTICIPATION
Stuart Lynn, president of the nonprofit Internet Corporation for Assigned Names and Numbers, says the organization he heads needs to be restructured to obtain more governmental participation: "I am now convinced that the original desire to avoid a totally governmental takeover ... led to an overreaction -- the choice of a totally private model." Such a model is unworkable, Lynn says, because it leaves ICANN "isolated from the real-world institutions -- governments -- whose backing and support are essential." His recommendation calls for the next ICANN board to have 15 members -- one-third nominated by governments, one-third selected through a committee process, and the remaining consisting of the group's president and appointments by four policy and technical groups. (AP/San Jose Mercury News 25 Feb 2002)
http://www.siliconvalley.com/mld/siliconvalley/2741326.htm

NEW PROPOSAL DISPARAGED BY ICANN CRITICS [25 Feb 2002]
The proposal made by ICANN president Stuart Lynn to expand the participation of the world's governments in making policy decisions over Internet domain names and other issues is being widely criticized for "closing the door to the public" (Karl Auerbach) and for giving "totalitarian governments power to influence rules that would go into direct effect in the United States" (Michael Froomkin). Lynn maintains that the national governments are "the most evolved form of representation of the public interest," even if not all are democratic. The acronym ICANN stands for Internet Corporation for Assigned Names and Numbers. (AP/San Jose Mercury News 25 Feb 2002)
http://www.siliconvalley.com/mld/siliconvalley/2745051.htm

Category 35.3 *Politics & management of the DNS*

2002-03-15 **DNS domain name system governance**

NewsScan

ICANN REJECTS BOARD MEMBER ELECTIONS
ICANN, the international nonprofit group that sets policy for the Internet's "domain-naming" (i.e., addressing) system, has decided against electing its board members by general elections, at least for the time being. In an ICANN meeting in Ghana, board chairman Vinton Cerf said, "It is obvious to all of us after carefully examining the issues that we're not doing elections now" -- and ICANN chief executive Stuart Lynn said the reason for the decision was that most board members feared general elections could be marred by fraud and dominated by special interests. Board member Karl Auerbach dissented vehemently from the group's decision: "ICANN made a great leap backwards. It repudiated the compact on which it was formed -- an agreement that ICANN would, being a public and tax-exempt entity, allow the public to meaningfully participate." The acronym ICANN stands for the Internet Corporation for Assigned Names and Numbers. (AP/San Jose Mercury News 14 Mar 2002)
http://www.siliconvalley.com/mld/siliconvalley/2861182.htm

Category 35.3 *Politics & management of the DNS*

2002-03-20 **DNS Domain Name System governance lawsuit**

NewsScan

ICANN SUED BY ONE OF ITS BOARD MEMBERS
ICANN dissident board member Karl Auerbach is suing to gain access to the group's travel records, payroll figures, and other information he says he needs "to exercise independent judgment and fulfill my duties as director." ICANN staff have refused to provide him that kind of information unless he first signs a confidentiality agreement, but he has attacked them for being secretive and unaccountable to millions of Internet members. In his lawsuit, Auerbach is being represented by the civil-libertarian Electronic Frontier Foundation. (Reuters/USA Today 18 Mar 2002)
http://www.usatoday.com/life/cyber/tech/2002/03/18/icann-sued.htm

---

Category 35.3 *Politics & management of the DNS*

2002-04-01 **DNS Domain Name System governance**

NewsScan

CRITICS TELL ICANN: NO YOU CAN'T
Critics of the nonprofit organization ICANN (the Internet Corporation for Assigned Names and Numbers) continue to be unimpressed with efforts (or perceived lack thereof) to involve ordinary Internet users in the process of managing the Internet. Criticized for his recent proposal to revamp the organization's board and committee structure, ICANN president and chief executive M. Stuart Lynn says, "The proposal put on the table was bound to change. If there are better ways, let's hear them." See www.icann.org. (New York Times 1 Apr 2002)
http://www.nytimes.com/2002/04/01/technology/ebusiness/01DOMA.html

---

Category 35.3 *Politics & management of the DNS*

2002-05-21 **DNS Domain Name System children legislation law**

FindLaw Download This 86

HOUSE APPROVES DOT-KIDS INTERNET DOMAIN
The House of Representatives' today approved legislation designed to cordon off a safe online "playground" for young children. House members voted 406-2 to approve the "Dot-Kids Implementation and Efficiency Act of 2002," which would mandate the creation of a "dot-kids" extension within America's sovereign "dot-us" Internet domain. The new Internet addressing space "will be a cyberspace sanctuary for content that is suitable for kids," said Rep. Edward Markey (D-Mass.) during today's debate.

http://www.newsbytes.com/news/02/176705.html

Dot-Kids Implementation and Efficiency Act of 2002 (H.R. 3833)
[Copy and paste link into browser] [PDF]
http://frwebgate.access.gpo.gov/cgibin/getdoc.cgi?dbname=107_cong_bills&docid=f:h3833ih.txt.pdf

---

Category 35.3 *Politics & management of the DNS*

2002-06-11 **DNS Domain Name System governance**

NewsScan

DYSON SAY ICANN HAS BECOME 'A REAL CESSPOOL'
Esther Dyson, tech celeb and former chair of ICANN (the Internet Corporation for Assigned Names and Numbers), told an audience at the Wharton business school that "ICANN has become a real cesspool," because of its tangled disputes about authority, accountability, and openness. The independent agency is in charge of managing policy for the Internet's name and address systems. "When I was a young student, I thought grow-ups would come and make things work. Now I realize that grown-ups are just kids with wrinkles. I only see juvenile behavior at ICANN." (Public Policy & Management Emory, Jun 2002)
http://knowledge.emory.edu/articles.cfm?catid=9&articleid=517&homepage=yes

---

Category 35.3 *Politics & management of the DNS*

2002-06-13 **DNS Domain Name System governance**

NewsScan

ICANN BY ANY OTHER NAME WOULD BE THE SAME
Testifying before a Senate subcommittee showing skepticism about the performance of ICANN, the nonprofit organization set up to assign Internet names and numbers and set policies to guide the Internet, U.S. Commerce Department official Nancy Victory said that "the department continues to be supportive of the ICANN model," and suggested that establishing a new group to take its place would accomplish nothing: "Yes, it gets you a new bunch of people, yes it gets you a new company with a new name, but you still encounter the same problems." Without disagreeing with Ms. Victory, subcommittee chairman Ron Wyden (D-Ore.) said: "If ICANN is going to reform itself, the Department of Commerce is going to have to push the organization harder than they have done in the past." (Reuters/New York Times 12 Jun 2002)
http://partners.nytimes.com/reuters/technology/tech-tech-icann.html

---

Category 35.3 *Politics & management of the DNS*

2002-06-25 **DNS Domain Name System governance dispute conflict business government membership**

NewsScan

SHOW-DOWN IN BUCHAREST
At its annual meeting in Bucharest this week the nonprofit organization ICANN, which stands for Internet Corporation for Assigned Names and Numbers, will be facing its fiercest critics and defending its recent proposal to limit ICANN board membership to representatives of business and government. Long-time ICANN critic and University of Miami law professor Michael Froomkin says: " I don't think governments are needed, nor at this time are they organized in a manner that would make their representation easy. The officials who turn up to ICANN meetings are the ones who heard about the Internet first, not necessarily the people who make, or should make, Internet policy." (Reuters/San Jose Mercury-News 25 Jun 2002)
http://www.siliconvalley.com/mld/siliconvalley/3540508.htm

Category 35.3 *Politics & management of the DNS*

2002-09-23 **DNS Domain Name System governance politics**

NewsScan

ICANN WINS ANOTHER YEAR
The U.S. Commerce Department has given a one-year renewal to ICANN (the Internet Corporation for Assigned Names and Numbers), whose mission is to oversee the Internet's domain name system. Acknowledging some criticisms that the group is not sufficiently accountable to the public, the Commerce Department is telling ICANN to increase participation from the broader Internet community and to make the group's decision-making processes more open. (AP/San Jose Mercury News 21 Sep 2002)

Category 35.3 *Politics & management of the DNS*

2002-10-15 **DNS Domain Name System politics governance**

NewsScan

INTERNET SOCIETY TO MANAGE '.ORG'
ICANN (the Internet Corporation for Assigned Names and Numbers) has tapped the nonprofit Internet Society to manage domain names ending in ".org" beginning next year. Currently, those names are managed by VeriSign Global Registry Services, whose contract expires Dec. 31, 2002. ICANN officials say the Internet Society plans to create a new nonprofit organization, dubbed the Public Interest Registry, which will subcontract with Afilias to handle the registration business. Afilias also operates the ".info" domain name. (AP 15 Oct 2002)
http://apnews.excite.com/article/20021015/D7MLV78O0.htm

Category 35.3 *Politics & management of the DNS*

2002-10-31 **DNS Domain Name System governance politics**

NewsScan

ICANN UNDER NEW ATTACKS
ICANN — the Internet Corporation for Assigned Names and Numbers — is one of those organizations apparently destined for continuous controversy. The organization recently eliminated five sitting board members from the 18-person directorate, leading to new charges of its running a closed and "illegitimate" organization. Hans Klein, chairman of the Computer Professionals for Social Responsibility, says of ICANN's leaders: "I think legitimacy matters, they don't. If you kill the legitimacy of an organization, you put the organization at risk. ICANN has decided that legitimacy doesn't matter; it's done away with many of the mechanisms that insured its legitimacy. If people start leaving the organization, it will be ruined." And Michael Froomkin, another ICANN critic, says: "What's outrageous is that because the ICANN staff can't stand to have its actions questioned, it's making sure it never has to face the user community in an election again. In fact, in the new 'reform' plan, ICANN's insiders have put themselves in charge of the process that will select their successors." (Internet News 30 Oct 2002)

Category 35.3 *Politics & management of the DNS*

2002-11-12 **DNS Domain Name System governance**

NewsScan

ICANN TO CREATE THREE MORE 'SPONSORED' DOMAINS
ICANN, the nonprofit Internet Corporation for Assigned Names and Numbers, is planning the creation of three new "sponsored" (or narrowly focused) Internet address domains, which, like dot-museum (for the museum community) or dot-coop (for employee-owned co-op organizations), will be reserved for specific audiences (as contrasted with, say, dot-com, which is open to all potential registrants). The reason for this strategy, says ICANN president Stuart Lynn, is to avoid a gold-rush environment that characterized the creation of new domains in the past. But ICANN board member Karl Auerbach, who is also a long-time critic of the organization, accuses Lynn of "making a down-and-out decision about who can be in business on the Internet and who cannot"; he thinks ICANN is creating an artificial scarcity of domain names, to benefit businesses that sell existing domains. (Washington Post 11 Nov 2002)

Category 35.3 *Politics & management of the DNS*

2002-12-16 **domain name system DNS regulations limits trademarks**

NewsScan

ICANN HEAD FAVORS MEMBERS-ONLY DOMAINS [10 Jan 2002]
ICANN president M. Stuart Lynn says he favors creating new members-only suffixes, such as .edu and .museum, over unrestricted domains such as .biz and .info. "A lot of the problems surrounding the new (top-level domains) are less (common) in a sponsored environment," he said, echoing sentiments expressed by ICANN chairman Vint Cerf at a meeting in December. Problems such as cybersquatting disputes would be greatly diminished in a more tightly regulated domain, said Lynn. "It may be that a number of these cybersquatting or trademark disputes are going to be less because there's a lot of careful evaluation to make sure that someone really is using them for their announced" purpose. Lynn and Cerf have both emphasized that their opinions are their own and not those of ICANN, but that they've talked with many people who agree with them. "More people I talk to think it's the more likely direction," said Lynn. (Reuters/CNet 10 Jan 2002)
http://news.cnet.com/news/0-1005-200-8436749.html?tag=mn_hd

THE INTERNET NAME GAME [14 Jan 2002]
The London-based Global Name Registry has begun offering registration of Internet names for individual persons. Name registration will cost about $30 a year (not including Internet access), and the registry plans to expand ".name" designations to mobile phones and other personal devices by the end of the year. (AP/San Jose Mercury News 14 Jan 2002)
http://www.siliconvalley.com/docs/news/svfront/002411.htm

ICANN ENDORSES NEW DOMAINS
At its annual meeting, ICANN (Internet Corporation for Assigned Names and Numbers) said it will endorse a limited number of new top-level domains for only the second time since 1985. The next group likely will be "sponsored domains" targeting a specific industry or field, such as .travel, .news, or .health. The decision will please some of the business that have been clamoring for ICANN to open up new addresses, but will also inevitably bring more disputes. "There will always be controversy. It's a very different world we're in today, a very noisy world," said ICANN president M. Stuart Lynn. (Wall Street Journal 16 Dec 2002)

Category 35.3 *Politics & management of the DNS*

2003-03-21 **DNS Domain Name System governance policies politics**

NewsScan

NEW ICANN CHIEF TO CONTINUE POLICY FOCUS
Succeeding Stuart Lynn as CEO of the often-controversial Internet Corporation for Assigned Names and Numbers (ICANN), in-coming chief Paul Twomey says that in addition to focusing on technical coordination, the organization will also have to continue its efforts to deal with the policy issues such as intellectual property, privacy, and law enforcement: "The consequences of those technical issues flow into other arenas, like intellectual property, consumer protection, and privacy, potentially even into commercial relationships between infrastructure providers. The law enforcement issues are potentially issues like identification for Whois databases (which list information on domain name owners), identification of those people who are committing computer crimes, (and) ensuring that financial scams don't take place on the Internet." Twomey, an Australian, has been a consultant and government bureaucrat. (CNet News.com 19 Mar 2003)
http://news.com.com/2100-1028-993390.html

Category 35.3 *Politics & management of the DNS*

2003-04-04 **forecast warning domain name system DNS work Internet future extension**

NIPC/DHS

April 04, Electronic Times — DNS pioneer warns of Internet security.

When it comes to the Domain Name System (DNS), the database architecture at the heart of the Internet infrastructure for the last 20 years, "the majority of the work to be done still lies ahead of us," said Paul V. Mockapetris who co-invented DNS in 1983. Mockapetris received the 2003 IEEE Internet Award for his pioneering work on DNS on Tuesday. Mockapetris warned that efforts need to be made to improve its security especially since the October 2002 attacks on 9 of the Internet's 13 DNS root-name servers that contain the master domain list for DNS and the March 27th 2003 hacker attacks on the al-Jazeera network, part of which were DNS-based. Despite attacks that portend graver security breaches, Mockapetris noted that The Internet Engineering Task Force has not yet hammered out a standard after nearly a decade of work. With a security model for DNS in place, extensions could be built onto DNS that would relate to creating greater opportunities on the Internet including phone numbers for IP telephony, distribution of security keys and certificates, and no-call lists for telemarketers. But without it, there is a "real opportunity for fraud" as the hacker community climbs the technology ladder and puts the 30 million people with web domains at risk, according to Mockapetris.

Category 35.3 *Politics & management of the DNS*

2003-04-27 **domain names non-English ICANN Chinese Japanese Korean**

NewsScan

NON-ENGLISH DOMAIN NAMES COMING SOON
The Internet Corporation for Assigned Names and Numbers (ICANN), is poised to approve technical standards that will enable registration of Internet domain names in Chinese, Arabic and other languages. "A great deal of progress has been made this week and I hope we will see progress as the weeks go by," said ICANN chairman Vinton G. Cerf at this week's meeting in Rio de Janiero. "The technical standards are ready. Now the policy work has to be done… The languages that are most advanced are Japanese, Chinese and Korean. Those groups have done a tremendous amount of work to translate their scripts into domain names." Currently, the core computers that handle online addresses understand only the 26 English letters, 10 numerals and a hyphen, along with a period for splitting addresses into sections. How soon users will be able to obtain domain names in other languages depends largely on the extent to which technicians using those languages have translated their alphabets into Internet protocol, said Cerf. (AP 27 Mar 2003)

Category 35.3 *Politics & management of the DNS*

2003-06-27 **ICANN At-Large structures infrastructure personal information whois**

NewsScan

ICANN PLANS TO OPEN THE DOORS
The Internet Corporation for Assigned Names and Numbers (ICANN) has long been accused by critics of being a closed organization, but a reform movement begun under outgoing president Stuart Lynn (and continued by his successor, Paul Twomey) will allow organization of the individual Internet user community for informed participation in the organization. Applications will be accepted from groups seeking designation as "At-Large Structures." In a separate discussion, the group tried to wrestle with the question of how much personal data collected by Internet domain administrators should be publicly available. Twomey said, "Although no definitive policy was formed, a lot of healthy dialogue took place paving the way for future policy development." (Internet News 27 Jun 2003)

Category 35.3 *Politics & management of the DNS*

2003-07-25 **domain name switch lawsuit sex.com**

NewsScan

NETWORK SOLUTIONS MAY BE LIABLE FOR SEX.COM SWITCH
A U.S. appellate court has ruled that Web registry Network Solutions may be liable for damages for its part in transferring the domain name "sex.com" from its rightful owner, Gary Kremen, to convicted forger Stephen Michael Cohen. In his ruling, Judge Alex Kozinski said that domain names should be treated as property, despite their virtual nature, comparing them to "a plot of land." "Exposing Network Solutions to liability when it gives away a registrant's domain name on the basis of a forged letter is no different from holding a corporation liable when it gives away someone's shares under the same circumstances. The common law does not stand idle while people give away the property of others," wrote Kozinski, who returned the case to the U.S. District Court in San Jose to be tried again. "This was a major victory, no doubt about it," said Kremen, who won a $65 million judgment against Cohen, but has been unable to collect because Cohen has fled the country. The case, which may garner landmark status for equating domain names with tangible property, likely will be retried within a year. (CNet News.com 25 Jul 2003)

Category 35.3 *Politics & management of the DNS*

2003-09-22 **ICANN Verisgn site finder typographical errors URL site Internet Corporation For Assigned Names and Numbers**

NewsScan

ICANN ASKS VERISIGN TO SHELVE SITE FINDER SERVICE
ICANN (Internet Corporation for Assigned Names and Numbers) has issued a statement voicing "widespread expressions of concern" over the technical repercussions possible from VeriSign's recently launched Site Finder service. Site Finder steers Web users who make typographical errors while entering URLs to a site operated by VeriSign. Critics say the technical process by which VeriSign "hijacks" users could disrupt e-mail delivery as well as impair the ability of ISPs to block "spam" sent from non-existent Internet addresses — a common technique for reducing the volume of junk e-mail. In self-defense, some ISPs and software groups have developed patches that prevent the Site Finder software from working on their networks. (Wall Street Journal 22 Sep 2003)

Category 35.3 *Politics & management of the DNS*

2003-10-06 **Versign DNS domain name ICANN site finder suspended**

NewsScan

VERISIGN AGREES TO SUSPEND SITE FINDER SERVICE
VeriSign and ICANN reached a temporary truce Friday, with VeriSign acquiescing to ICANN's demand that it suspend its controversial Site Finder service pending further technical review. ICANN could have fined VeriSign as much as $100,000 or even revoked its contract to manage the master list of .com and .net Internet domain names. Critics have charged VeriSign with undermining the collectivist culture of the Internet with the preemptive launch of its service, which redirects Web users who mistype a URL to the VeriSign Web site. "In the past when you made a dramatic change to the network structure that was the least bit potentially damaging, you went out through the community and you exposed what you were going to do and got reaction," says Carnegie Mellon computer science professor David Farber. VeriSign "just broke the whole process." In its defense, VeriSign executives say they notified ICANN of their plans ahead of time, but admitted that they sidestepped ICANN's lengthy approval process because it's too slow. In response, ICANN says it's "sympathetic to concerns" about its process and has proposed a more streamlined procedure for reviewing new services such as Site Finder. (Wall Street Journal 6 Oct 2003)

Category 35.3 *Politics & management of the DNS*

2003-10-16 **Verisign DNS Network Solutions sale ICANN URL**

NewsScan

VERISIGN SHEDS NETWORK SOLUTIONS
VeriSign is selling its Network Solutions domain registrar business to Pivotal Private Equity for about $100 million, but plans to retain control over the .com and .net database that Network Solutions operates. The domain registration business has essentially become a commodity service as more registrars have entered the field. VeriSign has been in the news recently for its controversial Site Finder service, which redirects all mistyped URLs to a search page that it operates. It suspended the service under pressure from ICANN, which expressed concern over the technical ramifications of the Site Finder service, but VeriSign said Wednesday that it plans to restart the service after having found "no identified security or stability problems" in the system. (CNet News.com 16 Oct 2003)

Category 35.3 *Politics & management of the DNS*

2003-11-06 **Internet address space**

NWF

The BBC reported in October 2003 that the Internet would run out of new IP addresses in 2005. Scott Bradner of Harvard University pointed out serious errors in the report. In contrast to the projections from the BBC, the consensus among Internet specialists predicts another 20 years to exhaust the 4B addresses under IPv4. Under IPv6, there will be an additional 64B addresses available.

Category 35.3 *Politics & management of the DNS*

2003-11-11 **internet united states european commission ICANN Internet Corporation for Assigned Names and Numbers public resource**

NewsScan

WILL THE U.N. TAKE OVER THE INTERNET?
Some of the developing countries want to put management of the Internet under United Nations control. U.N. officials expect governments to continue talks on Internet governance with the aim of reaching accord by 2005. Brazil, India, South Africa, China and Saudi Arabia are dissatisfied with the current Internet regulator, the semi-private California-based ICANN (the Internet Corporation for Assigned Names and Numbers), and argue that the Internet is a public resource that should be managed by national governments and by intergovernmental organizations. But both the United States and the European Commission are standing behind the ICANN model, in the belief that to turn Internet regulation over to governments could threaten the existence of the borderless Internet. (Financial Times 11 Nov 2003)

Category 35.3 *Politics & management of the DNS*

2003-12-10 **Internet domain name system DNS politics control ICANN**

NIPC/DHS

December 10, Washington Post — UN sets aside debate over control of Internet.

In a last-minute meeting this weekend before the start of this week's World Summit on the Information Society in Geneva, Switzerland, representatives set aside a debate over whether national governments, rather than private-sector groups, should be in charge of managing and governing the Internet around the globe. UN member states instead will ask Secretary General Kofi Annan to put together a panel of experts from government, industry and the public to study the issue and draft policy recommendations before the high-tech summit reconvenes in Tunisia in 2005. Leaders had planned to wade into a debate over the way Website and e-mail addresses are doled out, standards are set for Internet security and the thorny question of how Internet-based transactions are taxed, among other things. Some developing nations have complained that the world's most visible Internet governance body — the U.S.-based, nonprofit Internet Corporation for Assigned Names and Numbers (ICANN) — hasn't adequately represented non-U.S. interests, and should be replaced with a governmental group overseen by the United Nations. ICANN has managed the Internet's global addressing system since 1998 under an agreement with the U.S. government.

Category 35.3 *Politics & management of the DNS*

2004-02-26 **Verisign ICANN lawsuit Internet domain SiteFinder website redirection**

NewsScan

VERISIGN SUES ICANN

VeriSign has filed a federal lawsuit against ICANN, the regulatory body, charging that ICANN has unfairly prevented VeriSign from developing new services for Internet users. According to the suit, ICANN "has overstepped its authority by trying to become the regulator of the Internet." ICANN (the Internet Corporation for Assigned Names and Numbers) is a nongovernmental organization empowered by an agreement with the U.S. government, whereas VeriSign is a private-sector corporation. The lawsuit alleges that ICANN improperly prevented the company from maintaining an online search service, 'SiteFinder', that redirected mis-typed Internet addresses to an advertising-supported search service operated by VeriSign. A VeriSign executive said that ICANN had no authority to force it to shut down Site Finder, and complains: "Working the ICANN process is like being nibbled to death by ducks." But critics of VeriSign say that SiteFinder, by redirecting attempts to access non-existent Web sites, would force the rewriting of hundreds of programs and devices across the Internet. (Washington Post 26 Feb 2004)

Category 35.3 *Politics & management of the DNS*

2004-03-11 **Internet Corporation for Assigned Names and Numbers ICANN addresses mobile phone manufacturers protocols**

NewsScan

WANTED: INTERNET DOMAIN FOR MOBILE SERVICES

Microsoft, Nokia, Vodafone, Samsung, Hewlett-Packard and Sun Microsystems are proposing a new Internet domain name such as ".mobile" that would be dedicated to online services available to cell phone users. The companies have submitted their request to ICANN, which is soliciting suggestions for new domains before its March 16 deadline. Decisions could be made as early as this year on adding new domain names to the 250 already in existence. (AP 11 Mar 2004)

Category 35.3 *Politics & management of the DNS*

2004-03-11 **Internet Corporation for Assigned Names and Numbers ICANN addresses mobile phone manufacturers protocols**

NewsScan

SPECIAL INTERNET ADDRESS PROPOSED FOR MOBILE DEVICES

Nokia, Vodafone, Microsoft, Hewlett-Packard and five other companies are proposing creation of a new Internet domain for mobile Web access, probably with a name such as .mobile or .phone. Wireless ApplicaTion Protocol, a protocol created to reformat Web pages for handheld devices, has been submitted to the Internet Corporation for Assigned Names and Numbers (ICANN); it calls for a new for-profit joint venture set up by the companies to manage the mobile registry. A Vodafone spokesman says that a special site for mobile devices "could be organized for speed of download, ease of use and simplicity."(New York Times 11 Mar 2004)

Category 35.3 *Politics & management of the DNS*

2004-03-12 **Internet Corporation Assigned Names Numbers ICANN domain wireless registry**

NIPC/DHS

March 10, International Herald Tribune — New domain is proposed.

Nine technology and telecommunications companies joined Wednesday, March 10, to announce their application for a mobile-specific domain. The application, submitted to the Internet Corporation for Assigned Names and Numbers (ICANN) the overseer of the Internet's address system, calls for a new, for-profit joint venture set up by the companies to manage the mobile registry. Names purchased from the company would explicitly point to wireless-focused domains, making the registry a new type of electronic postal code on the Internet. The companies could require any name registered under the new address heading to have a mobile-specific purpose. By contrast, names registered for use with .com, .net and other generic endings need not have any specific thematic purpose. After ICANN's current application round closes on March 16, independent evaluators will examine the proposals. The technology and telecommunications group expects the application process to take three to six months, and services based on the new address, if approved, might arrive by the first half of 2005.

Category 35.3 *Politics & management of the DNS*

2004-03-24 **Internet domain name sale 100 years**

NewsScan

DEAL OF THE CENTURY — 100-YEAR DOMAIN SERVICE

Responding to frustration over the current Internet domain name registration renewal process, Network Solutions says it will offer a 100-year registration option for $1,000 per name. "We've had a number of customers who have allowed high-value domain names to lapse," says Network Solutions CEO Champ Mitchell, citing Microsoft's failure to renew its Passport.com address in 1999 and the Washington Post's temporary lapse in renewing its washpost.com domain name earlier this year. Mitchell agreed that most domain owners won't want to pony up $1,000 for something that costs $40 per year, but predicted that there might be up to 10,000 potential takers for the 100-Year Domain Service. But Wayne State University law professor Jonathan Weinberg says the deal may not be a bargain for customers. "Just as you wouldn't want to be locked into your phone company for the next hundred years, even if they offered you a really good deal on a phone, it doesn't make a lot of sense to be locked in with a domain registration company for the next hundred years. If Network Solutions should go bankrupt 30 years from now or 70 years from now, you're up a creek." (Washington Post 24 Mar 2004)

Category 35.3 *Politics & management of the DNS*

2004-10-25 **.net domain VeriSign ICANN e-commerce e-mail**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A60758-2004Oct25.html

'.NET' UP FOR GRABS '

.Net,' the world's fourth largest Internet domain, is looking for a new operator, and experts say the stakes are high. The winner, to be chosen by ICANN, could earn as much as $30 million a year, but if the domain were to fail, huge e-mail networks like those operated by Comcast and Earthlink, would go down with it. "It's the most important decision ICANN has ever had to make," says Tom Galvin, VP of government relations for VeriSign, which has operated the .net domain up until now. About 30% of all e-commerce traffic and more than 150 billion e-mail messages a year travel through .net. The handover is the culmination of a deal that VeriSign cut back in 2001, when it agreed to relinquish control over .net in favor of near-permanent ownership of the more lucrative .com domain. VeriSign is permitted to bid on the new .net contract, but will not be given preferential treatment. One likely rival will be Dublin-based Afilias, which in 2003 took over technical management of the .org domain. "There's no question that .net helps underpin the Internet," says Afilias CTO Ram Mohan. "The one [assertion] that strikes me as incongruous is that if you touch .net, everything will fall apart." (Washington Post 25 Oct 2004)

Category 35.3 *Politics & management of the DNS*

2004-10-28 **web domains ICANN .post .travel**

NewsScan; http://apnews.excite.com/article/20041028/D860EHTG0.html

NEW WEB DOMAINS ON THE WAY

Two new Internet domain names -- ".post" and ".travel" -- have received preliminary approval from ICANN, which says they could be in use as early as next year. Talks are now scheduled to hammer out the details on creating and running the domain names, a process that could take months. ICANN is also considering proposals for additional domains, including ".asia," ".jobs," and ".xxx," but the oversight group said the .post and .travel names were different from most existing names because they would be set aside for specific industries and interest groups. The Universal Postal Union in Switzerland wants .post for national postal services, local post offices, business partners and stamp collectors. Private delivery services such as FedEx and UPS would also be eligible. The UPU envisions establishing up to 650,000 virtual post offices to enable users to access their local postal functions anywhere in the world. The Travel Partnership Corp., a New York trade group, wants to make .travel available to travel agents, hotels, airlines, B&B operators, tourism bureaus and others in the travel industry. It hopes that having a specific domain will encourage more travelrelated businesses to put their information on the Web. (AP 28 Oct 2004)

Category 35.3 *Politics & management of the DNS*

2004-11-10 **domain hijacking ICANN deadline default transfer contact address errors**

NewsScan; http://theage.com.au/articles/2004/11/10/1100021855873.html

NEW DOMAIN RULES 'WILL MAKE HIJACKING EASIER'

New rules for domain transfers will come into effect on Friday, making it easier for people to hijack domains, according to the security and network services company Netcraft. The new rules, set by the Internet Corporation for Assigned Names and Numbers (ICANN), will mean that requests for transferring a domain will be automatically approved in five days unless they are denied by the owner of the domain. Currently, the ownership of a domain and the nameservers allotted are not altered if a request for a transfer evokes no response. Domain owners who do not manage their records carefully face problems under the new regime. If the contact addresses given in the records are incorrect, then a request for transfer would go to a wrong address and after five days of no response, the transfer would become effective. (The Age 10 Nov 2004)

Category 35.3 *Politics & management of the DNS*

2004-12-13 **ICANN .mobi .jobs domains**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A61424-2004Dec13.html

ICANN GIVES THE NOD TO TWO MORE DOMAINS

ICANN, the Internet's oversight agency, has given preliminary approval for two additional domain names -- ".mobi," which would delineate Web sites and other services specifically geared toward cell phones, and ".jobs," which would target the human resources community. In October, ICANN gave preliminary approval to ".post" for postal services and ".travel" for the travel industry. ICANN will now begin negotiations with the applicants of all four suffixes on creating and running the domains. There are currently about 250 domain names, mostly for specific countries, such as ".ch" for Switzerland. (AP/Washington Post 13 Dec 2004)

Category 35.3 *Politics & management of the DNS*

2005-02-22 **domains UN ICANN ITU World Summit global control Web developing countries international**

NewsScan; http://australianit.news.com.au/articles/0

U.N. PANEL HOPES TO END WEB WAR

A U.N.-sponsored panel aims to settle a long-running tug of war for control of the Internet at a Tunis meeting this November at the World Summit on the Information Society, where global control of the World World Wide Web may be decided. At present, the most recognizable Internet governance body is the U.S.-based non-profit corporation called the Internet Corporation for Assigned Names and Numbers (ICANN), but developing countries want an international body such as the UN's International Telecommunication Union (ITU) to have control over governance over Internet issues -- ranging from distributing Web site domains to fighting spam. (The Australian 22 Feb 2005)

Category 35.3 *Politics & management of the DNS*

2005-05-09 **Google denial of service DoS Website blackout Internet infrastructure Domain Name System DNS stability**

DHS IAIP Daily; http://www.newscientist.com/article.ns?id=dn7357

GOOGLE BLACKOUT LINKED TO INTERNET INFRASTRUCTURE

A brief blackout at Internet search giant Google has drawn attention to the addressing system that underpins the Web. The Google search page disappeared from view for about 15 minutes late Saturday night, May 7. Some users reported being redirected to an alternative search service called SoGoSearch, but Google has strongly dismissed suggestions that its servers were compromised in any way. Google spokesperson David Krane told the Associated Press that the problem was related to the Domain Name System (DNS), which maps Web names to the numerical Internet Protocol (IP) addresses used by computers. There are thousands of individual DNS servers dotted around the Internet that report back to 13 "root" servers holding master records for DNS mapping. It remains unclear whether the outage at Google was the result of a malfunction in one particular server or the wider system. The outage has drawn attention to widespread reliance of many Web users and services on Google and highlights existing concerns over the stability of DNS infrastructure. In March 2005, the National Academies National Research Council issued a report criticizing the current state of DNS infrastructure. National Academies' Report: http://www7.nationalacademies.org/cstb/pub_dns.html

---

Category 35.3 *Politics & management of the DNS*

2005-06-30 **domain naming system DNS ICANN control US retention United Nations poor countries equal participation**

EDUPAGE; http://news.zdnet.com/2100-9588_22-5770937.html

U.S. WILL KEEP CONTROL OF INTERNET ROOT

Despite previous statements from U.S. officials that the country would cede its control over the Internet to the Internet Corporation for Assigned Names and Numbers, a set of principles outlined this week by the Bush administration states that no such transfer of control will take place. The United States maintains control of the "root" system that determines which domains will function, including not just generic domains such as .com and .org but also country-specific domains. The principles, which were announced unexpectedly at a conference in Washington, D.C., are seen by many as a snub of the world community in general and of certain of its critics in particular. Pakistan and Brazil, for example, have long complained that the United States has too much control over the Internet and should give the world's poorer countries the opportunity to be equal participants. ZDNet, 30 June 2005

Category 35.3 *Politics & management of the DNS*

2005-07-18 **Internet control report recommendations United Nations US**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4692743.stm

UN REPORTS ON CONTROL OF INTERNET

A working group created by the United Nations (UN) to draft a recommendation about the future oversight of the Internet has come up with four options. The Working Group on Internet Governance (WGIG) was created in 2003 following the failure of the UN's World Summit on the Information Society (WSIS) to agree on an Internet governance structure. Three of the WGIG's proposals would take control of the Internet away from the Internet Corporation for Assigned Names and Numbers (ICANN), which is currently run by the United States. Many developing nations have complained that final oversight of the Internet should not rest with U.S. officials. The fourth option would leave control with ICANN but create a forum for debate on Internet issues that face all countries. The four options will be presented to the 2005 WSIS meeting in November, where delegates will choose one. Earlier this month, the United States stated that it would not relinquish control of ICANN or the Internet. BBC, 18 July 2005

Category 35.3 *Politics & management of the DNS*

2005-09-29 **US control Internet Web politics United Nations UN rejection**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/content/article/2005/09 /29/AR2005092900478.html

U.S. INSISTS ON KEEPING CONTROL OF WEB

The U.S. is rejecting offers from the UN to take control over the main computers that direct traffic on the Internet. Ambassador David Gross, the U.S. coordinator for international communications and information policy at the State Department said, "We will not agree to the UN taking over the management of the Internet. "Some countries want that. We think that's unacceptable." Some countries have been upset that the United States and European countries secured a multitude of available Internet addresses, thus leaving developing nations with a limited supply to share.

Category 35.3 *Politics & management of the DNS*

2005-11-14 **Internet Web DNS control United Nations conference US ICANN politics**

EDUPAGE; http://www.nytimes.com/2005/11/14/business/14register.html

UN MEETING TO ADDRESS CONTROL OF INTERNET

The United Nations (UN) is hosting an international conference this week in Tunisia to address concerns about U.S. control of the Internet. The Internet Corporation for Assigned Names and Numbers (ICANN) was set up in 1998 to oversee the Domain Name System, which reconciles Web addresses and directs Internet traffic to proper destinations. Despite an understanding that ICANN would become independent of any national ties, the Bush administration this year rejected such a move, and the organization still operates under the authority of the U.S. Department of Commerce. This situation has left many other countries complaining that the United States holds the power over a global resource, and nine different proposals for putting ICANN under the guidance of an international body will be addressed at the meeting in Tunisia, which will host as many as 15,000 delegates. Some individuals who were part of the work that led to the Internet have said that concerns over ICANN are misguided. Leonard Kleinrock, computer scientist at UCLA, said, "Everyone seems to think that the D.N.S. system is a big deal, but it's not the heartbeat of the Internet." Robert Kahn, one of the developers behind TCP/IP, said of ICANN, "There is nothing in there to control, and there are huge issues that the governments of the world really do need to work on." New York Times, 14 November 2005 (registration req'd)

Category 35.3 *Politics & management of the DNS*

2005-11-16 **Internet Web DNS control United Nations conference US ICANN politics**

EDUPAGE; http://www.siliconvalley.com/mld/siliconvalley/13180104.htm

U.S. TO KEEP CONTROL OF ICANN

Delegates at an international meeting in Tunisia have agreed to allow oversight of the Internet's Domain Name System (DNS) to remain with the United States. Leading up to the World Summit on the Information Society, a number of nations had put forth proposals that would have required the United States to cede DNS control to an international body. Instead, agreement was reached to leave DNS management with the Internet Corporation for Assigned Names and Numbers (ICANN) and create an international forum to address concerns, though the forum will not have binding authority. The Internet Governance Forum is to begin meeting next year and will address issues both within the purview of ICANN, such as the addition of domains in languages other than English, and outside ICANN's authority, such as spam and cybercrime. San Jose Mercury News, 16 November 2005

Category 35.3 *Politics & management of the DNS*

2005-11-29 **dot com management lawsuit DNS management politics ICANN Verisign**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4482292.stm

INTERNATIONAL GROUP SUES OVER .COM MANAGEMENT

The World Association of Domain Name Developers has filed a lawsuit in a California court against the Internet Corporation for Assigned Names and Numbers (ICANN) and VeriSign over a deal recently reached between the two organizations. After resolving a dispute over VeriSign's Site Finder service, which directed users who mistyped URLs to VeriSign's Web site, ICANN agreed to an extension of the contract that allows VeriSign to manage the .com and .net domains. Although the extension runs from 2007 to 2012, the lawsuit filed by the developers association contends that the contract "provides for the automatic renewal of the agreement and thereby precludes competitors from ever entering the .com and .net domain name registration market," thereby establishing a monopoly for the domains. The only means for another company to bid on the work, according to the suit, is if VeriSign goes out of business or fails to meet the terms of the contract. A statement from ICANN said the lawsuit is intended to divert attention away from an ICANN meeting currently being held in Vancouver. BBC, 29 November 2005

Category 35.3 *Politics & management of the DNS*

2005-12-07 **EU Internet domain business DNS politics**

EDUPAGE; http://online.wsj.com/article/SB113391801658415733.html

EU DOMAIN OPENS FOR BUSINESS

A new domain has been launched that supporters believe will help create a sense of identity and strength among the nations of the European Union (EU). The .eu domain is initially open to organizations that hold trademarks or have offices in any of the 25 nations in the EU. The domain will later be opened to other groups and eventually to individuals. More than 400 registrars have been approved to handle applications for the domain. Jean Pire, a senior partner in a Belgian intellectual property law firm, said he expects the .eu domain to grow to be second only to .com in the number of Web sites that use it. Currently, .com is the domain for more than half of the world's Web sites; Pire predicts .eu eventually to represent about 25 percent of Web sites. The .eu extension will not replace existing country-specific extensions, such as .de for Germany and . Fr for France. Wall Street Journal, 7 December 2005 (sub. req'd)

Category 35.3 *Politics & management of the DNS*

2006-03-01 **China Internet split domain .cn .com .net Chinese politics freedom of information domain name system DNS**

DHS IAIP Daily; http://news.zdnet.com/2100−9588_22−6044629.html 23

CHINA CREATES OWN INTERNET DOMAINS.

China has created three of its own top-level domains that will use the domain names .cn, .com and .net, in Chinese. The domain names were launched Wednesday, March 1, by the Chinese Ministry of Information Industry. The creation of Chinese character domain names has led to speculation that China could break away from the Internet Corporation for Assigned Names and Numbers completely, and undermine the global unity of the Domain Name System, the network of servers that resolves domain name requests. Internet experts are concerned that this move will see China administrating its top-level domains with its own separate root servers, which could cause a split in the Internet.

Category 35.3 *Politics & management of the DNS*

2006-03-28 **DNS servers Network Solutions Inc denial-of-service DoS attack**

DHS IAIP Daily; 23
http://www.computerworld.com/developmenttopics/websitemgmt/s
tory/0,10801,109972,00.html

TWO DNS SERVERS HIT BY DENIAL-OF-SERVICE ATTACKS.

In the second attack of its kind in the past few days, Domain Name System servers at Network Solutions Inc. were hit by a denial-of-service attack Tuesday afternoon, March 28, resulting in a brief performance degradation for customers, according to the company. The attacks, which started at around 2:20 p.m. EST, were targeted at the company's WorldNIC name servers and resulted in a service degradation for about 25 minutes before the server was restored to normal, a spokesperson for the company said. Over the weekend, Joker.com, a domain-name registrar in Germany, was hit with a similar distributed denial-of-service attack that disrupted service to customers.

Category 35.3 *Politics & management of the DNS*

2006-04-11 **DNS cache poisoning report study new attacks defense**

DHS IAIP Daily; http://www.lurhq.com/cachepoisoning.html 23

REPORT: DNS CACHE POISONING -- THE NEXT GENERATION.

The old problem of DNS cache poisoning has again reared its ugly head. While some would argue that the domain name system protocol is inherently vulnerable to this style of attack due to the weakness of 16-bit transaction IDs, the immediate threat cannot be ignored while waiting for something better to come along. There are new attacks, which make DNS cache poisoning trivial to execute against a large number of name servers running today. The LURHQ Threat Intelligence Group has released the report, "DNS Cache Poisoning -- The Next Generation," in order to shed light on these new attacks and recommend ways to defend against them. Refer to the source for the full report.

Category 35.3 *Politics & management of the DNS*

2006-04-11 **domain name registry DNS Europe hacked**

DHS IAIP Daily; 23
http://www.infoworld.com/article/06/04/11/77325_HNregistryhi jacked_1.html

EUROPE'S DOMAIN REGISTRY HIJACKED.

The registry for the new .eu domain has grown to 1.4 million Web addresses since Friday morning, April 7 -- but one registrar has accused the group that runs it of inept organization, allowing companies to cheat the system by setting up bogus registrars to work on their behalf. Eurid vzw, which runs the registry, required registrars to apply for accreditation before the "landrush" phase of registrations began. Bob Parsons, chief executive officer of domain name registrar GoDaddy.com Inc., claims that some companies spotted a loophole in the system: by creating additional registrars and applying for accreditation for them, they were able to multiply their chances of successfully making registrations.

Category 35.3 *Politics & management of the DNS*

2006-04-24 **DNS message decompression remote denial-of-service DoS vulnerability solution update**

DHS IAIP Daily; http://www.securityfocus.com/bid/13729/discuss 23

MULTIPLE VENDOR DNS MESSAGE DECOMPRESSION REMOTE DENIAL-OF-SERVICE VULNERABILITY.

Multiple DNS vendors are susceptible to a remote denial-of-service vulnerability. This issue affects both DNS servers and clients. Analysis: Under certain circumstances, it is possible to cause both DNS servers and DNS clients to terminate abnormally by sending it malformed messages. The text portions of DNS messages are specified by first giving the character count, followed by the characters themselves. For example to specify 'test.test.com', the message would look like '0x04test0x04test0x03com0x00' using 16-bit numbers. From RFC1035, Section 4.1.4, "Message Compression" specifies a way to create smaller messages so that they can easily fit into a DNS UDP packet. Hence if the top two bits of the label length byte are one, the remaining 14 bits specify an offset from the beginning of the text on where the remaining characters can be found. This way, redundant information can be removed and hence create a smaller message. For a complete list of vulnerable products: http://www.securityfocus.com/bid/13729/info The following versions are not affected by this issue; users are advised to upgrade: DeleGate 8.10.3 and subsequent versions; dnrd 2.18 and subsequent versions; PowerDNS 2.9.17. Solution: Cisco has released advisory cisco-sn-20050524-dns to address this issue. For further information: http://www.securityfocus.com/bid/13729/references

---

Category 35.3 *Politics & management of the DNS*

2006-05-02 **vulnerability issues Domain Name System DNS implementation**

DHS IAIP Daily; http://www.securiteam.com/securitynews/5IP020KIKU.html 23

VULNERABILITY ISSUES IN IMPLEMENTATIONS OF THE DOMAIN NAME SYSTEM PROTOCOL.

The vulnerabilities described in this advisory affect implementations of the Domain Name System protocol. Many vendors include support for this protocol in their products and may be impacted to varying degrees, if at all. Analysis: If exploited, these vulnerabilities could cause a variety of outcomes including, for example, a denial-of-service condition. In most cases, they can expose memory corruption, stack corruption or other types of fatal error conditions. Some of these conditions may expose the protocol to typical buffer overflow exploits, allowing arbitrary code to execute or the system to be modified. The following vendors have provided information about how their products are affected by this vulnerability: Cisco Systems, Inc MyDNS; Delegate pdnsd; Ethereal Sun; Hitachi Wind River; ISC; Juniper Networks; Microsoft. Refer to source advisory for further detail on vendor vulnerabilities.

---

36 Responses to intrusion

Category 36 *Responses to intrusion*

1998-12-07 **information warfare criminal hackers retaliation attack**

InternetWeek http://www.techweb.com/internet/story/TWB19981207S0003

Rutrell Yasin reported in InternetWeek on the apparently-growing trend for corporate security departments to take vigilante action in fighting computer intrusions. She cited _Corporate America's Competitive Edge_ <http://www.warroomresearch.com/ResearchCollabor/CorpAmerica.htm> an 18-month study of 320 Fortune 500 companies by the WarRoom Research firm <http://www.warroomresearch.com/> which suggested that 30% of the respondents had already installed software designed to counterstrike at attackers. This strategy could easily backfire if the sites attacked in retaliation turned out to be innocent victims of IP spoofing.

Category 36 *Responses to intrusion*

1999-01-12 **information warfare criminal hackers retaliation attack**

CNN http://cnn.com/TECH/computing/9901/12/cybervigilantes.idg/index.html

When "The Electronic Disturbance Theater" criminal hackers attacked Pentagon systems in September 1998, the Pentagon retaliated by flooding the attackers with high-volume traffic, crashing the attacking systems. According to Winn Schwartau, some corporate security operations are taking the law into their own hands; he claims that one group actually located the headquarters of an attacking hacker group, broke into their facility, and stole the cybervandals' equipment. The corporate vigilantes apparently left a note saying, "See how it feels?" The same group also claims to have resorted to baseball bats to intimidate hackers.

Category 36 *Responses to intrusion*

1999-04-17 **information warfare defense retaliation intrusion detection**

OTC

Network Flight Recorder announced retaliatory software that not only detects and blocks the notorious Back Orifice program but also sends back misleading responses to attackers using the program

---

Category 36 *Responses to intrusion*

1999-04-20 **spam legal civil litigation settlement prevention damages**

TechWeb, ZDNet

Virgin Net, a UK Internet Service Provider, sued Adrian Paris, an alleged spammer whom they accused of sending 250,000 junk e-mail messages from one of their accounts in violation of their terms of service. In addition, the ISP was blacklisted by the Realtime Blackhole List, which provides participating ISPs with "kill lists" to block further e-mail from sites originating spam. The ISP received 1,500 complaints as a result of the abuse and sued the scumbag filthy disgusting spammer for breach of contract.

In a similar case, another UK ISP, Bibliotech, sued Sam Khuri and his Atlanta-based company, Benchmark Print Supply, after the American slimeball sent out junk e-mail with forged headers pointing to the innocent ISP; as a result, the enraged staff at Bibliotech were subjected to a "torrent of rejected, unsolicited commercial e-mail." In addition to damages, Bibliotech demanded that Khuri and his co-conspirators refrain from repeating their stupid trick with anyone else. In the USA, forged e-mail headers are currently illegal in Washington, Massachusetts and Virginia.

Category 36 *Responses to intrusion*

2000-02-18 **intrusion honey pot monitoring logging audit criminal hacker penetration vandalism study report**

San Diego Supercomputer Center
http://security.sdsc.edu/incidents/worm.2000.01.18.shtml

The San Diego Supercomputer Center set up an old workstation running Red Hat Linux as a honey pot to attract criminal hackers so they could be monitored. The "worm.sdsc.edu" machine was repeatedly penetrated and vandalized as security specialists watched and analyzed every step taken by the criminals down to logging every single packet used in the intrusions.

---

37 Education in security & ethics

Category 37 *Education in security & ethics*

1999-05-12 **education universities learning research teaching NSA**

EE Times Online

In May, the National Security Agency named seven universities as Centers of Academic Excellence in Information Assurance Education: James Madison, George Mason, Idaho State, Iowa State, Purdue, Idaho, and the University of California at Davis.

Category 37 *Education in security & ethics*

1999-08-01 **criminal hackers sociology psychology harm morality ethics reasoning**

PC Magazine

John Dvorak wrote a blistering challenge to the nonsense spouted by criminal hackers when he wrote his column in PC Magazine on 2000-08-01. He provided a point-by-point rebuttal of the tired arguments of criminals that their depredations are actually socially useful. As Dvorak pointed out about the people who use Trojans to install back doors on victims' systems, "There's nothing good or noble about these Trojan horses or the people who use them. Eventually people will get on the systems of individual users, hack their online banking, and transfer money to themselves. Make no mistake about it, what appear to be harmless pranks today will be serious crimes tomorrow. As more and more people are adversely affected by these guys, the sympathy for them will fade to oblivion. The sooner the better." Dvorak's column made an excellent addition to the reading list for computer-ethics courses aimed at young people (and a slap in the face to the older fools who support criminal hacking).

Category 37 *Education in security & ethics*

1999-10-01 **education children school ethics anti-hacker surf law-abiding**

IDG.NET http://www.idg.net/go.cgi?id=166554

The Information Technology Association of America (ITA) announced a program of cooperation with the Department of Justice in educating children on ethical behavior in cyberspace. Many of the current criminal hacking incidents in recent years have involved juveniles, and other less criminal activities such as sending spam are "the modern-day equivalent of prank telephone calls" in the words of Keithe Perine, writing for <idg.net>.

Category 37 *Education in security & ethics*

1999-10-18 **information technology training basics CD-ROM DoD**

DoD DISA IPMO

At the 22nd NISSC in October 1999, the Defense Information Systems Agency INFOSEC Program Management Office (DIA IPMO) distributed free copies of a September 1998 CD-ROM entitled _Information Age Technology v 1.03_ which could serve as a good primer for novices about to take information security training in a corporate environment.

Other titles from the same source:

DoD INFOSEC Awareness v2.0 (April 1999)
Operational Information Systems Security Volumes 1 & 2 (August 1998)
CyberProtect Interative Training Exercise v1.0 (July 1999)
PKI — Public Key Infrastructure v1.0 (July 1999).

The same group distributed a May 1999 videotape containing four modules:
Computer Security 101 (DOJ)
Computer Security: The Executive Role (DOJ)
Safe Data: It's Your Job (DOL)
Think Before You Respond (NRO)

For information, send e-mail to <dodiaeta@ncr.disa.mil> or visit <www.disa.mil/infosec>. For an order form by fax, leave a message at 703-681-7944 or fax 703-681-1386.

Category 37 *Education in security & ethics*

1999-11-18 **criminal hacking juveniles international law enfocement investigation teaching video**

UPI

The FBI made an entertaining video about their capture of the kids involved in the February 1998 attack spree known as Solar Sunrise, where the Cloverdale Two hit DoD and other networks under the guidance of an Israeli criminal hacker, Ehud Tenebaum. The video was released in November with plans to make it widely available.

Category 37 *Education in security & ethics*

2000-05-22 **intellectual property copyright infringement theft counterfeit morality ethics open-source**

NewsScan

Although some in the "open source" movement, which encourages the voluntary sharing of software source code, think that Napster and similar technologies are "influenced by the open-source ethic," Linux creator Linus Torvalds disagrees: "Piracy is bad. Of course you should be able to sue over copyrights." And Larry Wall, the developer of the Perl programming languages, agrees: "Open source should be about giving away things voluntarily. When you force someone to give you something, it's no longer giving, it's stealing. Persons of leisurely moral growth often confuse giving with taking." (Wall Street Journal 22 May 2000)

Category 37 *Education in security & ethics*

2000-09-22 **intellectual property IP music copyright violations infringement education training ethics awareness debate ambiguous complexity children teenagers students over-simplification**

NewsScan, USA Today http://www.usatoday.com/life/cyber/tech/cti560.htm

In response to criticisms, the Justice Department has agreed to find "more precise" language for the following passage on its Web site answering the question "What is a cyber crime?" with the explanation: "Recently, tools have surfaced that allow Web users to download and save music from the Internet for free — music that is copyrighted by artists and sold in stores. Taking tracks from the Internet is no different from stealing a CD or tape from a music store." Consumer Electronics Association president Gary Shapiro complains: "I'm offended the DOJ would fund a Web site which is telling millions of Americans they are committing a crime when they are not. This is wishful thinking by the (music industry). The fact is, my son is not a criminal; 20 million Napster users are not criminals." The position of American University professor Peter Jaszi, a Napster supporter, is: "There is a real question about what we should teach about copyright," Jaszi said. "Do we want to be telling people the whole story, which is a complicated story, which is all about rights and balances, or are we going to tell them a simplified story that they aren't going to believe or accept? If you try to simplify the message you are going to lose credibility." (USA Today 22 Sep 2000)

Category 37 *Education in security & ethics*

2000-10-10 **ethics education morality training schools law enforcement government parents educators**

NewsScan, San Jose Mercury News
http://www.sjmercury.com/svtech/news/breaking/merc/docs/071435.htm

In alliance with the trade group Information Technology Association of America, the Justice Department has created a "Cybercitizen Partnership" program to encourage educators and parents to promote ethical behavior in cyberspace. FBI official Michael Vatis explains, "In a democracy in general, we can't have the police everywhere. One of the most important ways of reducing crime is trying to teach ethics and morality to our kids. That same principle needs to apply to the cyber world." (AP/San Jose Mercury News 10 Oct 2000)

Category 37 *Education in security & ethics*

2000-12-21 **plagiarism penetration teenagers adolescent criminal hackers education ethics awareness parental guidance ignorance**

RISKS 21 18

Winn Schwartau wrote in RISKS, "Two 8th-grade honor students in Tampa, Hillsborough County, Florida, hacked into the school computer and copied the final exam for one of their courses. They have been suspended. [PGN-ed]

We've wired up the country's schools, put the kids on the Internet, and only a small handful of teachers have any clue as to what goes on behind the mouse button. The teachers are not technically trained, they are underpaid and underappreciated. Is it any wonder? And I doubt the kids have been taught the first thing about CyberEthics by their schools or their parents."

Category 37 *Education in security & ethics*

2001-05-23 **information assurance education university government scholarships**

NewsScan

U.S. GOVERNMENT PLANS SCHOLARSHIPS FOR CYBER-SECURITY CORPS
The National Science Foundation has selected six universities to participate in a $8.6-million scholarship program designed to fund a "cyber corps" of 200 computer-security students who would earn graduate or undergraduate degrees in information security or a related field and agree to take government jobs upon graduating. The program would pay two years' tuition and participants would work at least one year for each year of assistance they received. Afterward they would be free to take jobs in the private sector. Participating schools include Carnegie Mellon, Iowa State, Purdue, the University of Idaho, the University of Tulsa and the Naval Postgraduate School. (Wall Street Journal 23 May 2001)
http://interactive.wsj.com/articles/SB990572871992181459.htm (sub req'd)

Category 37 *Education in security & ethics*

2001-10-08 **information security education failure weakness inadequate**

NewsScan

WULF AND SPAFFORD SAY U.S. DEFICIENT IN SECURITY RESEARCH
William Wulf, president of the National Academy of Engineering, and Eugene Spafford, director of Purdue University's Center for Education and Research in Information Assurance and Security, have a told a Congressional science committee that the nation must take serious steps to increase support for academic research on computer security techniques. Wulf said he was "appalled" at the state of security research in academia, while Spafford noted that he found that only 23 students involved in cybersecurity research have earned doctorates in the last three years. (Federal Computer Week 8 Oct 2001)
http://www.fcw.com/fcw/articles/2001/1008/web-cip-10-11-01.asp

---

Category 37 *Education in security & ethics*

2002-01-19 **human factors error efficiency effectiveness training**

RISKS 21 87

In an illustration of the importance of training for effective use of security measures, Dan Birchall reported on the introduction of speed cameras in Honolulu:

>After much debate, and general wailing and gnashing of teeth from those who like to drive fast, the powers that be here in Honolulu have a private contractor operating cameras to photograph vehicles which speed or run red lights. After the license number, time, and location of the violation are verified, a citation is mailed.

In their first day of operation, the cameras caught 927 speeders.
http://starbulletin.com/2002/01/03/news/index1.html

However, more than 80% were unenforceable due to human errors in operation of the cameras - poor aim, inaccurate location recording, etc.
http://starbulletin.com/2002/01/08/news/index4.html
<

Category 37 *Education in security & ethics*

2002-01-20 **academic education cyberterrorism infrastructure protection homeland security**

Security Wire Digest 4 5

MORE NEEDED TO GET WORKERS, STUDENTS INTO SECURITY
Congress needs to do more to encourage students and government employees to specialize in information security if cyberterrorism laws, such as the [U.S.A.P.A.T.R.I.O.T.] Act, are to succeed, say members of a network security symposium last week. Panelists at the Computing Technology Industry Association and Infrastructure Security Dialog said better trained infosecurity personnel are needed to make recently approved anti-terrorism measures work as intended. That's prompted several bills focused on security education, including the Homeland Security Education Act introduced by Sen. Richard Durbin (D-Ill.). That proposal and a similar bill for federal workers would offer financial incentives, such as fellowships and student loan repayment, to college students and government professionals who specialize in computer security.

For more information on the Homeland Security Education Act and its companion, the Homeland Security Federal Work Force Act, go to:

http://thomas.loc.gov/cgi-bin/query/C?c107:./temp/~c107iJmMdF
http://thomas.loc.gov/cgi-bin/query/C?c107:./temp/~c107gbgWnW

Category 37 *Education in security & ethics*

2002-02-07 **anti-fraud online safety security privacy education awareness Web alliance consumer protection**

NewsScan

NEW SUPPORT GROUP TARGETS PC SECURITY
A government-and-business alliance called the Stay Safe Online Campaign has established a site at http://www.staysafeonline.info to provide home and small business computer users with information about security techniques to protect themselves against network vandals. A spokesman for the group explains that individuals and small businesses "don't have the infrastructure support that people who work in large companies have at the office," and a recent study by Digital Marketing Services found that 97% of such users are vulnerable to attacks on the Internet because they fail to update antivirus software on a regular basis. (San Jose Mercury News 7 Feb 2002)
http://www.siliconvalley.com/mld/siliconvalley/2627667.htm

Category 37 *Education in security & ethics*

2002-02-14 **Internet fraud scam teenagers adolescents children ethics training education law enforcement police prevention prediction**

NewsScan

INTERNET KIDS: I WAS A TEENAGE SCAMMER
FBI agent Frank Harrill of the Los Angeles cybercrime squad says, "We have seen a rise in the crimes [Internet scams], with an increasing degree of sophistication by a younger demographic. I think it's safe to say we are going to see more of it." The use of the Internet to make fraudulent credit card purchases with stolen account numbers has become a fairly common practice. One knowledgeable observer says, "It's easy for them to pull off. A lot of teens don't take it seriously. They think it's a game." Chris Painter of the U.S. Department of Justice thinks he sees an answer to the problem: "We have to teach these kids some kind of cyberethics." (AP/USA 14 Feb 2002)
http://www.usatoday.com/life/cyber/tech/2002/02/14/net-scammers.htm

---

Category 37 *Education in security & ethics*

2002-04-22 **malware online discussion group education certification**

RISKS 22 04

Rob Slade announced a new group:

>I have created a Yahoo group for the Anti-virus Management and Protection topic, notified the CASPR people, and have apparently been accepted as the group leader. I have used the name malware in order to be somewhat more inclusive in the discussion. (I note that in CASPR viruses come under Computer Operations, whereas they appear in Applications Development in the ISC2 domains.)

The group name is CASPRmalware. To join, send e-mail to: CASPRmalware-mailto:subscribe@yahoogroups.com
or see the group home page:
http://groups.yahoo.com/group/CASPRmalware

The group e-mail address is: mailto:CASPRmalware@yahoogroups.com

This group is for discussion and preparation of the CASPR (Commonly Accepted Security Practices and Recommendations, http://www.caspr.org), Anti-virus Management and Protection document.<

Category 37 *Education in security & ethics*

2002-04-25 **university education academia security research policies scholarship**

Security Wire Digest 4 32

*COLLEGES ASKED TO MAKE CYBERSECURITY BIGGER PRIORITY
Colleges are being asked to pledge their support for better cybersecurity by making IT security a bigger priority on campus. "It's not just about protecting research going on at your (university). It's about protecting your country," said cybersecurity czar Richard Clarke last week at an IT conference focused on higher education. Clarke asked university administrators to endorse a framework that calls for more research in information security and better collaboration with government agencies. It also asks colleges and universities to better defend their own networks against attacks. The pledge request comes seven months after the National Science Foundation launched a federal scholarship program at 10 universities to encourage students to study information security. Every year of financial support must be repaid with a year of employment with the federal government.

Category 37 *Education in security & ethics*

2002-06-06 **education students technical support reliability maintenance hands-on budgets funding**

NewsScan

STUDENTS PROVIDE BULK OF TECH SUPPORT IN SCHOOLS
Fifty-four percent of U.S. schools rely on students to provide technical support for their computer systems, according to a report titled "Are We There Yet?" (http://www.nsbf.org/thereyet/index.htm), released yesterday by the National School Boards Foundation. In 43% of the 811 districts surveyed, students troubleshoot for hardware, software and other problems, and 39% of the districts, students are tasked with setting up equipment and wiring. Nearly as many districts also report that students perform technical maintenance. The fact that students are providing so much hands-on assistance is viewed as a "win-win" situation by John Bailey, director of education technology for the Department of Education. Their tech savvy helps compensate for a dearth of tech support funding in school budgets and teachers who are "unevenly prepared for using technology as a tool for teaching and learning," according to the NSBF, which reports that 69% of the survey respondents rated new teachers as average or novices in computer skills. The role reversal signals a shift in the relationship between teachers and students as online lessons become integrated into the school curriculum, says Anne Bryant, executive director of the National School Boards Association: "Teachers become the guide on the side, instead of the sage on the stage." (AP 5 Jun 2002)
http://apnews.excite.com/article/20020605/D7JV8EP00.html

Category 37 *Education in security & ethics*

2002-06-06 **security awareness posters**

Security Wire Digest 4 44

* NSA LAUCHES CYBER "SECRECY" CAMPAIGN
Powerful images of soldiers and sailors towering over the banner "Information Security Begins with You" are the cornerstone of a new National Security Agency campaign to raise infosec awareness in military ranks. With poster reminiscent of the World War II era "Loose Lips Sinks Ships" campaign, the NSA hopes the awareness program will make military personal more cognizant of the importance of preventing information--including electronic data--from reaching the hands of terrorists and foreign adversaries in the post-9/11world. "We hope to increase the awareness of military personnel to the absolute necessity of guarding sensitive information, using secure communication methods and practicing good computer security," the NSA said in an interview with AdAge.com. The posters will be distributed to military installations around the world and similar ads will appear in military publications, the NSA says.

Category 37 *Education in security & ethics*

2002-07-12 **graduate studies information assurance INFOSEC**

NewsScan

GRAD PROGRAM IN INFORMATION ASSURANCE OFFERED VIA NET
Norwich University is offering an 18-month master's degree program in Information Assurance (MSIA) intended to appeal primarily to candidates who are currently working in the information technology sector and who can consecrate an average of 12-15 hours a week to reading, online discussions, essays, and research about information technology. Because the program is carried out using asynchronous Web-based instruction, candidates from around the world are invited to apply.
http://www3.norwich.edu/msia/

Category 37 *Education in security & ethics*

2002-08-01 **criminal hackers crackers infrastructure protection infowar information warfare homeland defense education ethics**

NewsScan

HACKERS ARE GOOD, CRACKERS ARE BAD
Richard Clarke, President Bush's cybersecurity czar, sees a big difference between online vandals (also called "crackers") who hack into systems for malicious purposes, and true hackers and security professionals who explore security holes that weren't found by the software maker. In fact, Clarke regards hacking as an obligation. He's told a group of hackers: "Some of us, here in this room, have an obligation to find the vulnerabilities." (AP/USA Today 31 Aug 2002)

Category 37 *Education in security & ethics*

2002-08-21 **piracy intellectual property parents education awareness laws penalties**

NewsScan

JUSTICE OFFICIAL CALLS NET 'THE WORLD'S LARGEST COPY MACHINE'
The U.S. Justice Department is gearing up to prosecute peer-to-peer pirates, warned Deputy Assistant Attorney General John Malcolm on Tuesday. Malcolm said Americans should realize that swapping illicit copies of songs and movies is a criminal offense punishable by prison terms. "A lot of people think these activities are legal, and they think they ought to be legal," Malcolm told attendees at the Progress and Freedom Foundation's annual meeting. "There does have to be some kind of a public message that stealing is stealing is stealing, whether it's done with sleight of hand by sticking something in a pocket or it's done with the click of a mouse." A few weeks ago, some members of Congress pressured the Justice Department to invoke the 1997 No Electronic Theft (NET) Act against P2P users who swap copyrighted files without permission. Under the Act, it is a federal crime to share copies of copyrighted products, such as software, movies or music, worth more than $1,000 with anyone -- even friends or family members. Violations are punishable by one year in prison and by "not more than five years" in prison for works valued above $2,500. "Most parents would be horrified if they walked into a child's room and found 100 stolen CDs? However, these same parents think nothing of having their children spend time online downloading hundreds of songs without paying a dime," said Malcolm. Meanwhile, Gary Shapiro, head of the Consumer Electronics Association, said there should be a distinction drawn between stealing real property and copying intellectual property. "When you copy intellectual property, there may or may not be harm. They assume that every copy made is a copy lost. That's not always the case." (AP 20 Aug 2002 & CNet News.com 20 Aug 2002)
http://apnews.excite.com/article/20020821/D7LHFC182.htm
http://news.com.com/2100-1023-954591.html

Category 37 *Education in security & ethics*

2005-01-01 **eLearning prediction URL piracy RSS online courses technology advances games**

NewsScan;
http://www.elearnmag.org/subpage/sub_page.cfm?article_pk=13262&page_numbe
r_nb=1&title=COLUMN

WHAT'S UP NEXT FOR E-LEARNING?

"Colleges, universities and the military will outpace corporations in rolling out innovative and effective learning programs. Computer games will increasingly be viewed as a new type of scalable content that will raise the bar on engagement and enable new types of skills to be taught," predicts author Clark Aldrich, author of "Simulations and the Future of Learning," in a collection of expert prognostications assembled by eLearn Magazine editor Lisa Neal. Among the contributors are Don Norman, co-principle of the Nielsen Norman Group, who forecasts the rise of adult educational tools: "I expect language tutors for adults. Why not combine handheld dictionaries, phrase translators, and CD-ROM courses into a portable device?" And Indiana U. professor Curt Bonk sees a bright future for open-source courseware: "Jumping on the open-source bandwagon may mean supporting innovative pilot projects, funding code enhancements and joining the Sakai community." But as emerging technologies such as blogs, wikis and podcasts draw the attention of major commercial players like Microsoft, Yahoo and Google, look for a new bout of legal wrangling, says Canada's National Research Council's Stephen Downes: "But as grassroots technologies are appropriated for commercial objectives, conflicts over rights and use emerge, and competing standards extensions create genuine difficulties for users. Expect, for example, patent claims and threats of lawsuits over aspects of content syndication technology, lawsuits regarding unauthorized use of RSS feeds… Behind the scenes (and mostly unnoticed), the Web is beginning to fracture. Some time in the next three years the first case of URL-piracy (releasing the address of a resource without authorization) will be heard." (eLearn Magazine Jan 2005)

37.1 Elementary & middle school programs

Category 37.1 *Elementary & middle school programs*

2002-09-26 **security education children government infrastructure protection schools kids**

NewsScan

DEWIE THE TURTLE COMES OUT FOR COMPUTER SECURITY
In the tradition of Smokey the Bear's campaign for fire safety, the new cartoon figure Dewie the Turtle is being promoted by the Federal Trade Commission to teach kids and their parents of the importance of computer and network security (http://www.ftc.gov/infosecurity). Dewie urges the selection of hard-to-guess passwords, the use of antivirus software and computer firewalls, and other security practices. Do as Dewie says or you'll be sorry. (San Jose Mercury News 25 Sep 2002)

Category 37.1 *Elementary & middle school programs*

2003-11-20 **education children schools ethics cybercrime cheating parents**

St Peterburg Times <
http://www.sptimes.com/2003/11/20/Tampabay/Some_kids_turn_the_ta.shtml >

Winn Schwartau, author of many books on information warfare and of the popular new book, _Internet & Computer Ethics for Kids (and Parents & Teachers Who Haven't Got a Clue)_, was disappointed by the response of teenagers to a series of ethical challenges that were part of the Great American Teach-in in his son's school in Seminole Florida. For example, one question in the "Cyberethical Survivor Game" was, "You accidentally receive an e-mail with answers to next week's big test. Without them you could fail. No one will ever know if you peek." Although a few students strongly asserted that they would not cheat, hundreds of teenagers express their contempt for such a position. According to a report by Thomas Tobin of the St. Petersburg Times, "Boos and catcalls rained down from about 200 ... students, who made it clear during the spirited 40-minute game that they favored unfettered computer use, no parental controls and cheating."

Category 37.1 *Elementary & middle school programs*

2005-06-08 **UK Britain charity children downloading habits parent education effort pamphlet**

EDUPAGE; http://news.bbc.co.uk/2/hi/entertainment/4072566.stm

EDUCATING PARENTS ABOUT KIDS' DOWNLOADING HABITS

A British charity focused on children's issues on the Web has launched a campaign designed to educate parents about the downloading habits of their kids. According to Childnet, as many as 90 percent of parents do not understand how music can be downloaded from the Internet. The charity is producing leaflets in 8 languages for distribution in 19 countries to try to address and correct this gap of understanding between parents and children. Representatives of the entertainment industry applauded the initiative. Peter Jamieson, chairman of the British Phonographic Industry, said, "We are committed to working with parents to make them aware of the dangers of illegal downloading." Dennis Henderson of Virgin Megastores noted that spreading the word about legal download services is as important as fostering an awareness of illegal file sharing. BBC, 8 June 2005

37.2 High school programs

Category 37.2 *High school programs*

2002-09-26 **intellectual property theft piracy education awareness campaign ethics**

NewsScan

MUSIC ARTISTS SLAM DOWNLOADING
Record labels are using the talents of dozens of big-name recording stars, including Madonna, Sting and Britney Spears, in a multi-million-dollar ad campaign designed to shame people out of illegally swapping their songs. "Would you go into a CD store and steal a CD?" asks Spears. "It's the same thing — people going into the computers and logging on and stealing our music." The new ad campaign is one facet of a multipronged approach aimed at quashing illegal file-swapping. The Recording Industry Association of America has also sued several file-swapping sites, threatened to crack down on companies and individual file-swappers, and lobbied for legislation that would mandate anti-copying technology in new products. Meanwhile, a KPMG study recently released said that instead of fighting Internet piracy, the recording industry would be better served by devoting more time to developing new Internet business models. (CNet News.com 25 Sep 2002)
http://news.com.com/2100-1023-959537.html

Category 37.2 *High school programs*

2003-07-25 **hacking contest Japan cybercrime computer expertise**

NewsScan

JAPANESE GOVERNMENT SCRAPS HACKING CONTEST
Japan's Economy, Trade and Industry Ministry has canceled a national computer-hacking contest, bowing to an outpouring of angry mail and phone calls complaining that sponsoring such an event would just encourage cybercrime. The ministry said the "Security Koshien" contest was intended to foster computer expertise among high school and vocational students, and would have involved teams of students attempting to hack into opponents' systems while protecting their own from similar breaches. (AP 25 Jul 2003)

Category 37.2 *High school programs*

2005-03-21 **high school K-12 fight stop hacker hacking school network denial of service DoS attack report education**

DHS IAIP Daily; http://www.nwfusion.com/news/2005/032105−hacker−kids.html

K-12 SCHOOLS FIGHT TO STOP STUDENT HACKERS

When today's K-12 students act up, they increasingly are going high-tech by using the school's network to launch denial-of-service attacks, sending harassing e-mails or breaking into databases to try to change their records. With public schools now widely equipped with LANs and high-speed Internet access, IT administrators have to cope with many cyber incidents. Some infractions, such as attempts to get to pornography sites, might force administrators to temporarily yank a child's network access as punishment. But some types of incidents, such as hacking and e-mail threats, even end up with students being booted out of school or in trouble with the law. Philip Scrivano, management analyst at Fiscal Crisis & Management Assistance Team (FCMAT), agrees. Scrivano says that in his role as adviser, he's seen students expelled for installing a keylogger on the teacher's PC and changing grades or breaking into a server. Some troublemakers are spending inordinate amounts of time planning break-ins - sometimes 50 to 100 hours for one attack. The hard part is making teenagers understand that what they're doing is a crime. Department of Education's "Internet Access in U.S. Public Schools and Classrooms: 1994-2003" report:
http://nces.ed.gov/pubsearch/pubsinfo.asp?pubid=2005015

Category 37.2 *High school programs*

2005-04-08 **ethical hacking teaching education security awareness University of La Salle Barcelona Spain ISECOM**

EDUPAGE; http://news.bbc.co.uk/2/hi/programmes/click_online/4423351.stm

PROGRAM TEACHES HACKING TO RAISE AWARENESS

The University of La Salle in Barcelona has begun a program to raise awareness of computer hacking and to teach teens how to protect themselves. Sponsored by the Institute for Security and Open Methodologies (ISECOM), the Hacker High School invites students from local high schools to the La Salle campus to expose them to the ins and outs of hacking. Pete Herzog, managing director of ISECOM, said the program shows participants how computer hacking is accomplished so that they can understand the concepts behind what computers do, how to clean them, how applications can compromise computers, and the implications for personal privacy. According to one official from the program, the goal is to provide experiences for students to learn how hacking happens so that they will become "ethical hackers, good hackers, knowing what they do and what the limits are." School officials believe having skills as an ethical hacker could be beneficial when students go looking for jobs later. BBC, 8 April 2005

Category 37.2 *High school programs*

2006-03-11 **security education cybersecurity school program Rome NY US Air Force Research Lab**

DHS IAIP Daily; http://www.wired.com/news/wireservice/0,70396−0.html?tw=rss. Index 23

HIGHSCHOOL STUDENTS LEARN ABOUT CYBERSECURITY VIA PILOT PROGRAM.

A group of students at Rome Catholic School in Rome, NY, are learning how to become the future defenders of cyberspace through a pilot program that officials say is the first of its kind in the country. The program teaches students about data protection, computer network protocols and vulnerabilities, security, firewalls and forensics, data hiding, and infrastructure and wireless security. Most importantly, officials said, teachers discuss ethical and legal considerations in cyber security. The pilot program was developed with help from computer experts at the U.S. Air Force's Research Lab in Rome, who four years ago created a 10-week Advanced Course in Engineering Cyber Security Boot Camp for the military's Reserve Officers Training Corps, said Kamal Jabbour, the lab's principal computer engineer. The material covered in the course is subject matter that college students typically don't receive until their junior year.

Category 37.2 *High school programs*

2006-03-11 **high school program computer security education program Rome New York Syracuse University**

EDUPAGE; http://www.wired.com/news/wireservice/0,70396-0.html 23

PROGRAM TEACHES HIGH SCHOOLERS ABOUT COMPUTER SECURITY

High school students at a Catholic school in Rome, New York, are the first to participate in a computer-security course developed by the school, the U.S. Air Force's Research Lab in Rome, and Syracuse University. The 20-week course, which covers topics including data protection, network protocols and vulnerabilities, firewalls, data hiding, and wireless security, is based on a 10-week course developed at the Research Lab. Kamal Jabbour, principal computer engineer at the lab, said the new course was designed in part to encourage students to pursue college degrees and careers in computer security. Eric Spina, dean of Syracuse's engineering and computer science programs, said the program is considerably different from the kind of computer course available in many high schools today. This course, he said, exposes high school students to material not seen by many college students until their junior year. "A high school student with this kind of background," said Spina, "would be an asset anywhere they went." Starting next year, the course will be available statewide and could be offered nationally by 2008.

37.3 Undergraduate programs

Category 37.3 *Undergraduate programs*

2003-03-15 **digital forensics AS associate BSc bachelor baccalaureate online major**

http://digitalforensics.champlain.edu/

Champlain College officially approved a new major called Digital Forensics Technology. Commencing in the 2003-2004 academic year, Champlain College offers Associates of Science (A.S.) and Bachelor of Science (B.S.) degrees in Computer & Digital Forensics. This major combines aspects of computer and network technology, criminal justice, digital forensics methods, and other related fields. Individuals interested in the technical content of the Computer & Digital Forensics curriculum but who do not want to obtain a B.S. degree (such as those individuals who are pursuing a degree in another discipline or who already have a Bachelors degree) would be able to take a subset of the courses and earn a Professional Certificate. More information can be found in the program information sheet.

All of the courses for this curriculum are available on-line. For more information about the program, contact program director Gary Kessler.

Category 37.3 *Undergraduate programs*

2003-05-23 **unviersity canada calgary virus writing education malware worms trojan horses**

NIPC/DHS

May 23, Sophos — Canadian university offering course in virus-writing.

The University of Calgary in Canada is offering its students a course in malicious virus-writing this autumn. The course, titled "Computer Viruses and Malware," is described by university literature as focusing on "developing malicious software such as computer viruses, worms and Trojan horses that are known to wreak havoc to the tune of billions of dollars world-wide on an annual basis." The course professor, Dr. John Aycock, is said to have convinced the University authorities to allow virus writing to be part of the course in the belief that it will lead to a greater understanding of how to stop viruses.

Category 37.3 *Undergraduate programs*

2003-05-27 **virus course writing skills student understand hackers criminals crackers motivation**

NewsScan

VIRUS WRITING 101
The University of Calgary is drawing fire for its decision to offer a class next fall in "Computer Viruses and Malware," giving students the opportunity to perfect their virus-writing skills. Ken Barker, head of Calgary's computer science department, defends the decision, saying the class will enable students to better understand the motivations of crackers who are responsible for the proliferation of malicious attacks against corporate networks and personal computers. "Somebody who is suggesting we are doing enough really has their head in the sand," says Barker. In response to concerns that the students' work could lead to more cracking incidents, school officials say they've taken extra precautions, with plans to use a closed network and prohibitions on students removing disks from the lab, which will be secured 24 hours a day. But it's the financial consideration that likely will keep students focused on preventing viruses rather than proliferating them, says Barker. "They are not really employable as virus writers," he notes. (CNet News.com 27 May 2003)

Category 37.3 *Undergraduate programs*

2003-06-01 **Cyber Corps education Department of Defense's Information Assurance Scholarship Program stipend tuition students**

NIPC/DHS

June 01, Information Security — Cyber Corps' failing grades.

Federal administrators are overhauling Cyber Corps because conflicting policies and management structures are making it increasingly difficult to place graduates of the infosec training program in government jobs. University coordinators say getting the first 50 Cyber Corps graduates into federal jobs proved extremely difficult. Federal agencies were unwilling to hire inexperienced security admins when more senior infosec positions went unfilled. Complicating the situation is the Office of Personnel Management (OPM), which is responsible for placing students but has little authority to compel placements. Officials are still working on details, but it has already been decided to reorganize Cyber Corps based on the Department of Defense's Information Assurance Scholarship Program. The government launched Cyber Corps in 2001 under the scholarship for service model. Students receive tuition and a stipend in exchange for serving in a summer internship and working at a government agency for up to two years. Cyber Corps has distributed nearly $30 million to upgrade university infosec programs and fund scholarships for 200 students at 13 universities certified as Centers for Academic Excellence by the National Security Agency.

Category 37.3 *Undergraduate programs*

2004-01-16 **virus writing class students professor university publicity consortia industry protest ethics education**

http://chronicle.com/free/v50/i19/19a03301.htm

COLLEGE COURSE USES VIRUS-WRITING AS TOOL

A storm of criticism washed over a University of Calgary Professor in early summer of 2003 when he announced his intention to teach a fall course entitled "Computer Science 599.48: Computer Viruses and Malware." Assistant Professor John Aycock shocked the antivirus world by including his intention to have his undergraduate students write some malicious code. Many experts objected on the following grounds:

* Writing malicious code was unnecessary in teaching how viruses, worms and Trojan horses work or how to fight them;

* Keeping the malicious code contained within the class of laboratory would be difficult or impossible;

* Some students would take the wrong message home about the ethical implications of creating malicious code;

* Students with experience writing malware would be on unemployable by antivirus firms, always concerned about the widespread rumor that they engage in writing viruses for profit.

Supporters of the course scoffed at these arguments, assuring critics that the Laboratory would be well secured and insisting on the pedagogical value of such exercises. In addition, they stressed that virus writing would be only a small part of the course, which would also teach students about the history of malware, economic consequences of these programs, countermeasures, legal and ethical considerations, and wider principles of computer and network security.

After the course was over, there appeared to have been no breaches of security and University spokespersons insisted that they would offer the course again despite their critics.

Category 37.3 *Undergraduate programs*

2004-05-13 **Norwich University bachelor science computer security information assurance undergraduate**

http://www.nwfusion.com/newsletters/sec/2004/0510sec2.html

Bachelor's Program in Information Assurance

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Norwich University is proud to present a completely new Bachelor of Science in Computer Security and Information Assurance (BSIA for short). The program has been designed from the bottom up; unlike most IA undergraduate degrees, it is not an add-on to a computer science degree. Instead, the BSIA has been built to include a wide range of interdisciplinary studies that will contribute to a sound management approach to information assurance.

As part of the team that designed the program and as the program director, I was particularly concerned to complement the many find programs already in existence that focus on highly technical aspects of information assurance. Because Norwich is a small school, our division (of Business and Management) decided to emphasize our strengths. The program, unusually for IA undergraduate degrees, includes such topics as criminal law, psychology (especially social psychology), management, finance, statistics, operations management, humanities courses and technical writing as well as the expected mathematics, programming, data structures, databases, systems engineering, cryptography, and networking. There's also room for such courses as computer forensics and special research projects.

While we wait for information to be posted on our University Web site about the new BSIA and also about the revised minor in information assurance programs, I have prepared documentation and placed it online at

http://www2.norwich.edu/mkabay/bsia

On that page you will find the following documents:

* Short description of the BSIA (Major)

This one-page summary describes why you might be interested in registering for the Bachelor of Science in Computer Security and Information Assurance at Norwich University. HTM PDF

* Summary of Courses in BSIA (Major)

This one-page sheet lists all the required courses and available options in the BSIA program. HTM PDF

* Complete Rationale Justifying the BSIA

This document was prepared for the Norwich University Curriculum Committee and provides the complete background for the decision to create the BSIA program. Because of the formatting and footnotes, this document is provided only in Acrobat PDF format.

* Minor in IA

This one-page summary lists the required courses and their prerequisites for the minor in information assurance. HTM PDF

I hope that you and any students you know or counsel will find this information helpful. I'd appreciate your help in making this information known to any young people who are interested in an IA career.

Please inform me of all errors you find on the Web page and in the documents posted there so I can correct them quickly.

Category 37.3 *Undergraduate programs*

2004-07-12 **cyberterrorism battle universities academia courses degrees CyberCorps**

NewsScan

BATTLING CYBERTERRORISM

At the University of Tulsa, a program called Cyber Corps has become one of the nation's largest institutions specifically created to combat cyberterrorism. Since September 2001 the corps has grown from six universities to twenty universities. The Tulsa program and similar programs at Carnegie Mellon University, the Naval Postgraduate School, and the State University of New York at Stony Brook have received large new grants from the National Science Foundation. [The leaders at the Naval Postgraduate School are professors Dorothy Denning and Peter Denning, special friends of NewsScan.] (AP/San Jose Mercury News 12 Jul 2004)

Category 37.3 *Undergraduate programs*

2004-07-20 **IBM assistance colleges universities course development Java DB2 J2EE technology**

NewsScan

IBM OFFER OF ASSISTANCE TO UNIVERSITIES

IBM is offering free access to IBM software and course-development assistance to any university interested in broadening its curricula, in a move designed to ensure that computer-science programs will teach students about open-source software such as Linux and Sun's J2EE and Java languages as well as IBM's proprietary DB2 database and WebSphere Internet software. IBM said it was "getting strong signals from schools that they want an alternative to Microsoft"; Kevin Schofield of Microsoft Research University relations admitted generously: "Anyone who focuses on just one technology is doing themselves a disservice." (Wall Street Journal 20 Jul 2004)

Category 37.3 *Undergraduate programs*

2004-08-08 **computer science engineering major college university academia technology study**

NewsScan

DECLINING NUMBERS OF COMPUTER SCIENCE MAJORS

The Computing Research Association says that the number of newly declared computer science and computer engineering majors in the U.S. and Canada fell last year 23% from the year before. The explanation is fairly straightforward: since the dot-com bust a computer science degree no longer seems the key to instant riches. But Peter Lee, an associate dean of computer science at Carnegie Mellon University, is unworried by the falloff in applications: he thinks today's students are often of higher quality, because they're motivated not by money but by love of technology. (USA Today 8 Aug 2004)

Category 37.3 *Undergraduate programs*

2004-10-13 **National Security Agency NSA information assurance roadmap IA curriculum program colleges**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/27627−1.html

October 13, Government Computer News — NSA: Global grid will have data assurance.

The National Security Agency (NSA) is revising its two-month-old, 2,200-page information assurance (IA) roadmap for the Defense Department's Global Information Grid (GIG), NSA's Daniel G. Wolf said Thursday, October 13, at the Microsoft Security Summit East in Washington. After incorporating feedback from government and industry, NSA will release a three-phase architectural plan for secure worldwide data sharing among and across military and intelligence agencies over the next two decades. It spells out no specific solutions at this point, but it will ensure that IA is "baked in" by authenticating credentials, security clearances, roles and situational awareness throughout the GIG, he said. NSA has also recruited 59 colleges and universities to set up an IA curriculum and teach safe programming practices. The Homeland Security Department has joined the Defense Department as a joint sponsor of the IA curriculum program.

Category 37.3 Undergraduate programs

2005-02-02 **college online education fraud Department Education diploma mills online fraud**

NewsScan; http://www.wired.com/news/culture/0

DATABASE DOCUMENTS DIPLOMA MILLS

The U.S. Department of Education has launched a searchable database that prospective online students may browse to determine whether a particular distance learning institution is accredited by organizations sanctioned by the government. The white-list enables students and prospective employers to distinguish between Hamilton College, a small, distinguished (and accredited) New York college, and Hamilton University, a diploma mill in Wyoming. And while Hamilton University is licensed by the state of Wyoming, using a degree from that school for employment in other states, such as Oregon or New Jersey, could lead to jail time for fraud. The database was created following calls for action from Congress last year, after some high-level government officials were discovered to have purchased questionable degrees to beef up their resumes. (Wired.com 2 Feb 2005)

Category 37.3 *Undergraduate programs*

2005-02-06 **academic university course spyware spam ethics**

RISKS 23 70

UNIVERSITY OF CALGARY TEACHES STUDENTS TO WRITE MALWARE

Rob Slade comments on the University of Calgary's penchant for teaching students how to write malicious code:

The University of Calgary is back at it again.

Http://www.cbc.ca/story/canada/national/2005/02/05/email-course050205.html
http://pages.cpsc.ucalgary.ca/~aycock/
aycock@cpsc.ucalgary.ca, barker@cpsc.ucalgary.ca

(Interesting that his homepage is entitled "Unfettered by Content." He certainly seems to be unfettered by logic.)

This time they are adding spam and spyware to the curriculum.

I can vaguely see a dim advantage to having students write viruses in order to understand them (rather inefficiently, in terms of time spent), but getting them to write a spamming program in order to understand how to fight spam seems even less effective.

As previously noted, John Aycock doesn't seem to have any credentials in security or malware (no papers published prior to the virus course, nobody in the field seems to know him), so why he, and the university, chose to do this, other than pure self-promotion, is completely beyond me.

I am somewhat relieved by the fact that the paper submitted to EICAR shows that a modicum of thought was given to the security of the laboratory. The irrelevance of the measures undertaken is no great surprise. The bibliography is interesting: Lugwig's second edition is there, along with Mitnick's "19 chapters of gotcha," but on the AV side Cohen's 1994 edition stands alone with Skoudis' rather pathetic work. I would have thought that anyone with even a pretence of academic intentions would have consulted Ferbrache, and possibly Nazario's pompous but flawed attempt at worm analysis. Given Aycock's involvement in a rather banal crypto lab, I'm a bit surprised that he hasn't tried to create Young and Yung's proposed crypto-nasties.

In a follow-up response in RISKS 23.71, someone called "Hendrik" retorted that studying malware is essential for development of effective countermeasures. Some of his comments follow:

>….In 1992 I found a small book in a bookstore in Saudi Arabia, that had been published by the German "Kaos Computerclub". In this book the authors explained how viruses worked, from an angle of approach of how to write viruses (at that time we had to deal mostly with DOS boot sector viruses). The authors further described how they had approached major software companies with this information, none of whom was the least bit interested in the information or in any cooperation with people who knew how to write viruses. Some of the approached companies had furthermore warned the authors against publishing the information about viruses they had on hand.

I am not impressed, to say the least, that 13 years after the Kaos Computerclub had the right idea, in a world awash in viruses, worms, and spam, with a world-wide deployed home computer OS that seems to have less security than the front door of my house, we still have not made any progress in regards to how we deal with knowledge about malware.

In the the CBC article that Rob Slade refers to, Aycock (the "virus teacher" at UofC) is quoted as saying "[S]ome companies have said they're not going to hire [our] graduates because they don't like the perception of having someone on board who has written viruses."

Well, I imagine reading the following in Time Magazine: "The White House official said, 'We are not going to hire body guards who have been trained at school X because we don't like the perception of having someone on staff who has been trained to kill.'" Would you forgive me for laughing?

Rob Slade further writes: I can vaguely see a dim advantage to having students write viruses in order to understand them (rather inefficiently, in terms of time spent), but getting them to write a spamming program in order to understand how to fight spam seems even less effective.

Not all approaches to learning something are equally effective, and in an area where something is being pioneereed, the first steps may not be quite in the right direction or not as effective as future approaches. But that alone is not a good reason to abolish a certain curriculum. My question would be "What would make this training more effective?"

….I hope one day we will see malware courses in all university computer science programs - then I would have reason to be more optimistic that the "security mess" we are finding ourselves in might be cleaned up. Creativity, more than anything else, is what we need to deal with the future, and anybody who fosters and harnesses such creativity has my vote.<

Matthew Holmes pointed out in RISKS 23.71 that contrary to Slade's dismissive comments, Aycock does in fact publish technical articles:

>I did survey Aycock's professional literature, much of which is available on-line, and I notice that a great deal of it centers on reverse-engineering methodology, compiler/parser theory, etc. These are in fact the tools of the virus writer - the real ones, not the script kiddies and buffer-overflow people.<

Category 37.3 *Undergraduate programs*

2005-02-08 **University Calgary course spam spyware viruses malicious code ThreatLab grades prosecution**

EDUPAGE; http://software.silicon.com/security/0,39024655,39127703,00.htm

UNIVERSITY OF CALGARY OFFERS COURSE ON SPAM, SPYWARE

The University of Calgary, which gained attention in 2003 when it began offering a course on writing viruses, has now introduced a course devoted to writing spyware and spam. Although the virus-writing course prompted strong criticism, response to the new offering has been warmer. Some members of the computer-security community noted that such a course could give students a strong understanding of how to combat malicious computer code in practice. "If we're looking for an engineer to [fight] spam, then we'd rather have somebody who has already been taught about these things and who knows how they work," said Steve Purdham, CEO of SurfControl. Mark Murtagh of Websense echoed those comments. He compared computer security to a game of chess, saying, "You need to be completely up to date on what's available to ensure you understand your opponent's potential next move." Pete Simpson, ThreatLab manager at Clearswift, disagreed, however, saying that such arguments "really [fall] flat for spamming tools." He said the course will tempt students to put their skills to harmful use. Students who do so risk failing grades and prosecution, according to the university.

Category 37.3 *Undergraduate programs*

2005-02-16 **software vendor quality assurance blame college security education secure programming responsibility NSA DoD**

DHS IAIP Daily;
http://news.com.com/Software+firms+fault+colleges+security+e ducation/2100−
1002_3−5579014.html

SOFTWARE FIRMS FAULT COLLEGES' SECURITY EDUCATION.

In a panel session Tuesday, February 15, at the Secure Software Forum in San Francisco, Oracle, Microsoft and other software makers attempted to analyze why flawed software is still overwhelmingly the rule and not the exception in the industry. A major contributor, the companies said, is college students' lack of a good grounding in secure programming. Many software makers believe that better training of computer science graduates is a key step toward improving software quality, but some security researchers have criticized the industry, pointing out that industry demand for programmers generally does not give preference to those trained in secure programming. To influence curricula, private industry has established scholarships at universities. Also, several federal agencies, including the Department of Defense and the National Security Agency, have named several college programs as National Centers of Academic Excellence in a variety of security disciplines. However, some panel members laid the blame for the problems squarely at the feet of software makers. Until companies are willing to foot the bill for security, applications will not get better, said Fred Rica, a partner in PricewaterhouseCoopers' Threat and Vulnerability Assessment Services.

Category 37.3 *Undergraduate programs*

2006-04-18 **National Security Agency NSA Cyber Defense Exercise CDX US Naval Academy network security test**

DHS IAIP Daily; http://www.news.navy.mil/search/display.asp?story_id=23208 23

NATIONAL SECURITY AGENCY SPONSORS CYBER DEFENSE EXERCISE

The U.S. Naval Academy joined forces with fellow service academies in the sixth annual Cyber Defense Exercise (CDX) held Monday-Friday, April 10-14, at the Academy in Annapolis, MD. Sponsored by the National Security Agency, CDX brings Midshipmen and their peers together to create a computer network they must then defend against attack from hackers. The service academy that best defends its portion of the network from attack wins the competition. Results will be announced between late April and early May. The hackers in the exercise tested the security of the network, observed how long it took the students to become aware of the attacks, and assessed how they responded.

37.4 Master's programs

Category 37.4 Master's programs

2003-04-23 **cyberspace war games Internet warfare education US military academies**

NIPC/DHS

April 18, Monterey Herald — Cyberspace games teach real world lessons.

On Thursday, 39 students at the Naval Postgraduate School (NPS) ended four days of mock Internet warfare that pitted a team made up of NPS, the Air Force Institute of Technology, and the U.S. Military, Naval, Air Force, Coast Guard and Merchant Marine academies against a team made up of the Army's Land Information Warfare unit and the Air Force's 92nd Aggressor Squadron. The object of the exercise is for each side to try to penetrate the other's computer systems, aiming to infect them with viruses, shut them down or take them over. The mock war in cyberspace draws students "who are interested in what a real-world situation is," said Marine Corps Capt. Eric Walters who led the Navy school team this year. Some of the team members are military officers enrolled in various information technology classes, others are civilians enrolled in the National Science Foundation's federal Cyber Service Corps scholarship program, which began in 2001. That program offers a two-year, full-ride scholarship in a computer science master's degree program aimed at safeguarding computer systems. Graduates are expected to serve two years with a U.S. government agency as specialists in safeguarding computer systems.

Category 37.4 Master's programs

2005-12-13 **online Internet higher education e-learning for-profit seven times music industry**

EDUPAGE; http://chronicle.com/daily/2005/12/2005121305n.htm

ONLINE EDUCATION BOOMING

Analysts speaking at a conference on the business of higher education this week argued that the market for online learning, though often downplayed relative to other topics, is thriving and represents the future of for-profit education. Online music, for example, receives a lot of hype in the media, according to one analyst, but the market for online education is seven times larger than that for online music. Douglas L. Becker, CEO of Laureate Education Inc., which operates a network of international universities, said that in many parts of the world the demand for higher education far outstrips the supply. Moreover, while for-profit colleges enroll less than 5 percent of all college students, more than a third of all students taking an online course are enrolled at a for-profit institution. The conditions are ripe for online education to lead to significant growth in for-profit colleges in the coming years, according to analysts. Chronicle of Higher Education, 13 December 2005 (sub. req'd)

Category 37.4 Master's programs

2006-04-17 **University of Pennsylvania graduate students NSF grant telephone wiretap quality research network security**

DHS IAIP Daily; http://www.gcn.com/online/vol1_no1/40428−1.html 23

UNIVERSITY OF PENNSYLVANIA STUDENTS RESEARCH WIRETAP VULNERABILITIES.

A team of graduate students from the University of Pennsylvania working with a National Science Foundation grant set out to determine just how trustworthy the most common types of telephone wiretaps used by police and intelligence agencies are, said Professor Matt Blaze. The results of these taps are accepted uncritically by courts, Blaze said at the 2006 International Conference on Network Security being held in Reston, VA. “It turns out, it can fail in all sorts of unexpected ways,” he said. The techniques exploit vulnerabilities in the single signaling and audio channel used in analog telephone systems. Blaze said the project was an attempt to establish some baselines for network security by assessing how easy it is to conduct reliable eavesdropping on the century-old protocols used in analog voice phone systems.

37.5 Doctoral programs

Category 37.5 *Doctoral programs*

2004-12-13 **US universities science engineering doctorates increase NSF 2004**

DHS IAIP Daily;
http://news.com.com/Science%2C+engineering+Ph.D.+numbers+buck+downturn/2100−1008_3−5489359.html?tag=nefd.top

December 13, CNET News — Science, engineering PhD numbers rise.

U.S. universities awarded 25,258 science and engineering doctorates from July 1, 2002, to June 30, 2003, according to data published this month by the National Science Foundation (NSF). That's a 2.8 percent rise from the 24,571 doctorates awarded the previous year, reversing a downward trend that began after a 1998 peak of 27,278. Production of science and engineering doctorates in the United States is seen by some as vital to the country's technological leadership, given the way fundamental research can translate into new products and even industries. A more recent worry centers on a decline in enrollment of international graduate students in the United States. Foreigners historically have earned a large percentage of technology-related doctorates. According to NSF data, foreign students with temporary visas comprised 55 percent of the 5,265 engineering PhDs last year. Not everyone thinks the number of PhDs awarded is critical to the country's global competitiveness. Some observers argue that the country already has plenty of doctorates and that a drop in foreign students isn't cause for alarm.

37.7 Conferences

Category 37.7 Conferences

2004-05-17 **broadband access social implications**

DHS IAIP Daily; http://www.itu.int/newsroom/press_releases/2004/12.html

May 17, ITU Press Release — Global support for information society targets.

Targets set for improving access and connectivity to information and communication technologies (ICT) by 2015 at the first phase of the World Summit on the Information Society (WSIS) have received strong support in a global International Telecommunication Union (ITU) survey. The Summit approved a Declaration of Principles and Plan of Action that set forth a roadmap to bring the benefits of ICT to underserved economies. The Summit was organized by ITU under the patronage of UN Secretary-General Kofi Annan to ensure that social and economic development, which is increasingly driven by ICTs, will result in a more just, prosperous and equitable world. The survey shows overwhelming support for the belief that if the information society is to be one in which all citizens throughout the world can equally access and use information resources for sustainable economic and social development, that cyberspace should be declared a resource to be shared by all for the global public good. This opinion was held by more than 94% of survey respondents.

Category 37.7 Conferences

2004-10-12 **India US cybersecurity talks New Delhi security conference intellectual property rights laws discussion**

DHS IAIP Daily; http://abcnews.go.com/Business/wireStory?id=158551

October 12, Associated Press (India) — India, U.S. experts discuss cybersecurity cooperation.

At a New Delhi security conference, U.S. Under Secretary of Commerce Kenneth Juster urged India to tighten its laws to protect intellectual property rights and ensure that sensitive information stays out of the hands of tech-savvy criminals. Juster said India must protect the privacy of personal and financial data as an increasing number of American companies rely on Indians to handle their technical operations and other software work. He cited Europe's efforts as a good example.

Category 37.7 Conferences

2004-10-21 **hacker technology fair Italy security privacy implications**

DHS IAIP Daily;
http://www.reuters.com/audi/newsArticle.jhtml?type=technologyNews&storyID=6572719

October 21, Reuters (Milan, Italy) — Beat hackers and learn to spy at Italy tech fair.

Fingerprint sensors, gadgets to pry open doors and transmitters to spy on unsuspecting targets were among the wizardry on show at the opening of Italy's biggest technology fair on Thursday, October 21. This year a large chunk of the fair was devoted to security in its forms reflecting a growing fear of crime and militant attacks. One of the most popular exhibitors was a company called Global System from the tiny city-state of San Marino teaching people how to spy. Global System offers clients tools to pick locks as well as micro transmitters hidden in watches, baseball caps and phones.

Category 37.7 *Conferences*

2005-03-17 **Cellular Telecommunications Internet Association CTIA Wireless 2005 homeland security cooperation**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/recover y/story/0,10801,100458,00.html

CTIA: EXPERTS CALL FOR HOMELAND SECURITY, WIRELESS INDUSTRY COOPERATION

To bolster the value of wireless voice and data communications for U.S. homeland security purposes, industry and government officials need to work closer together, security experts at Cellular Telecommunications & Internet Association (CTIA) Wireless 2005 said last week. The consensus among experts from the Federal Communications Commission and Department of Homeland Security who took part in a panel discussion was that wireless technologies have improved since the September 11, 2001, terrorist attacks. But they said much remains to be done to set up effective warning systems in the event of a terrorist or natural disaster and to improve interoperability of wireless devices for emergency responders. The toughest issue for police, firefighters and other emergency responders may be the widespread lack of interoperability between public safety networks and devices, experts said. Several panelists called for development of emergency warning systems to notify a large group of people of an emergency, similar to one county officials use in Arlington, VA. That system is used by police and fire officials to call residents over wired or wireless phones, or the Internet, to warn them of traffic disasters or crimes. CTIA: http://www.ctia.org

---

Category 37.7 *Conferences*

2005-03-21 **information technology IT physical perimeter security manager responsibility Business Continuity Expo London**

DHS IAIP Daily; http://news.zdnet.co.uk/internet/security/0,39020375,3919183 9,00.htm

PHYSICAL SECURITY BECOMING AN IT PROBLEM.

The proliferation of technologies such as identity management mean more IT managers are having to take responsibility for physical security, according to a panel of leading IT security managers. Speaking at the Business Continuity Expo in London's Docklands, IT security experts from the Royal Mail Group, Proctor & Gamble and Barclaycard acknowledged that their companies are increasingly merging systems used to authenticate employees' entry to physical facilities with those used to control access to computing resources. David McCaskill, manager for global security solutions at Proctor & Gamble, explained that the pharmaceutical giant had also integrated its physical and IT authentication systems. "Before, if you forgot your passcard to access the building that wasn't a major problem, but now it is." Companies have generally treated physical security as the responsibility of the facilities department and computer security as that of IT. But employee information has increasingly become integrated, allowing businesses to link the two systems, said Steve Hunt, an analyst with Forrester Research.

Category 37.7 *Conferences*

2005-11-25 **Iowa State University Cyber Defense competition network security skills practice**

DHS IAIP Daily; http://www.iowastatedaily.com/media/paper818/news/2005/11/18 /News/Students.Fight.It.Pros.In.Hacker.Competition−1110048.s html?norewrite&sourcedomain=www.iowastatedaily.com

STUDENTS FIGHT IT PROS IN HACKER COMPETITION

Students at Iowa State University competed in the university's second-annual Cyber Defense Competition on Friday, November 18 through Saturday, November 19. During the event, several student teams competed against a group of Internet technology professionals whose job it is to hack into and disrupt each team's network. Thad Gillispie, a graduate student in electrical and computer engineering, said that the students had a chance to see what they really know about network security as well as learn more. It also provides the students with an opportunity to see Internet security from a point of view that is not often represented and helps them start to appreciate Internet services being there when they want them, Gillispie said.

37.8 Web sites

Category 37.8 Web sites

2004-05-25 **government Websites Web content posting schedule**

DHS IAIP Daily; http://fcw.com/fcw/articles/2004/0524/web−web−05−25−04.asp

May 25, Federal Computer Week — Agencies to inventory Web info.

By the end of the year, agencies are expected to have an inventory and posting schedule for information they plan to publish online. The requirement is part of draft recommendations released in April by the Web Content Standards Working Group of the Interagency Committee of Government Information (ICGI), which outlines standards for common information that should be on all federal Web sites to make them more user-friendly. By December, agency officials must make the schedules available for public comment, said Sheila Campbell, co-chairwoman of the working group. "We're hoping this guidance gets out soon" to help agency officials to comply with this recommendation, Campbell said at the FedWeb conference in Arlington, Va. "It's going to take a little bit of effort here." By next month, OMB officials expect to recommend ways to establish a public domain directory and policies to improve agencies' repositories for research and development funds, Womer said. By the end of the year, OMB officials hope to recommend standards for categorizing and indexing government information.

Category 37.8 Web sites

2005-02-15 **privacy technology society audio commentary awareness**

RISKS 23 72

"THE MOTHER IS BACK!" ANNOUNCING "DAYTHINK" AUDIO FEATURES

Lauren Weinstein of the Privacy Forum wrote:

Greetings. I'm pleased to announce "DayThink" -- a new series of very brief (one-minute) MP3 audio features illuminating a wide range of relevant and important topics. Each day's feature will focus on one specific issue affecting our lives -- issues definitely worth thinking about. Many of these segments will deal directly with the impacts of technology on individuals and society.

DayThink features can be accessed via the DayThink main page at:
http://daythink.vortex.com

The debut segment is titled: "The Mother is Back!"

and looks at the current round of telecom mergers and what they may mean for us all.

A notification mailing list has been established that will send out a brief message to subscribers as each new feature becomes available (never more than one per day), including the segment title, a brief description, and a link to the feature audio itself that can be played at one's leisure.

Subscriptions to that list can be established via:
http://lists.vortex.com/mailman/listinfo/daythink

or by simply sending a note (no subject or body necessary) to: daythink-subscribe@vortex.com

I hope that these features will be of some value in helping folks wade through the maze of many important issues.

Thanks very much.

Lauren Weinstein
lauren@pfir.org
lauren@vortex.com
lauren@privacyforum.org
1 818-225-2800
http://www.pfir.org/lauren
Fact Squad - http://www.factsquad.org

Category 37.8 *Web sites*

2005-05-19 **privacy data theft confidentiality breaches personal information control databases summary**

RISKS 23 88

PRIVACY JOURNAL LISTS DATA LEAKAGE & DATA THEFTS IN 1Q2005

Robert Ellis Smith, publisher of the _Privacy Journal_, published a summary of some of the major losses of control and confidentiality in the first quarter of the year 2005:

To appreciate THE CUMULATIVE EFFECT, Privacy Journal newsletter in its May issue compiled the following list of breaches of sensitive personal information, disclosed just since January. It's not an atypical list for a three-month period, but breaches are obviously getting more press attention.

* Tepper School of Business at Carnegie Mellon University reported that a hacker had access to Social Security numbers and other sensitive personal information relating to 5000 or more graduate students, staff, and alumni. Another department at the university is responsible for receiving complaints of Internet breaches and solving them.

* Tufts University notified 106,000 alumni, warning of "abnormal activity" on its fund-raising computer system listing names, addresses, phone numbers, and, in some cases, Social Security numbers and credit-card account numbers.

* ChoicePoint, the insurance and employment investigative company and "information broker" based in Georgia, sold personal data on from 100,000 to 500,000 or more persons to fraud artists posing as legitimate businesses. (Still, the State of California plans to award a $340,000 contract to the Equifax-created company to gather information on suspected criminals and terrorists, according to The Sacramento Bee.)

* DSW Shoe Warehouse experienced a hacking incident involving access to an estimated 1.4 million credit-card numbers and names, 10 times more than investigators estimated at first, as well as driver's license numbers and checking-account numbers from 96,000 transactions involving other customers.

* A computer system breach at an unnamed retailer involved at least 180,000 customers, perhaps more. HSBC North America, which issues GM's MasterCard, urged all customers to replace their cards as quickly as possible because the personal data was compromised. The Wall Street Journal identified the retailer as Polo Ralph Lauren Corp., but the company insisted that in fact no information was leaked, although a computer flaw was discovered and fixed.

* Ameritrade Holding Corp., the online discount broker, informed about 200,000 current and former customers that a back-up computer tape containing their account information was lost when a package containing the data was damaged during shipping.

* Canadian Imperial Bank of Commerce, CIBC, one of Canada's leading banks, "failed to recognize" that misdirected confidential faxes sent to outside parties over a three-year period were a breach of customers' privacy that could have been prevented, according to a finding by the federal Privacy Commissioner in Canada. Bank of Montreal, Royal Bank of Canada, Scotiabank, TD Bank, and National Bank have also misdirected faxes with customer information.

* Motor vehicle departments in four states have lost personal data. The Texas Department of Public Safety mailed to 500 to 600 licensed drivers renewal documents that pertained to other persons. In March, burglars rammed a vehicle through a back wall at a Nevada Department of Motor Vehicles facility near Las Vegas and drove off with files on about 9000 people, including Social Security numbers. In April police arrested 52 people, including three examiners at the Florida Department of Motor Vehicles, in a scheme involving the sale of more than 2000 fake driver's licenses. Also, Maryland police arrested three people, including a DMW worker there, in a plot to sell about 150 fake licenses.

* A Boston-based storage company named Iron Mountain Inc., lost Time Warner Inc.'s computer back-up tapes with Social Security numbers and names of 600,000 current and former employees and dependents. This is the fourth time this year that Iron Mountain has lost tapes during delivery to a storage facility, according to The Wall Street Journal.

* Someone gained access to the personal information of 59,000 current, former, and prospective students at California State University, Chico, the university revealed in March.

* A laptop that contains about 100,000 Social Security numbers of students and personnel at the University of California, Berkeley was stolen from the school's campus.

* Someone hacked into a database at the Kellogg School of Management at Northwestern University, possibly exposing data pertaining to 21,000 individuals at Northwestern.

* More than 1600 parents discovered in January that records in the Colorado State Health Department relating to an autism study were lost. A laptop computer left in a health department employee's automobile was apparently stolen last October.

Mr Ellis kindly added this invitation:

A free copy of the current issue of Privacy Journal is available through < mailto:orders@privacyjournal.net >. Specify e-mail copy or hard copy (and include a mailing address).

Category 37.8 *Web sites*

2005-09-06 **Web application design security programming training education hands-on online free download**

RISKS; http://www.owasp.org/software/webgoat.html 24 04

WEBGOAT 3.7 - APPLICATION SECURITY HANDS-ON LEARNING ENVIRONMENT

The *only* way to learn application security is to test applications "hands on" and examine their source code. To encourage the next generation of application security experts, the Open Web Application Security Project (OWASP) has developed an extensive lesson-based training environment called "WebGoat".

WebGoat is a lessons based, deliberately insecure web application designed to teach web application security. Each of the 25 lessons provides the user an opportunity to demonstrate their understanding by exploiting a real vulnerability. WebGoat provides the ability to examine the underlying code to gain a better understanding of the vulnerability as well as provide runtime hints to assist in solving each lesson. V3.7 includes lessons covering most of the OWASP Top Ten vulnerabilities and contains several new lessons on web services, SQL Injection, and authentication.

WebGoat 3.7 is available for free download from: < http://www.owasp.org/software/webgoat.html >.

Simply unzip, run, and go to WebGoat in your browser to start learning.

The OWASP Foundation is dedicated to finding and fighting the causes of insecure software. Find out more at < http://www.owasp.org >.

Category 37.8 *Web sites*

2006-01-29 **quality assurance QA spreadsheet errors education awareness training**

RISKS 24 16

SITE LISTS SPREADSHEET ERRORS

Gene Wirchenko reported on a site that lists signficant errors in spreadsheets:
< http://www.eusprig.org/stories.htm >. The site is managed by the European Spreadsheet Risks Interest Group (EuSpRIG); their description reads, "These stories illustrate common problems that occur with the uncontrolled use of spreadsheets. We say how we think the problem might have been avoided. An obvious form of risk avoidance is simply to check your work before sending it out. For important spreadsheets, a second pair of eyes ('peer review') is even better. Where stakes are high, a thorough test and audit is a further defence." The group runs an annual conference that concentrates on quality assurance for spreadsheets.

Category 37.8 *Web sites*

2006-02-28 **Symantec Internet Threat Meter release state of security**

DHS IAIP Daily; 23
http://news.com.com/Symantec+keeps+weather+eye+out+for+Net+threats/2100−7349_3−6043873.html?tag=cd.top

SYMANTEC LAUNCHES FREE THREAT METER.

Symantec on Tuesday, February 28, launched the Symantec Internet Threat Meter, a free service meant to inform consumers about the state of Internet security. "There are other threat indicators on the Web," Dave Cole, a director at Symantec Security Response, said. "But what was missing was a place for consumers that breaks it down in plain English and gives actionable advice." Available on the Symantec Website, the new threat meter will provide information on the current risk level associated with specific online activities: e-mail, Web surfing, instant messaging and file-sharing. Symantec Internet Threat Meter: http://www.symantec.com/avcenter/home_homeoffice/index.html

---

Category 37.8 Web sites

2006-03-01 **virus world map release F-Secure online tool**

DHS IAIP Daily; http://www.f−secure.com/news/items/news_2006030101.shtml 23

NEW F-SECURE WORLD VIRUS MAP OFFERS CURRENT GLOBAL PERSPECTIVE AT A GLANCE.

F-Secure has launched a comprehensive online tool for those interested in understanding the world virus situation at a glance. The resource, which was developed for research purposes at F-Secure is now available to the general public in four languages, respectively English, French, German and Finnish. F-Secure World Map: http://worldmap.f-secure.com/vwweb_1_2/en/previous_day

---

Category 37.8 Web sites

2006-03-15 **SiteAdvisor spyware quiz categories adware**

DHS IAIP Daily; 23
http://www.techweb.com/wire/security/181504133;jsessionid=NWEB3IBSWCXDGQSNDBCSKHSCJUMEKJVN

QUIZ REVEALS SPYWARE CHICANERY.

Security vendor SiteAdvisor unveiled an online quiz Wednesday, March 15, that tests consumers' ability to spot sites hosting spyware and adware. Dubbed "Spyware Quiz" by SiteAdvisor, the 12-URL test covers five categories of sites notorious for distributing adware and spyware, including those dedicated to screensavers, smileys (emoticons), games, musical lyrics, and file sharing. SiteAdvisor's spyware quiz: http://www.siteadvisor.com/quizzes/spyware_0306.html

---

Category 37.8 Web sites

2006-03-27 **Microsoft public bug database Internet Explorer IE feedback open disclosure**

DHS IAIP Daily; http://news.zdnet.co.uk/software/applications/0,39020384,39259531,00.htm 23

MICROSOFT CREATES PUBLIC BUG DATABASE FOR INTERNET EXPLORER.

Microsoft is for the first time encouraging people to give public feedback on Internet Explorer (IE), with the creation of a bug database for the next version of its browser, IE 7 beta. The bug database is accessible from the Microsoft Connect site and can be accessed by anyone that has a Microsoft Passport account.

37.9 White papers

Category 37.9 *White papers*

2003-06-06 **SQL Slammer Code ATM worm educate**

NewsScan

PUBLISHING THE SQL SLAMMER CODE: TRAINING OR EDUCATION?
Wired magazine has decided to include the code of the SQL Slammer worm to educate its readers on how worms work and how they cause damage. (SQL Slammer shut down Internet service providers in South Korea, disrupted plane schedules, and jammed ATM bank machines.) Symantec security director Vincent Wheeler warns that the publication of such code is "something you need to be cautious of, particularly in a broad-based magazine. You need to be aware of your audience and what you're saying to them." Blaise Zerega, Wired's managing editor, says that "the people who are in a position to wreak havoc on the Internet don't have to read about it on Wired." (Reuters/USA Today 6 Jun 2003)

Category 37.9 *White papers*

2005-05-09 **National Institute of Standards and Technology NIST report cryptographic key management recommendation draft**

DHS IAIP Daily; http://www.fcw.com/article88818−05−09−05−Web

NIST RELEASES REPORT ON CRYPTOGRAPHY KEYS

National Institute of Standards and Technology (NIST) officials have some advice for managing cryptographic keys. NIST recently released a draft document, "Draft Special Publication 800-57: Recommendation for Key Management," that is now available on the agency's Website for public review and comment. Poorly managed keys can easily compromise even the strongest cryptographic algorithms, according to the document written for systems administrators and software developers. The two-part document classifies cryptographic key types, their uses and the methods for protecting each type. Part 1: http://csrc.nist.gov/publications/drafts/draft-800-57-Part1- April2005.pdf Part 2: http://csrc.nist.gov/publications/drafts/draft-800-57-Part2- April2005.pdf

---

37.A Books

Category 37.A *Books*

2006-01-29 **software quality assurance QA textbook**

RISKS 24 16

GARY MCGRAW ON SOFTWARE SECURITY

Gary McGraw (2006). Software Security: Building Security In.
Addison-Wesley (ISBN 0-321-35670-5)

This book is a "hands-on, how-to guide for software security" for software security professionals. It completes a trilogy together with McGraw's Building Secure Software (Addison-Wesley, 2001) and Exploiting Software (Addison-Wesley, 2004), but it also stands alone as a useful book. It considers best practices for software security in detail, as a fundamental part of the development lifecycle. It is very much in the spirit of what RISKS has promulgated in the past 20.5 years.

[Review by Peter G. Neumann]

38 Consumer/employee / individual privacy, profiling & surveillance (non-governmental)

Category 38 *Consumer/employee / individual privacy, profiling & surveillance (non-govern*

1997-10-01 **privacy crypto law key escrow recovery policy**

RISKS 19 41

Bruce Schneier and Dave Banisar published their new book on electronic privacy issues. Schneier, B. & D. Banisar (1997). _The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance_. John Wiley & Sons (New York). ISBN: 0-471-12297-1; 747 pages. See <http://www.counterpane.com/privacy.html> for details.

Category 38 *Consumer/employee / individual privacy, profiling & surveillance (non-govern*

1997-11-09 **book privacy laws confidentiality**

RISKS 19 45

Philip E. Agre and Marc Rotenberg published a new book entitled _Technology and Privacy: The New Landscape_ (MIT Press, 1997) ISBN 0-262-01162-x. vi + 325 pp. Peter Neumann, the RISKS moderator, praised the work, writing, "This is a remarkably comprehensive and provocative collection of essays. . . . The analysis is generally penetrating and informative, and fundamental to the interactions and tensions between the steadily advancing information technology and the corresponding risks to privacy."

Category 38 *Consumer/employee / individual privacy, profiling & surveillance (non-govern*

1998-03-01 **privacy Web FTC government law**

EDUPAGE

In February 1998, the FTC began an investigation of 1,200 commercial Web sites to compile a profile of US privacy policies on the Web. A separate project was planned to compare the Web sites's actual performance on privacy with their stated policies.

Category 38 *Consumer/employee / individual privacy, profiling & surveillance (non-govern*

2000-01-12 **privacy book review study survey overview**

EPIC Alert; NetworkWorld Fusion

Respected author Simson Garfinkel published his new book, _Database Nation: The Death of Privacy in the 21st Century_ and received rave reviews from privacy activists. The Electronic Privacy Information Center (EPIC) published this brief summary in the EPIC Alert 7.01: "Fifty years ago George Orwell imagined a future in which privacy was vanquished by a totalitarian state that used spies and video surveillance to maintain control. In 2000 we find that the threats to our privacy are not coming from a monolithic "Big Brother", but — even harder to grapple with — hundreds of sources, not seeking to control us, merely to market to us, track us, count us, or streamline paperwork. The result, though, is still as chilling as _1984_. _Database Nation_ explores the many threats to privacy in the Twenty First century and warns its readers, as Orwell's 1984 did before, that the cost of inaction will be the loss of freedom." The article continued with references to the book's own Web site, < http://www.databasenation.com >. Sandra Gittlen, writing in NetworkWorld Fusion on 2000-03-22, said, "From its first pages, it grips you and makes you realize that the onus for privacy is not just on companies. You, too, have to take some responsibility for how much information you hand out. After all, Garfinkel contends, pretty soon every database could be hooked into every other database, creating a huge Web of information about you." Ralph Nader wrote, "Database Nation by Simson Garfinkel is a graphic and blistering indictment of the burgeoning technologies used by business, government, and others to invade the self — yourselves — and restrict both your freedom to participate in power and your freedom from abuses of power. The right of privacy is a constitutionally protected right, and its erosion or destruction undermines democratic society as it generates, in one circumstance after another, a new kind of serfdom. This book is one that you're entitled to take very personally." Peter Neumann of SRI, the moderator of the RISKS Forum, wrote, "You will find this book very much in tune with what you have been reading in RISKS and in Lauren Weinstein's PRIVACY FORUM all these years. Simson has brought it all together very nicely in a highly readable book."

38.1 Consumer / employee / individual profiling & surveillance (non-governmental)

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

1997-06-10 **privacy database FTC**

EDUPAGE

LARGEST DATABASE COMPANIES TO RESTRICT USE OF PERSONAL DATA
Eight of the largest database companies in the U.S., including the Lexis-Nexis online search service, have agreed to restrict the kinds of personal information they maintain about individuals, and to refrain from augmenting their own records with data from private marketing databases containing such information as individual's magazine subscriptions, shopping habits, and personal income. Privacy advocates have endorsed the agreement but have expressed concern that smaller database companies that did not sign on, and will continue to sell such marketing information; they also criticized the agreement for failing to provide an enforcement mechanism. (Washington Post 10 Jun 97)

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

1997-06-24 **privacy online databases**

AP

Two weeks after the online database industry assured the public in early June that it was committed to protecting the privacy of data subjects, Lexis-Nexis announced plans to release its P-Trak data so that individuals could verify their own records. Privacy advocates expressed concern about controls over who could see these data.

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

1998-02-15 **privacy**

EDUPAGE

DRUGSTORE DATABASE USE RAISES PRIVACY ISSUES
CVS Corp. and Giant Food Inc. are using a computer database marketing specialist to send personalized letters to customers who haven't refilled their prescriptions, reminding them to keep taking their medicine and pitching new products that treat the customer's ailments. The editor of the Journal of the American Medical Association calls the practice a "breach of fundamental medical issues" and asks: "Do you want ... the great computer in the sky to have a computer list of every drug you take, from which can be deduced your likely diseases — and all without your permission?" CVS and Giant Food say their efforts are merely intended to help customers stay healthy. (Washington Post 15 Feb 98)

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

1998-04-28 **privacy e-mail address identity game upload clandestine**

RISKS 19 70

Computer games played over the Internet present an opportunity for game-makers to collect information about players. Blizzard Entertainment makes Starcraft, a popular multi-user online game; the company was embarrassed when news surfaced that it was collecting user information surreptitiously. Blizzard protested that no harm was meant and that the information was collected only when users experienced connection problems, but also promised to ask for permission before doing so again. In another case, Virgin Entertainment, makers of the Subspace game, claimed to be collecting the identifiers of people using their software without physically having the game CD-ROM in their drives.

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

1998-05-14 **privacy data mining credit cards marketing junk**

EDUPAGE

AMERICAN EXPRESS TEAMS UP WITH DATA MINING COMPANY
American Express has formed a relationship with a "data mining" company called KnowledgeBase Marketing in order to be able to sell merchants detailed information on which people are most likely to purchase which products and services. KnowledgeBase obtains its information from public sources, and keeps data such as home values, ages and sexes of household occupants, etc. Privacy advocates are worried about ventures of this kind, but an AmEx executive says that by helping retailers and marketers more closely target their most likely customers, the ultimate result of the project would be to cut down on the overall quantity of junk mail and junk phone calls. (USA Today 13 May 98)

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

1998-08-16 **privacy policy monitoring profile advertisers demographics**

EDUPAGE

TRACKING ACTIVITY ON THE WEB
Another privacy-related story: Lycos, Geocities and NBC's Videoseekers are among the major Web sites that will participate in a new service, called Engage, that was developed to track what people are looking at on the Internet, so that advertisers can target their marketing efforts. David S. Wetherell, the chief executive of CMG Information Services, the company behind Engage, gives this example of how the service would be used: "If someone comes to your bookstore for the first time, you can find out if they are interested in mountain climbing, organic gardening and tennis; you can present them books related to their interests immediately." Mr. Wetherell adds: "We took the highest road you could possibly take with respect to privacy. We think you can learn a lot more about someone from their behavior than from their name and address." The system will keep information on age, sex, income, zip code and number of children; it will not collect information on sexual or health related topics and will not store individual names, addresses, and birthdays. Privacy consultant Jason Catlett says: "Engage has done many good things to protect privacy, but my worry is that they are firing the starting gun in the race for the bottom. The worst actors will be left to use the most sophisticated surveillance techniques as they please." (New York Times 16 Aug 98)

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

1999-03-01 **credit card fraud prevention profiling**

RISKS 20 23

A diner's credit card was refused because (1) he and his wife had bought expensive tableware that was charged in two lots at the store; (2) the credit-card company's profile of habitual purchase patterns was tripped by the unusual pattern; (3) a hold was put on the credit card; and (4) no one bothered to inform the user. [Moral: if you're going to impose security profiles on a system, you have to follow through all the way. Half a security measure can be worse than none.]

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

1999-04-16 **privacy browser bookmark Web**

Wired

Kevin Cooke, Development Manager at Wired Magazine, discovered that Microsoft's Internet Explorer version 5.0 sends information to a Web site when the user bookmarks the site's URL. Chris Oakes of Wired reported: "This is one of those things where we did not see the privacy issue when we were creating the feature," said Microsoft product manager Mike Nichols. "The feature doesn't pose a super-huge risk. But Microsoft is looking at ways of modifying this feature in future releases." Apparently the feature was designed to allow a Web site to supply an icon to be stored on the user's system so any "Favorite" would be "branded" with that icon.

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

1999-11-03 **privacy monitoring playlist music recording interest aggregate data mining policy disclosure scandal**

Wired, RealNetworks
http://www.real.com/company/pressroom/pr/99/updateadvisory.html

RealNetworks admitted that it had been collecting information about exactly what its users of RealJukebox player had been listening to. The company did not inform its users of the monitoring and got hammered by its competitors, privacy advocates and many users. The company immediately changed its public privacy statement to let people know about the data collection function and its spokesperson swore that the data had been aggregated so that no one could trace the specific interests of any one user. The company immediately apologized to the public for the concerns it had caused and provided a patch to disable detailed reporting. The company's statement included the following text:

This RealJukebox update causes the following changes to the product:

The RealJukebox globally unique identifier (GUID) is now disabled, and is set to zeros for all users. As a result, GUIDs cannot be associated with any personal registration information (such as name and e-mail) that you may have given RealNetworks.

Since the RealJukebox GUID is disabled and set to zeros, it no longer contains any reference to the network card MAC address of the user's computer.

The following information will no longer be sent during the Get Music service update:
- Encoding options
- Portable devices
- Total song tracks in music database (recorded and downloaded)
- Total recorded song tracks in music database (recorded only)
- User option to receive automatic music downloads (set to blank)
- Genre preference A unique RealJukebox ID will no longer be sent during requests for CD information.

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2000-01-04 **privacy marketing information leakage software spying lawsuits**

NewsScan, USA Today http://www.usatoday.com/life/cyber/tech/cth061.htm

In 1999, RealNetworks management were embarrassed by public outrage over private information about users that was sent discreetly over the Internet by RealJukebox. In January, the company went to court itself demanding relief from lawsuits claiming violation of privacy laws; according to the company attorneys, consumers had agreed to be bound by their licenses for the software. A Seattle judge granted the company a temporary restraining order against the lawsuits.

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2000-01-28 **Web privacy identification tracking monitoring shadow spoof restriction access-control**

Wall Street Journal, Reuters, Wired

Using the IP addresses of visitors to their Web sites, some Webmasters are programming their sites to show different faces to different people. In a kind of weird intrusion-detection mechanism, companies are restricting access so that competitors or known hackers cannot enter. DoubleClick openly admitted that they use cookie-tracking to tailor ads on certain sites so that viewers see a subset based on the sites they previously visited. Many commentators argued that this process violates browsers' privacy, and DoubleClick provided an opt-out feature. Nonetheless, lawyers for Hariett Judnick in California filed suit in January 2000 stating that the company was unlawfully obtaining and selling private information about consumers.

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2000-03-03 **consumer privacy compilation data mining targeted advertising marketing**

ZDNet http://www.zdnet.com/zdnn/stories/news/0,4586,2428392,00.html, Los Angeles Times http://www.latimes.com/business/20000215/t000014627.html

DoubleClick got into a public-relations quagmire when it announced in late January 2000 that it would compile information about visitors to numerous Web sites and feed the browsing data to an engine for selection of specific banners ads likely to be more interesting than usual. Many privacy advocates protested that this Abacus Alliance (formed in November 1999) would be too intrusive. DoubleClick executives protested that individual client identification would be protected — only the shopping and browsing patterns would be stored and used for ad selection.

[In mid-February] DoubleClick [announced] plans to launch a massive ad campaign as part of its "five-point privacy initiative" designed to ameliorate concerns over the advertising firm's online data collection practices. The New York-based company recently was targeted with lawsuits and complaints alleging it violates consumers' privacy by tying Internet users' surfing habits to their names in its massive database. The company also says it plans to hire a "chief privacy officer" and enlist PricewaterhouseCoopers to perform periodic audits of its data collecting procedures. The ad campaign will steer consumers to a new Web site, www.privacychoices.org, which will house information on how the company collects consumer data and how to opt out of that process. Privacy advocates call DoubleClick's efforts too little, too late: "They're launching a major ad campaign because they're trying desperately to avoid legislation," says the director of the Electronic Privacy Information Center, a plaintiff in one of the lawsuits. (Los Angeles Times 15 Feb 2000)

The attorney general of Michigan . . . filed a "notice of intended action" against DoubleClick, charging the Web advertising firm with "failing to disclose to Internet users that DoubleClick is systematically implanting electronic 'cookies,' or electronic surveillance files, on hard drives of users' computers without their knowledge or consent." In addition, the notice criticizes DoubleClick's recent attempts to combine its tracking data with personal data such as names obtained through its acquisition of Abacus Direct last year. Michigan's filing, which is preliminary to a lawsuit, is the third action taken against DoubleClick this week — the Federal Trade Commission and the New York attorney general earlier launched separate inquiries into the company's business practices. (Financial Times 18 Feb 2000)

The online advertising agency DoubleClick, under pressure from privacy advocates, has put aside its plan to integrate the anonymous data it collects about consumer online purchasing patterns with personal information about millions of consumers in the databases of Abacus Direct Corporation, a company DoubleClick purchased last year. DoubleClick chief executive Kevin O'Connor says, "I made a big mistake. It was wrong to try to match that information in the absence of industry or government standards, so until that there's agreement on it, will not... Now we're just happy to get this behind us and move on." (New York Times 3 Mar 2000)

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2000-03-16 **privacy children monitoring inference inquiry prediction banner advertisement consumer profiling advice**

NewsScan

E-tractions, a Bedford, Mass. sells online quizzes and games to Web companies that want to jazz up their sites, but their games do more than entertain. E-tractions GameServer software analyzes the quiz-takers' answers to learn more information about them in order to target them with ads or steer them toward other parts of the site. For instance, on WebHire's site, an "HR IQ" test under development will poll readers on their experience with various employment issues, and then the company will offer them products based on their answers. A game under development for the upcoming MsMoney.com site will poll girls on the cost of items in a "Price is Right" -type game, quiz them on the type of lifestyle they'd like to have, and then counsel them on the type of job they will need to support that lifestyle. "If you want a BMW and to live in the Marina district, you'll need an engineering degree and a Stanford MBA," says MsMoney.com's CEO. (Wall Street Journal 16 Mar 2000)

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2000-05-01 **Web consumer data behavior profiling marketing banner advertisements privacy**

NewsScan, Wall Street Journal
http://interactive.wsj.com/articles/SB957139612628916016.htm

Predictive Networks Inc., a Web company opening its doors today, began drawing protests among privacy advocates well before its launch. Predictive has developed software that can track every site a Web surfer visits and then build a profile of him. Based on the profile, Predictive automatically sends ads targeting his interests. Predictive believes that surfers are willing to give up some privacy in exchange for free Internet access, and advertisers are already coughing up ad rates as much as six times higher than usual for the service. But privacy advocates caution that the technology pushes the depth of digital eavesdropping to a new level. "It takes a court order and tight supervision to listen over a telephone link," says one. "It's really time for Congress to set limits and decide that we need a privacy policy." (The Wall Street Journal 1 May 2000)

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2000-05-08 **consumer profiling Web privacy e-commerce**

NewsScan, Los Angeles Times
http://www.latimes.com/business/20000508/t000043365.html

If you buy event tickets online, you'll have noticed an increase in associated merchandise and memorabilia offered by the ticketseller at the same time. Online ticketing companies like Ticketmaster's Internet partner and Tickets.com are scrambling to come up with new revenues over and above the price of the tickets to offset the 20% to 50% more it costs them to sell electronically rather than through traditional channels. Ultimately, online ticketers say their services will lead to increased convenience for customers and a profitable bottom line, but right now, they're struggling to cover hefty marketing, infrastructure and customer service expenditures. Ticketmaster Online-CitySearch lost more than $121 million last year, and Tickets.com recorded losses of $66.6 million. Meanwhile, ticketsellers are reaping the benefits of a new resource — more information about their customers. By requiring a bit of demographic data from would-be buyers, they're building valuable databases. "One of the realities about Springsteen is that 200,000 people will try to buy tickets when we only have 20,000 seats," says Ticketmaster.com president Tom Stockham. "We used to know nothing about 180,000 of those people." (Los Angeles Times 8 May 2000)

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2000-08-15 **privacy monitoring Web cookies lawsuit consumer profiling**

NewsScan, Washington Post http://www.washingtonpost.com/wp-dyn/articles/A25494-2000Aug14.html

The Boston technology company Pharmatrak is able to use "cookies" to surreptitiously track the movements on the Web of visitors to the sites of various pharmaceutical companies, and, because it is not an advertiser, is not bound by a recent agreement by such online advertisers as DoubleClick and Engage to allow computer users to choose whether or not they wish to allow their activities on the Web to be monitored. Threatening the possibility of legal action against Pharmatrak, Michigan's attorney general . . . [said], "They've taken stealth to a new low... It's a classic example of corporate surveillance. There's no way your average computer user has any idea." Pharmatrak says it doesn't collect the names of individuals, and has no intention of doing so, and Pharmatrak's chief executive says of the lawsuit threatened by Michigan: "If they file a suit like that they're idiots," because people know or ought to know that "they're using an open access means of communication." (Washington Post 15 Aug 2000)

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2000-08-15 **I&A identification & authentication token monitoring**

NewsScan, New York Times
http://partners.nytimes.com/library/financial/columns/081600tv-adcol.html

A new system called Whispercode, designed by a New Jersey company for monitoring the effectiveness of TV advertising, will involve the encoding of commercials with inaudible, identifying signals that can be picked up by a small device worn by a participant (perhaps in a bracelet or keychain) and relayed to a nearby recording box that records the fact that the wearer was in the room when the commercial was broadcast. [It should be noted, though, the system can't detect whether the participant is awake, attentive, and not bored to death.] The company's chief executive officer says, "With Whispercode, we will finally be providing our clients with a true accounting of where their advertising money is going." (New York Times 15 Aug 2000)

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2000-08-30 **surveillance monitoring positioning chip mobile phone**

NewsScan, San Jose Mercury News
http://www.sjmercury.com/svtech/news/breaking/reuters/docs/356409l.htm

The Irish chip designer Parthus Technologies has developed a product called NavStream, based on the Global Positioning System (GPS), that will be able to identify the location of a mobile phone user to within five yards. That kind of capability would allow the creation of various new location-sensitive information services, including emergency assistance calls. A company executive adds: "Parents can keep track of their children's exact location by embedding GPS technology into a watch or other device, giving them peace of mind." (Reuters/San Jose Mercury News/30 Aug 2000)

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2000-10-02 **e-commerce ethics marketing pricing consumer tracking profiling privacy**

NewsScan, Los Angeles Times
http://www.latimes.com/business/20001002/t000093531.html

Although it's proven a public relations debacle for Amazon, industry analysts say that the "dynamic pricing" model recently tested by the online merchant could spread to other e-tail operations. "Dynamic pricing is the new reality, and it's going to be used by more and more retailers," says one Internet consultant. "In the future, what you pay will be determined by where you live and who you are. It's unfair, but that doesn't mean it's not going to happen." What's especially troubling about the Amazon test, say some customers, is that regular customers were being charged more than new visitors for the same item. "This is a very strange business model, to charge customers more when they buy more or come back to the site more," says a message posted to the DVDTalk.com message board, where participants recently discerned Amazon's new pricing practice. "This is definitely not going to earn customer loyalty." (Los Angeles Times 2 Oct 2000)

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2001-02-14 **privacy ISP Internet service provider cable DSL Web access logging monitoring recording data collection privacy consumer profiling**

NewsScan

COMCAST RECORDS SURFING MOVEMENTS OF ITS SUBSCRIBERS [12 Feb 2001]
Comcast, the nation's third-largest cable company and a provider of high-speed Internet access to a million computer users, says it has begun recording the Web surfing movements of its subscribers in order to improve its technology and services. Admitting that it began the monitoring without notifying its customers, the company said it believes its actions are permitted by the language in their service agreements with subscribers, and insists that "Comcast absolutely does not share personal information about customers, and we have the utmost respect for our customers' privacy." Privacy advocates are upset about the Comcast action, and Internet security expert (and Comcast customer) George Imburgia says: "I'm furious." (AP/San Jose Mercury News 12 Feb 2001)
http://www.siliconvalley.com/mld/iliconvalley/2661735.htm

COMCAST STOPS STORING INDIVIDUAL WEB-SURFING PATTERNS [14 Feb 2002]
In response to criticism from privacy advocates, Comcast has decided to cease collecting data that would allow it to track the Web surfing habits of individual subscribers. The company says it had never contemplated using the information for anything other than to determine aggregate usage patterns so it could improve the performance of its computers and networks. Comcast executive Dave Watson says, "We don't want anyone to be concerned we'd take that next step forward. We just want to take this issue off the table." David Sobel of the Electronic Privacy Information Center says his group's concern was not necessarily that Comcast itself would track individual usage, but that law enforcement agencies might get the information by subpoena. (New York Times 14 Feb 2002)
http://partners.nytimes.com/2002/02/14/technology/14PRIV.html

---

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2001-06-07 **consumer profiling GPS geographical positioning system law enforcement surveillance personal information privacy accident emergency vehicle**

RISKS 21 46

Chris Norloff contributed an interesting essay to RISKS about the implications of having GPS on automobiles:

"You just can't outrun a satellite. A Merced, California, man took his fully equipped 2001 SUV out onto some nearby country roads, navigating swiftly and confidently with the optional OnStar Global Positioning System. When he got into an accident, he decided to run for it. But the guidance system had already notified OnStar headquarters of the accident, specifying where it had happened and giving a complete description of his vehicle to the California Highway Patrol. The officers followed a trail of coolant about a mile into an orchard, where they found and arrested the driver. [Source: *Road & Track* magazine, July 2001; PGN-ed]"

Norloff continued, "What constitutes an "accident"? (Air bags seem to go off quite easily, taking out the windshield and dashboard [$$$] in a fender-bender). Will GPS-reported accidents become like household burglar alarms - sending out mostly false alarms? Who will hack into the OnStar system to falsely report accidents? Who will use the OnStar system to efficiently dispatch lawyers to accident sites? How soon until OnStar sells accident records so used-car purchasers can learn the vehicle's history?"

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2001-09-10 **privacy miniature wireless camera broadcast voyeurs peeping Tom spying surveillance law enforcement police**

NewsScan

LITTLE BROTHER MAY BE WATCHING YOU (WITH X10 VIDEOCAMS)

A company called X10 Wireless Technology is marketing its tiny color video cameras for their use in keeping an eye on your kids or even engaging in voyeuristic activity. One ad for the $79.99 device displays a bare-backed woman and the headline "Quit Spying on People! (we never told you to do that)." The technology uses radio frequencies for communication among devices within a 100-foot radius, and represents a development that one attorney says "is outstripping everything we once contemplated about privacy." X10 devices have been found planted secretly in such places as college shower rooms, attorneys' offices, and corporate meeting rooms. (San Jose Mercury News 10 Sep 2001)
http://www.siliconvalley.com/docs/news/svfront/027254.htm

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2001-10-22 **cookies persistent state targeted advertising consumer profile privacy**

NewsScan

AOL TO USE "COOKIES" FOR TARGETED ADVERTISING
Privacy advocates seem to have no objections to AOL's new decision to begin using "cookies" (tiny files left on user computers to track their Web travels), which AOL says it's doing to help prevent customers from receiving advertisements irrelevant to their interests. AOL maintains that the company and its advertisers will use cookies "to determine, on an anonymous basis, which advertisements members have seen and how members respond to them," but will not let the cookies to be used "to compile profiles about the different Web sites that a particular member visits." (Gannett/USA Today 22 Oct 2001)
http://www.usatoday.com/life/cyber/2001/10/22/aol-cookies.htm

---

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2002-02-21 **consumer privacy contract tracking surveillance vehicle automobile rental GPS Geographical Positioning System**

NewsScan

RENT-A-CAR COMPANY WILL CONTINUE SPYING ON SPEEDERS [9 Jul 2001]
Acme Rent-a-Car in New Haven has rebuffed the Connecticut Department of Consumer Protection and plans to continue using Global Positioning System (GPS) technology to track individuals who speed in rented vehicles, and levy fines on them of $150 if the speeding continues for more than two minutes. The consumer agency's complaint against Acme is based not on privacy issues but on the charge that Acme's rental contract didn't give adequate information about what it was doing. (USA Today 9 Jul 2001)
http://www.usatoday.com/life/cyber/tech/2001-07-09-rental-car-tracking.htm

CAR RENTAL AGENCY CITED FOR SPYING ON SPEEDERS [21 Feb 2002]
Acme Rent-a-Car, based in Connecticut, has been cited by the state's Consumer Protection Commission for its practice of tracking customers' driving habits via GPS devices and assessing customers $150 each time they exceeded 79 miles per hour. The commission said the company violated Connecticut's unfair trade practices act by not notifying customers of the monitoring, and ordered Acme to pay back "every single customer who they took money from illegally." Many car rental agencies use GPS to locate their vehicles in case they are stolen or taken out of the country. (Reuters/CNet 21 Feb 2002)
http://news.com.com/2100-1040-842821.html

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2002-03-28 **privacy survey Web sites e-commerce control**

NewsScan

WEB SITES COLLECTING LESS PERSONAL DATA
Many commercial Web sites are cutting back on the amount of personal data they regularly collect on visitors, with 84% of the 85 sites polled reporting that they're gathering less data than they did two years ago. That said, most of the sites -- 96% -- still collect at least some data from users, according to a survey conducted for the Progress and Freedom Foundation. The survey included such popular Web sites as Amazon, Google and Travelocity. Foundation President Jeffrey Eisenach said that the responses indicated a trend toward giving consumers more control over how their private information is used: 93% of the Web sites surveyed gave users the option of restricting the sale or transfer of their information to other businesses, up from 77% in 2000, and some 72% of sites promised consumer data would be secure, up from 48% the year before. (Wall Street Journal 28 Mar 2002)
http://online.wsj.com/article/0,,SB1017247161553469240.djm,00.html (sub req'd)

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2002-03-30 **privacy preferences management policy junk mail spam advertising preferences**

RISKS 22 02

In March 2002, Yahoo Groups caused a ruckus among its subscribers by unilaterally resetting all its members privacy preferences from NO to YES. Every member had to manually unsubscribe all over again.

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2002-08-27 **consumer profiling cookies monitoring Web surfing legal agreement**

NewsScan

WEB AD COMPANY WILL NOW TELL YOU ABOUT YOUR SURFING PROFILE
Bringing an end to a 30-month investigation by 10 states charging improper use of profiles on network users, the Web advertising firm DoubleClick has agreed to provide consumers with better disclosure of what they're doing and to give them access to their own profiles. As part of the agreement, DoubleClick will pay a $450,000 fine. Some privacy advocates say the agreement falls short of what is needed, because it still allows the company to create individual profiles, even though it must now openly acknowledge what it is doing. (Washington Post 27 Aug 2002)

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2002-09-30 **consumer profiling privacy policy e-commerce**

NewsScan

AMAZON CHANGES ITS TUNE ON PRIVACY POLICY
E-commerce giant Amazon has bowed to the wishes of a coalition of state attorneys general and is changing its privacy policy to make it more consumer-friendly. The changes mean the online retailer will provide consumers with information on what specific personal data is being collected, as well as examples of how it might be used. In addition, Amazon says it will not sell its customer database to marketers and will close some loopholes in its policy. Massachusetts Attorney General Thomas Reilly, who spearheaded the group of 16 states and the District of Columbia, said of the changes: "It's extremely important for all companies — especially Internet sellers — to handle consumer data carefully and confidentially." However, Junkbusters president Jason Catlett dismissed the changes as mostly cosmetic and called for an independent audit of Amazon's practices. Meanwhile, a report by Forrester Research estimates that consumers' concerns over privacy cost online retailers $15 billion in lost sales in 2001. "It's still right up there on the front of consumers' minds, so anything Amazon and others can do to soothe those fears is important," says Forrester analyst Christopher Kelley. (E-Commerce Times 27 Sep 2002)
http://www.ecommercetimes.com/perl/story/19525.html

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2003-04-23 **privacy concern Amazon FTC COPPA**

NewsScan

TC ASKED TO INVESTIGATE AMAZON
A coalition of privacy and consumer groups has asked the Federal Trade Commission to investigate online retailer Amazon.com, and has charged Amazon with violating the Children's Online Privacy Protection Act of 1998 (COPPA) by allowing minors to post personal, identifying information. Chris Hoofnagle of the Electronic Privacy Information Center says, "When you find a posting that says, 'I'm Jane Done, I'm 11 and I'm from Hampsted, New York,' that's information that can be verified with the White Pages." Amazon's response is that its Web site is directed not at children but at adults: "We sell products for children to be purchased by adults." The company says it does not "knowingly solicit or collect personally identifiable information online from children under the age of 13 without prior verifiable parental consent." And if it receives such information anyway? Amazon says it removes it "as soon as we see it." (San Jose Mercury News 23 Apr 2003)

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2003-06-27 **TV advertising ads private information TiVo data consumer**

NewsScan

TV ADVERTISING EXECS IN DENIAL OVER TIVO DATA

Television advertising has long relied on Nielsen ratings, which indicate how many viewers are watching a particular TV show, but not whether they're sticking around for the commercials, or heading off to the kitchen for a snack or channel-surfing to check on the baseball score. But the data service recently launched by TiVo offers a much more complete vision of what's happening in the home when the TV's on. It can track what viewers record, what they watch, when they change the channel and which commercials they skip. This ability to pinpoint viewer behavior has received a less than enthusiastic reception from advertisers. "This kind of information is the holy grail for marketers. But it's not the holy grail for advertising agencies and media companies, which have built an industry around the idea of getting a shallow message to a broad audience rather than a tailored message to a narrower one," says the chief strategy officer for interactive ad agency Avenue A. According to the TiVo data, genres like big-budget situation comedies (think "Friends") tend to have the lowest commercial-viewing rates because couch potatoes record them and skip through the commercials when they watch. Reality TV, news programs such as "60 Minutes" and "event" programming such as the Academy Awards do significantly better. With Forrester Research predicting that by 2007, more than half of American households will have either a personal video recorder such as TiVo or other on-demand services, advertisers will be forced get their heads out of the sand and come with a new business strategy. (Business Week Online 27 Jun 2003)

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2003-06-29 **privacy black box car data event recorders speed limit**

NewsScan

IS YOUR PRIVACY INVADED BY THE 'BLACK BOX' IN YOUR CAR?

A recent survey found that most people are unaware that many later-model automobiles are equipped with "black box" recording devices (called "data event recorders") which are capable not only of triggering the release of accident airbags but also of recording driving data (such as speed of the car) in the last few seconds before a crash. Such information is increasingly being used as evidence in criminal and civil cases related to the accident, as part of "normal reconstruction" of what happened. But civil libertarians are balking. Defense attorney Bob Weiner calls the black boxes "a tremendous invasion of privacy," and David Sobel, general counsel for the Electronic Privacy Information Center, say: "The real issue is one of notice, and the problem arises from the fact that information is being collected about people's driving behavior without them knowing. If drivers knew about the device, they could at least then begin asking questions." (USA Today 29 Jun 2003)

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2003-07-19 **closed circuit TV camera surveillance privacy spy chip**

NewsScan

SMILE, YOU'RE ON CLOSED CIRCUIT TV

In Cambridge, England, RFID technology will cause a CCTV camera to take a photo of anyone taking a package of Gillette Mach3 razorblades from the shelves of supermarket chain Tesco Ltd.; a second camera then takes a picture at the checkout and security staff then compare the two images. "Customers know that there are CCTV cameras in the store," said a spokesman for Tesco, and says that the purpose of the pilot project is to provide stock information rather than provide security. However, the manager of the Cambridge store says he has shown the police photos of a shoplifter. Civil libertarians says that the so-called "spy chips" are an invasion of consumers' privacy, but manufacturers point out that the chips can be disabled simply by having the data erased at checkout when a consumer leaves the store. (The Guardian (UK) 19 Jul 2003)

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2003-09-29 **surveillance classroom parents children England**

NewsScan

BIG MUMMY AND DADDY ARE WATCHING YOU

Some teachers in England say that Webcams should be installed in every classroom in order to involve parents in their children's education — and let them see whether their children are misbehaving. One advocate said: "Bad behavior in class is a big issue throughout the school system, but teachers have to handle it on their own. If pupils knew their parents could see how they were behaving then they would think twice about disrupting classes." (Evening Standard 29 Jul 2003)

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2003-12-31 **privacy surveillance car Big Brother remote sensing**

RISKS 23 11

Car-monitoring service allows you to be your own Big Brother

A remote car-location service offered California company raises questions about privacy, says Monty Solomon. An article in the LA Times said that "a La Jolla company has offered to provide remote sensing of a car's systems and to post that data to a private Web page, along with verifying to state agencies that the car is in compliance with the emission laws of California and a few other states." Likening this positioning system to George Orwell's Big Brother, Solomon feels that Orwell would have been shocked to discover that Big Brother has become "a matter of convenience" to consumers.

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2004-01-05 **school Mississippi webcam monitor classroom chilling effect creativity**

NewsScan

GO STAND IN THE CORNER AND WATCH THE WEBCAM

A public school in Mississippi is apparently the first to use webcam technology to make sure that students being punished for bad behavior don't miss out on what's happening in class. Cameras document everything that takes place in the classroom, good and bad alike. But Barry Steinhardt of the American Civil Liberties Union worries that the cameras could have a "chilling effect" on students and teachers by making them "feel under constant observation" and affecting "the willingness of teachers to be creative or to introduce unpopular topics." (USA Today 5 Jan 2004)

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2004-01-08 **terrorism Microsoft Julie Olearcek staples**

DHS/IAIP Update

Flight Sim enquiry raises terror alert

A mother's enquiry about buying Microsoft Flight Simulator for her ten-year-old son prompted a night-time visit to her home from a state trooper. Julie Olearcek, a USAF Reserve pilot made the enquiry at a Staples store in Massachusetts, home to an earlier bout of hysteria, during the Salem witch trials.

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2004-02-04 **privacy consumer choices preferences log WebFountain IBM buzz reports Internet scouring**

NewsScan

WHO'S SAYING WHAT TO WHOM: WEBFOUNTAIN KNOWS

Hundreds of computer servers at IBM's Almaden Research Center in San Jose, CA, each week gathers 250 million new Web pages and the data (512,000 gigabytes of it) to software called WebFountain designed to capture what everybody is saying about something. IBM has begun licensing the WebFountain technology to corporations to create "buzz reports" developed by scouring every part of the Internet (Web logs, chat rooms, newspaper stories, and so forth) to find out consumer reaction to some new product. In contrast to standard search engines that just match patterns, WebFountain takes a subject and does detailed analyses of what it finds, taking special note of how often someone's name is associated with someone else's with reference to a particular topic. (San Jose Mercury News 4 Feb 2004)

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2004-05-13 **e-mail disk storage advertising profiling**

http://www.nytimes.com/2004/05/13/technology/circuits/13stat.html

GMAIL SECURITY ISSUES

When Google announced its new free Gmail service, many people protested in shock at the idea that Google would scan their e-mail messages and introduce tailored advertisements at the bottom of the e-mail. However, as David Pogue of the New York Times pointed out,

* no human being reads the e-mail;
* a file-storage capacity of 1GB per user will radically change how people use the service
* there's a good spell-checker
* address book
* autocomplete for addresses
* ability to specify a different REPLY-TO address
* online help
* keyboard shortcuts for frequent functions
* automatic spam filters
* 9 month persistence of the account after the last use.

[MK adds: one suggestion is that the 1GB storage capacity would allow users to store files as a kind of universal flash drive. From a security perspective, one should remember that (a) transfer to the remote Gmail server would be unencrypted; (b) any data on that site would, at least in theory, be accessible by Google staff running the servers. I don't think it is likely that this would in practice pose a serious threat, but anyone concerned with critically sensitive data should encrypt them before storing them on the server.]

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2004-08-23 **radio listening habits tracking privacy concern Navigauge Arbitron**

NewsScan

NEW SERVICE TRACKS CAR RADIO LISTENING HABITS

Wake up, Arbitron -- a new service offered by Navigauge is combining global positioning technology with continuous tracking of the radio dial to measure radio audiences in cars. While Arbitron has long been the dominant audience information supplier, relying on paper diaries filled out by consumer volunteers, Navigauge executives are betting there's room for improvement. "For a long time, the radio industry itself has lamented the fact that it gets a large percentage of consumers' media consumption but a disproportionately small share of advertising revenue," says Navigauge CEO Tim Cobb. "That's based on the fact that they cannot articulate to advertisers the value that they are delivering." Navigauge is hoping that its capacity to track participants cars through GPS technology will add new layers of useful information for marketers. For example, the company will be able to tell marketers where drivers stop for lunch and whether radio commercials change people's destinations or driving habits. The system can also be used to measure the amount of traffic moving past billboards, assisting the outdoor ad industry in determining its signage exposure. (New York times 23 Aug 2004)

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2004-10-25 **radio monitoring MobilTrak Washington advertising sensing marketing**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A60013-2004Oct24.html

ADVERTISERS TRACK RADIO LISTENING HABITS

In 14 locations around the Washington area, a company called MobilTrak has installed sensing devices on utility poles that pick up the electronic signals from cars' antennas as they speed by and record which station they're listening to. The monitoring process gives businesses a welcome insight into the listening habits of their target audience and helps them decide how to allocate their advertising budget, says MobilTrak managing partner C. David Boice: "It's all about precision marketing. It's about giving marketers real-time data about what's happening in certain areas at certain times so they don't waste their advertising dollars." The most enthusiastic adopters have been car dealerships, who generally believe that 80% of their business comes from people who live or work within 10 miles of their location. One dealer found that the two stations he'd been investing in -- a talk-personality station and a contemporary music station -- didn't even rank in the top 10 for in-car radio listeners driving by his dealership. "It was a real eye-opener," he says. Currently, MobilTrak picks up only FM signals, but the company says it plans to introduce technology that picks up AM and satellite station signals next spring. (Washington Post 25 Oct 2004)

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2004-10-28 **fMRI functional magnetic resonance imaging neuromarketing consumer profiling**

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/10040162.htm

GETTING INSIDE YOUR HEAD

Brain scanning technology (long used to detect conditions such as Alzheimer's and autism) is now being used to understand how people make choices and how they react to such things as religious experiences, Coke versus Pepsi marketing, and Democrat versus Republican political campaigns. Known as functional magnetic resonance imaging (fMRI), brain scans measure blood flow. During an fMRI, active regions of the brain can be seen lighting up on a computer monitor, indicating either empathy or opposition to what (or whom) the subject is being asked to think about. But the technology is raising strong ethical concerns about "neuromarketing" from critics such as Gary Ruskin of the nonprofit organization Commercial Alert: "This is a story of the corruption of medical research. It's a technology that should be used to ease human suffering, not make political propaganda more effective." (AP/San Jose Mercury News 28 Oct 2004)

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2004-10-31 **spyware epidemic AOL Microsoft helpdesk support costs performance widespread**

NewsScan; http://apnews.excite.com/article/20041031/D862JARG0.html

SPYWARE EPIDEMIC THREATENS TO STALL COMPUTER INDUSTRY

Computer makers say that their technical support lines are lit up by consumers frustrated over sluggish performance and increasingly they're tracing the problems back to one culprit: spyware. Companies are concerned about the cost of the calls, but they're even more worried that that customers will wrongly blame them for performance deficiencies. Russ Cooper, senior scientist with TruSecure Corp., says now that spyware has become epidemic, it's time for Microsoft and other technology companies to launch a public education campaign along the lines of the old "Only *you* can prevent forest fires" concept. The industry's incentive is pure survival, says Cooper. Microsoft officials blame rogue software for up to a third of applications crashes on Windows XP computers and AOL estimates that just three such programs together cause about 300,000 Internet disconnections per day. Forrester Research analyst Jonathan Penn says spyware-related customer support can cost $15 to $45 per phone call, but it's worth it. "Security is a component of loyalty. People, they want all these various services, but they expect security to come with it." (AP 31 Oct 2004)

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2005-01-28 **Marketscore ire campuses institutions students security risk spyware data names passwords credit card numbers confidential IT**

EDUPAGE; http://chronicle.com/prm/weekly/v51/i21/21a03701.htm

MARKETSCORE RAISES IRE AT SEVERAL CAMPUSES

Officials at a number of U.S. institutions are warning students about what they consider a security risk posed by Marketscore software, which promises those who install it significantly greater Internet connection speeds. Unlike applications more commonly referred to as spyware, Marketscore requires users to accept its terms and conditions before installing it. Once loaded, the software routes all of a users Web traffic through Marketscore servers, which then sell usage data to various clients. In monitoring traffic, however, the Marketscore servers also monitor encrypted information, such as user names and passwords, credit card numbers, and other confidential information. Cornell University and the University of Notre Dame have decided to completely block Marketscore from campus networks. Steven J. Schuster, director of IT security at Cornell, called the company's handling of encrypted traffic "absolutely criminal." Officials from Columbia University opted to block Marketscore from what they called its "critical servers," and students who use Marketscore to access other servers at the university receive e-mail warnings about the risk to personal data. At Notre Dame, students who try to use Marketscore receive a warning explaining the risk. Executives from Marketscore defended their products and said they make every effort to explain to users what they do with collected information.

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2005-11-20 **libraries services retailers personal privacy concern USA PATRIOT Act**

EDUPAGE; http://www.nytimes.com/2005/11/20/weekinreview/20cowan.html

LIBRARIES FOLLOWING RETAILERS' LEAD

Libraries increasingly find themselves in a quandary between growing expectations among patrons for personalized services and libraries' traditional stance as a strong advocate for personal privacy.
Commercial enterprises such as Amazon and Netflix typically make suggestions to customers based on previous purchases and can notify users when certain products are available. The library at North Carolina State University is implementing a program that offers students similar services based on past usage. To offer such services, however, the library must keep more-detailed patron records than many libraries keep, given the authority of government officials under the USA PATRIOT Act to subpoena those records. Officials from the university report that students are comfortable trading some measure of privacy for the convenience of personalized services. Another program at the University of Notre Dame offers similar suggestions to users, which, according to its developer, should simplify research for many students. Michael Golrick, the city librarian in Bridgeport, Conn., said that the large numbers of immigrants in his community would not be so willing to trade privacy for convenience. Many of them, he said, "came to this country to avoid the kinds of surveillance and persecution we're seeing tinges of today."
New York Times, 20 November 2005 (registration req'd)

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2006-01-19 **Apple response iTunes user privacy infringement complaints**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4627214.stm 23

APPLE CHANGES ITUNES IN RESPONSE TO COMPLAINTS

Responding to complaints that its iTunes software infringed on user privacy, Apple has made changes to the application. At issue is a feature called MiniStore, which recommends songs to users based on what they are listening to. When the new feature was released earlier this month, some users discovered that the feature transmitted information about iTunes users to Apple with unique identifiers. Those ID numbers exposed the users of the service to violations of their privacy because the iTunes software did not alert users to the feature and how it works. Critics also pointed out that Apple did not disclose what exactly it does with the data that is transmitted to the company. Apple has changed the software to include a pop-up that tells users about the feature and allows them to turn it off. Apple also said that it has not done anything with the data it has collected. Kirk McElhearn, one of the users who first reported the concerns about MiniStore, commended Apple for its response, saying it had "done the right thing."

Category 38.1 *Consumer / employee / individual profiling & surveillance (non-governmental*

2006-01-24 **study survey Google personal data privacy 77% users ignorant**

DHS IAIP Daily; http://www.theregister.co.uk/2006/01/24/google_privacy_poll/ 23

77% OF GOOGLE USERS DON'T KNOW IT RECORDS PERSONAL DATA.

More than three quarters of Web surfers don't realize Google records and stores information that may identify them results of a new opinion poll show. The phone poll which sampled over 1000 Internet users was conducted by the Ponemon Institute. Google maintains a lifetime cookie that expires in 2038 and records the user's IP address. But more recently it has begun to integrate services which record the user's personal search history e-mail shopping habits and social contacts. After first promising not to tie its e-mail service to its search service Google went ahead and opted its users in anyway. It's all part of CEO Eric Schmidt's promise to create a "Google that knows more about you."

38.2 Trade in personal information

Category 38.2 *Trade in personal information*

1997-04-03 **Social Security database privacy SSN**

RISKS 19 5

Simson Garfinkel published a detailed analysis of the Social Security debacle, when the SSA put its PEBES (Personal Earnings and Benefit Estimate Statement) system on its Web site for free access. No one has any idea how many of the requests, which need only the mother's maiden name and state of birth for validation of the request by Social Security Number, are fraudulent. Three days after the Garfinkel column, the site was shut down. It reopened in September with careful modifications — earning histories were removed from the display — to prevent abuse.

Category 38.2 *Trade in personal information*

1997-04-10 **Privacy**

EDUPAGE

SOCIAL SECURITY SITE SHUT DOWN BECAUSE OF PRIVACY CONCERNS
Because of privacy concerns, an Internet site used by the Social Security Administration to supply information about an individual's personal income and retirement benefits has been closed. The shut-down followed receipt by the Administration of a harshly critical letter written by a bipartisan group of legislators who said the site's security systems were inadequate. To obtain information, a computer user needed merely to supply a name, address, telephone number, place of birth, Social Security number, and mother's maiden name — items that are available in many private databases. (Washington Post 10 Apr 97)

Category 38.2 *Trade in personal information*

1997-06-12 **privacy**

RISKS 19 22

In a move that had privacy advocates howling with horror, The Public Link Corp. of Dallas, TX installed a database lookup service on their Web page that allows anyone to find the address of the owner of a vehicle with Texas license plates. The opportunities for abuse include targeting owners of expensive automobiles for theft and providing stalkers with an easier way of locating their victims.

Category 38.2 *Trade in personal information*

1997-06-26 **privacy**

AP

In Dover, NH, City Prosecutor George Wattendorf started publishing the names of people arrested and charged with domestic violence. The city's Web site now has a section listing such information, which the Prosecutor considers a matter of public record. Some civil libertarians were livid, as were a number of the accused.

Category 38.2 *Trade in personal information*

1997-07-19 **privacy**

AP

Presented with alternatives pitting personal privacy against public disclosure, 86% of 1008 US respondents to an AP poll chose to support personal privacy. On the other hand, 70% of the respondents supported public access to drivers' records.

Category 38.2 *Trade in personal information*

1997-07-24 **ISP AOL privacy junk phone**

EDUPAGE, CNET, AP

AOL began a firestorm of protest by announcing that it would rent out members' phone numbers for a fee. The company made no announcement of its change of policy other than posting a modest change of its Terms of Service. Within one day of publication of hostile stories in the press, the company backtracked and reversed its new policy.

Category 38.2 *Trade in personal information*

1997-10-09 **privacy medical**

AP

California doctors and dentists sued the Medical Board of California in October to prevent Web publication of the home addresses of thousands of doctors. The physicians want more time to ensure that their home addresses not be disclosed without explicit permission, preferring to use office and hospital addresses in the public list instead.

Category 38.2 *Trade in personal information*

1998-01-18 **privacy free speech hate data mining**

EDUPAGE

In Ontario, the government privacy watchdog, Ann Cavoukian, warned that businesses ought to give customers more control over how information about themselves is shared with and exploited by other companies.

Category 38.2 *Trade in personal information*

1998-01-27 **confidentiality spamming ISPs privacy**

EDUPAGE

In December 1997, U.S. sailor Timothy R. McVeigh (not the Oklahoma City bomber) was accused of revealing that he is homosexual by including the word "gay" in his AOL member profile (a violation of the controversial "Don't ask, don't tell" rule). Civil libertarians were incensed that someone at AOL revealed the man's full name to Navy investigators without a subpoena or other legal instrument. Even though the members profile is a public document available to all AOL members, the sailor used only his nickname, Tim but identified him as a US sailor. According to attorneys, this unauthorized release of private information may constitute a violation of the 1986 Electronic Communications Privacy Act. In January, in a curious twist, the sailor lost his AOL account because he sent appeals for help to other AOL members with "gay" in their profiles. AOL apologized for the leak, saying that the Navy had misled their staff into violating corporate policies. Later that month, U.S. federal judge Stanley Sporkin stayed the dismissal because of the legal irregularities in collecting evidence pending resolution of the issues in court.

Category 38.2 *Trade in personal information*

1998-06-03 **privacy ISP user lawsuit liability violation procedure**

TechWeb http://www.techweb.com/wire/story/TWB19980603S0012

On July 15, AOL — the largest ISP in the world — introduced new procedures and regulations to protect privacy, improve billing, and protect children. AOL promised to protect confidential information about users' profiles and their Web surfing and buying patterns. Private communications would no longer be susceptible to reading by AOL employees and clients would have more options on how their information could be used by AOL. AOL would no longer collect information from children under 13. Observers noted that increasing the level of protection inherently carries the potential for increased legal liability to AOL if the guidelines are violated by AOL staff.

Category 38.2 *Trade in personal information*

1998-08-16 **privacy policy fraud ISP Web site lying FTC regulation**

EDUPAGE

FTC SAYS WEB SITE LIED ABOUT PRIVACY ASSURANCES
The Web site Geocities, accused by the Federal Trade Commission of falsely assuring two million subscribers that their personal information was not being disclosed to others, has agreed to post its privacy policy on the site and to discourage children under 13 from using the site without parental permission. The new privacy statement, which admits that the company releases personally identifiable information on its subscribers, is reachable from a link on the Geocities home page. (Washington Post 14 Aug 98)

FREE E-MAIL SERVICES COME WITH HIDDEN COST
Online companies seeking to become "portals" to the Internet, such as Juno and GeoCities, may offer free e-mail as a come-on to consumers, but at a hidden cost. The free services generally are available only after the user has answered a series of questions about age, income, education level and personal interests. That information can turn into a gold mine once it's made available to advertisers seeking to target specific audiences. "If you care about your privacy, the free e-mail and Web sites probably aren't worth it," says the editor of Privacy Times. Last Thursday, GeoCities was accused by the Federal Trade Commission of lying to its two million customers when it said it would not give away the personal information it collected from them. The company has now agreed to post a privacy notice on its Web site that tells customers how the information they divulge will be used. International Data Corp. estimates that there will be 40 million registered free e-mail boxes by the end of the year, up from 14 million last year. (Washington Post 21 Aug 98)

Category 38.2 *Trade in personal information*

1999-01-06 **lawsuit ISP privacy database personal information data**

Wired
http://www.wired.com/news/print_version/email/member/politics/story/17188.html

The Aware Woman Center for Choice in West Palm Beach, FL sued CompuServe in January for allowing abortion foes to collect enough personal information to support terrorism against abortion supporters. Abortion foes recorded car license plates of visitors to abortion centers and then used NY-based TML Information Services' databases to look up the home addresses of the car owners. TML makes its services available for a fee through CompuServe and other ISPs.

Category 38.2 *Trade in personal information*

1999-01-19 **privacy homosexual military navy AOL ISP**

CyberTimes via Benton Project; New York Times
http://www.nytimes.com/library/tech/99/01/cyber/articles/19mcveigh.html

YEAR LATER, SAILOR IN AOL CASE REMAINS A SYMBOL
Issue: Privacy
Tim McVeigh will be honored at an Out magazine ceremony noting the year's biggest newsmakers. Last year, the 18-year Navy veteran became the center of two fights — over gays in the military and the right to privacy online. Using a private email account to organize a toy drive, Mr McVeigh was turned in by a colleague who noticed that his America Online screen name list McVeigh's marital status as "gay." The Navy investigated and AOL voluntarily confirmed that McVeigh's screen name belonged to the sailor. The Navy then started proceedings to oust McVeigh. After building a website and sending out email asking for help, McVeigh was aided by Servicemembers Legal Defense Network [1], a group that helps homosexuals in the military, and the Electronic Privacy Information Center (EPIC) [2] in actions against both the Navy and AOL. "I did win my case — the military had to keep me. The downfall was the military wasn't going to give me an equivalent job," McVeigh said recently. "Even though there was a ruling by a federal judge that they had to return me, the judge didn't have the power to restore my job." [SOURCE: CyberTimes, AUTHOR: Lisa Napoli] [3]

_____
[1] <http://www.sldn.org/>
[2] <http://www.epic.org/>
[3] <http://www.nytimes.com/library/tech/99/01/cyber/articles/19mcveigh.html>

Category 38.2 *Trade in personal information*

1999-01-20 **privacy database sex offender individual rights errors data**

RISKS 20 17

The Virginia state database listing known sex offenders — and their addresses — quickly ran into trouble. In the first three weeks, 49 residents of the state were listed in a weekly publication as sex offenders; two of those addresses were wrong. The ACLU very properly said I-told-you-so.

Category 38.2 *Trade in personal information*

2001-01-10 **data subject personal information database privacy**

NewsScan

DEFUNCT TOYSMART AGREES TO DESTROY CUSTOMER DATABASE
Online etailer Toysmart, which was sued by the Federal Trade Commission and other plaintiffs to prevent it from selling its customer database when it went out of business, has agreed to destroy the database in exchange for $50,000 from a subsidiary of its majority stockholder, the Walt Disney company. A spokesman for the privacy group TRUSTe said, "This is a landmark case because it tells other companies that the privacy promises you make while you're in business must be kept when you go out of business. If you don't keep them, there are third parties that will stop you." (AP/USA Today 10 Jan 2001)
http://www.usatoday.com/life/cyber/tech/cti977.htm

Category 38.2 *Trade in personal information*

2001-03-12 **confidential arrest records law enforcement Web site privacy accuracy completeness**

RISKS 21 27

Dan Graifer noted that "Fairfax County police are posting their arrest records online. Everything from speeding tickets to homicide. . . .[These] are never updated to indicate the disposition of the cases, nor is that information available elsewhere." In addition, Mr Graifer reported, all the original crime reports in MS Word format were also available online.

Category 38.2 *Trade in personal information*

2001-04-03 **privacy consumer information resale mergers acquisitions**

NewsScan

EBAY MODIFIES PRIVACY POLICY TO ALLOW POSSIBLE USER INFO SALE
EBay has refined its privacy policy to clarify its right to sell users' information if the company is acquired or merges with another business. In a notice on its Web site, eBay said it is "possible that eBay, its subsidiaries, its joint ventures, or any combination of such, could merge with or be acquired by another business entity. Should such a combination occur, you should expect that eBay would share some or all of your information in order to continue to provide the service." EBay said it was making the change in response to government efforts to block the sale of customer information by ToySmart.com, a bankrupt toy e-tailer, to other companies. (Wall Street Journal 3 Apr 2001)
http://interactive.wsj.com/articles/SB986241729530570517.htm

Category 38.2 *Trade in personal information*

2001-08-20 **privacy protection technology Internet consumer information traffic**

NewsScan

HP CHIEF CALLS FOR WEB PRIVACY LEGISLATION
Carly Fiorina, the chief executive of Hewlett-Packard, told a technology conference this week that federal legislation is needed to protect the privacy of Internet users, and suggested that the problem is caused technologists more than it is by technology itself: "I think we in the technology industry have fallen in love with technology. And in the end it is not about the technology. Privacy and security, or trust, are vital to consumers, and that is what we should focus on. There is a role for legislation." (Reuters/New York Times 20 Aug 2001)
http://partners.nytimes.com/reuters/technology/tech-tech-privacy.html

---

Category 38.2 *Trade in personal information*

2001-12-07 **trade commerce sell personal information privacy identity theft government authentication opt-out**

NewsScan

CALIFORNIA SELLS BIRTH DATA TO PRIVATE WEB SITE, 'RAISES RED FLAG' [29 Nov 2001]
The State of California has sold the birth data of California residents to a privately operated genealogy Web site that can now be used to retrieve such personal data as someone's place of birth or mother's maiden name -- information frequently used as identifying information for purposes of accessing bank accounts and making various kinds of financial transactions. State Senator Jackie Spier (D, San Mateo) warns: "The time has come for us to recognize that identity theft has become a big problem. The fact that this information is public should raise a red flag." (San Jose Mercury News 29 Nov 2001)
http://www.siliconvalley.com/docs/news/svfront/037140.htm

ASK AND YOU SHALL BE REMOVED ... BUT YOU'VE GOT TO ASK [30 Nov 2001]
Responding to complaints by consumers and privacy advocates who protested California's legal sale to the Web genealogy company RootsWeb.com of public information containing such personal data as people's birth dates and their mothers' maiden names, the company now says it will remove from its Web site the names of anyone who makes a specific request. A spokesman for the company said: "The mission of our company is to create places to help people reconnect with their families. We're not in any way doing anything except helping our customers and if a customer is concerned about it, it doesn't do any good to leave them up on the site." A legal council for the Electronic Privacy Information Center says that California's sale of data to the genealogy Web site "a situation where all the residents of California have now been exposed to a new risk of identity theft." (San Jose Mercury News 30 Nov 2001)
http://www.siliconvalley.com/docs/news/svfront/priv113001.htm

CALIFORNIA GOVERNOR HALTS SALES OF BIRTH & DEATH RECORDS [7 Dec 2001]
California Gov. Gray Davis has issued an order placing a 45-day freeze on the state's sale to Web sites of records containing such personal data as mothers' maiden names of state residents. Critics of the sale of this kind of information are afraid it could be used for identity theft and other fraudulent purposes, while defenders of the practice say there's no evidence that the sites are actually being used like that. The general counsel for the California Newspaper Publishers Association says: "I'm an eighth-generation Californian and the fact that my ancestors were born here and died here is pretty much basic historical information. That has always been accessible in California and I'm not sure what new emergency there is that would warrant this executive order." (San Jose Mercury News 7 Dec 2001)
http://www.siliconvalley.com/docs/news/svfront/trade120701.htm

According to several reports to RISKS (see for examle issue 21.81), as of at least 1 December 2001, the entire CA and TX birth records databases were removed from the MyFamily.com, Ancestry.com and RootsWeb.com Web sites.

Category 38.2 *Trade in personal information*

2001-12-18 **children online privacy data information traffic trade government regulation proposed legislation Congress**

NewsScan

GOVERNMENT PLANS TO RESTRICT SALE OF KIDS' PERSONAL DATA [18 Dec 2001]
Congress and the Bush administration seem united in a broad effort to require public schools to give parents the right to deny businesses the ability to gather personal information about their children. Senator Richard C. Shelby (R., AL.) complains, "They're basically selling access to kids without parents knowing about it," and Senator Christopher J. Dodd (D., CN) agrees, saying: "These companies were using the classroom market research." Some of the opposition to the proposed restrictions on sharing student data has come from the National School Boards Association, which says the law could become an "administrative nightmare" that would deprive schools of "productive relationships with businesses." (Washington Post 18 Dec 2001)
http://www.washingtonpost.com/wp-dyn/articles/A57156-2001Dec17.html

---

Category 38.2 *Trade in personal information*

2002-05-02 **privacy surveillance wireless communication phone location position service**

NewsScan

SWEDISH CELL PHONE USERS CAN PINPOINT FRIENDS' LOCATIONS
Customers of Sweden's Telia Mobile have a new way to find out where their friends are -- by using their cell phone. The service, called friendPosition, uses graphic and text messages to reveal the locations of other users. Both people -- the seeker and the sought -- must be using specially enabled cell phones equipped with wireless location services. The friendPosition service could prove a boon to Telia, which, like other wireless carriers, is looking for ways to boost average revenues per user. The $2 a month charge may not seem like much, but could be critical in an industry with very slim profit margins. Meanwhile, similar services could be heading this way, says one analyst: "Commercial location services will be available here by the end of the year," predicts Al Fross, a principal at Pelorus Group. He estimates that global revenue from wireless location services could reach $3.2 billion by 2006. (Investor's Business Daily 2 May 2002)

Category 38.2 *Trade in personal information*

2002-09-05 **privacy public records Web Internet freedom information access**

NewsScan

DO ME A FAVOR, OPEN THE DOOR, AND LET 'EM IN, OOH YEAH
So just who is that knocking that door and ringing that bell? In Hamilton County, Ohio, trouble has flowed from the decision of the clerk of courts to make all public records freely available on the Web. (They were already available to anyone who would go to the county courthouse.) The official explained: "It was the natural progression of technology. Everything we get is scanned and available. It was very easy to open the door to the public." And so now anyone can look on the Web to see anyone else's state tax liens, arrest warrants, bond posting, etc. People are searching the records to find out the dirt on their neighbors - or just to get copies of the floor plans of their houses. Bank executive Jim Moehring says, "You do kind of feel like Big Brother because you can look right in and get into what everyone's doing." The clerk of courts says ruefully: "We didn't realize we were walking into a hornet's next until after we were under way. " (New York Times 5 Sep 2002)

Category 38.2 *Trade in personal information*

2003-02-10 **privacy personal information search engines**

NewsScan

THE GOOGLING OF AMERICA
The search engine Google is changing the kind of information Americans can find out about each other — information that once was the purview of private investigators or the extremely nosy. Now with one click, potential employers, salespeople, and just about anyone can find out every publicly reported detail of your past life, says Boston Globe columnist Neil Swidey. "Now, in states where court records have gone online, and thanks to the one-click ease of Google, you can read all the sordid details of your neighbor's divorce with no more effort than it takes to check your e-mail. 'It's the collapse of inconvenience,' says Siva Vaidhyanathan, assistant professor of culture and communication at New York University. 'It turns out inconvenience was a really important part of our lives, and we didn't realize it.'" (Boston Globe 2 Feb 2003)

Category 38.2 *Trade in personal information*

2003-09-01 **selling personal data Do Not Call list personal information business privacy identity ownership**

NewsScan

WHO OWNS YOUR PERSONAL DATA ANYWAY?
Harvard Business School professor John Deighton says that instead of relying on regulators to protect their privacy through contrivances such as the "Do Not Call" list, consumers should capitalize on the value of their personal information and get something in return for allowing businesses to use it. With companies doing a brisk business in selling and reselling your data, it's time for individuals to get into the act, demanding rewards such as better customer service, price discounts or maybe just plain money. "The challenge is to give people a claim on their identities while protecting them from mistreatment. The solution is to create institutions that allow consumers to build and claim the value of their marketplace identities and that give producers the incentive to respect them. Privacy and identity then become opposing economic goods, and consumers can choose how much of each they would like to consume" says Deighton. (HBS Working Knowledge/CNet 1 Sep 2003)

Category 38.2 *Trade in personal information*

2003-10-16 **search engine Google text data mining FBI**

NewsScan

TEXT-SEARCHING OR TEXT-MINING?
Whereas Google and other Web search engines retrieve information and display links to documents that contain certain keywords, text-mining programs dig deeper in order to categorize information, make links between seemingly unconnected documents, and provide visual maps that lead down new pathways of exploratory learning. Unlike data mining, text mining works on unstructured data — such as e-mail messages, news articles, internal reports, phone call transcripts, and so on. A good example of the problem it seeks to solve is suggested by the comment of researcher Randall S. Murch, who says: "I was an FBI agent for 20 years. And I have yet to see anyone who is able to model the way an agent thinks and works through an investigation." And a good example of the solution offered by text-mining is its use in the 1980s University of Chicago information scientist Don R. Swanson in studying the medical literature on migraines. Starting with the word "migraine," he downloaded abstracts from 2,500 articles from Medline and noticed a reference to a neural phenomenon called "spreading depression" — which prompted him to look for articles with that term in their titles, which in turn led him to the discovery that magnesium was often mentioned as preventing this spreading depression. Thus, as a result of text-mining he was able to hypothesize a link between headaches and magnesium deficiency — a link that was later confirmed by actual experiments. (New York Times 16 Oct 2003)

Category 38.2 *Trade in personal information*

2003-11-07 **security consumer profiling private personal sensitive information outsourcing**

SF Chronicle http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2003/11/07/MNG4Q2SEAM1.DTL

Credit agencies sending our files abroad (via Dave Farber's IP)

David Lazarus writes in the San Francisco Chronicle that, "[T]wo of the three major credit-reporting agencies" are "outsourcing sensitive operations abroad, and a third may follow suit shortly." The information being sent overseas includes Social Security Numbers and full credit histories, so there are fears that identity theft will rise. Credit agencies justify their moves as "necessary cost-cutting". Senator Dianne Feinstein recognizes the threat to US citizens' privacy from this development. She said "she would ensure that the matter was raised as senators and House members completed changes to the Fair Credit Reporting Act." She hopes to protect Americans from "...such outrageous
invasions of privacy."

Category 38.2 *Trade in personal information*

2003-11-12 **online job search privacy consumer sensitive information background checks authority**

RISKS; http://finance.lycos.com/home/news/story.asp?story=36422485 23 3

Holes found in online job search privacy

A report led by Pam Dixon of the World Privacy Forum established that some online job-search Websites may be violating employment and credit laws in their lack of privacy protection. The report indicates that some online job applications even require social security numbers, and perform background checks without having proper authority. Pam Dixon encourages job seekers to ask for better privacy on job Websites. Writes Brain Berstein of AP Online, "She [Dixon] also wants the Federal Trade Commission and the Equal Employment Opportunity Commission to look more closely at how job sites and recruitment services handle information."

Category 38.2 *Trade in personal information*

2003-12-03 **privacy Supreme Court hearing government disclosure**

RISKS; http://www.wired.com/news/privacy/0,1848,61439,00.html 23 5

How Much Is Privacy Worth?

Contributor Monty Solomon summarizes a Wired.com story on the cost of privacy loss. On December 3, 2003, the Supreme Court was set to "hear oral arguments today over whether the federal government should reimburse individuals whose sensitive data was disclosed illegally, even if no harm can be proven." The Privacy Act of 1974 promises $1000 to an individual if she is "adversely affected" by intentional governmental disclosure of her private information without her permission.

Category 38.2 *Trade in personal information*

2004-01-04 **privacy bank account credit card assets stock report information violation**

RISKS 23 11

FORGET YOUR BANK BALANCE? IT'S AVAILABLE ON THE INTERNET

Monty Soloman cites an instance of personal financial information being uncovered through Internet asset-research services. _The Boston Globe_ was able to discover bank account and stock and bond information of Eric F. Bourassa, a Massachusetts Public Interest Research Group privacy advocate. Bourassa had charged _The Globe_ with trying to find as much publicly-available financial information about him as possible. An article in _The Boston Globe_ about this incident asks where asset-research firms get their information from: "Does it come directly from financial institutions? Or does it come through more indirect, possibly illegal, methods?"

Category 38.2 *Trade in personal information*

2004-01-29 **technology Internet background checks dating**

NewsScan

SMILE, YOU'RE BEING GOOGLED

By making the mistake of dating a woman who knew how to use the Internet, fugitive LaShawn Pettus-Brown found himself jailed soon after the woman looked his name up in Google and found he was wanted by the FBI for alleged wire fraud. Use of the Internet for background checks is gaining a lot of popularity in the dating world, so stop doing whatever it is you're doing wrong, or restrict yourself to dating Luddites. (USA Today 29 Jan 2004)

Category 38.2 *Trade in personal information*

2004-03-08 **background checks prospective employees product security privacy**

NewsScan

BACKGROUND CHECK-IN-A-BOX

ChoicePoint is marketing a new product aimed at security-conscious employers who want to make sure their new hires are trouble-free. Stacked between gallon jars of mayonnaise and office furniture at Sam's Club, the ChoicePoint check-in-a-box package urges shoppers to "make better hiring decisions" by purchasing the $39.77 product, which contains a CD-ROM that allows users to tap into ChoicePoint's online databases. The new marketing effort signals data vendors' shift toward small businesses, which have lagged behind large corporations in conducting criminal background checks when hiring. Privacy advocates warn that such products put too much information at the fingertips of anyone with $40 to spend, and argue that ChoicePoint's requirement that users have a business license provides inadequate safeguard against the product's abuse. "If Joe's Bait Shop… goes out and buys this thing with a business license and then he wants to find out information about a neighbor, then he would be able to essentially do that," says the head of the Georgia Association of Professional Private Investigators. (AP 8 Mar 2004)

Category 38.2 *Trade in personal information*

2004-03-19 **consumer data sales Australia privacy profiling**

NewsScan

SALES OF CUSTOMER DATA RILE AUSTRALIAN TELECOM USERS

Australian telecommunications service providers are selling customer information to other companies for direct marketing and other commercial activities, according to the Australian Communications Authority. Acting ACA chairman Bob Horton cites evidence that customers' information is being collected by producers of public number directories and collated with data from other sources to create consumer "profiles": "Current use of telecommunications customer data appears to go beyond what is allowed under existing legislation. In fact, our investigations indicate that databases are being created and maintained based on information provided by customers to their telecommunications service providers. These databases are then sold to other companies for direct marketing and other commercial activities. In the ACA's opinion, this is not only a breach of existing law but also outside what customers providing personal information expect to happen." (The Age 19 Mar 2004, rec'd from John Lamp, Deakin University)

Category 38.2 *Trade in personal information*

2004-04-03 **Google Gmail e-mail service policy privacy issues**

NewsScan

PRIVACY ADVOCATES TARGET GOOGLE'S GMAIL STORAGE POLICY

Privacy advocates are voicing concern over Google's data retention plans, following the search company's splashy launch of its free Gmail service last week. Google's Gmail privacy policy tells users: "The contents of your Gmail account are also stored and maintained on Google servers in order to provide the service. Indeed, residual copies of e-mail may remain on our systems, even after you have deleted them from your mailbox or after the termination of your account." The fact that e-mail records potentially could be combined with Google search cookies, designed to index users' searches through 2038, and an Orkut cookie that contains personal identification information, is what has privacy watchdogs worried. "Once users register for Gmail, Google would be able to make that connection, if it chose to," says Pam Dixon, head of the World Privacy Forum. "And if Google ever compared the two sets of data, there are some people who would be chilled and embarrassed." Archivist Daniel Brandt adds: "While Google brags that no humans will read your e-mails, the entire Gmail program will involve extensive automated profiling of you as an individual. Google will be sharing non-identifiable portions of your profile with anyone they choose. If the ownership of Google changes, or there is a merger, the entire personally-identifiable profile will be available to the new owners or partners." (The Register 3 Apr 2004)

Category 38.2 *Trade in personal information*

2004-05-20 **campaign contributions tracking privacy publication access neighborhoods**

http://www.nytimes.com/2004/05/20/technology/circuits/20dona.html?th

Fundrace.org provides detailed information on precisely who is giving exactly how much money to which political candidates. The information is public, in that it is registered by the Federal Election Commission and available on demand. However, the shift to Web-accessibility changes the theoretically public into the very public, and not everyone is pleased. Some observers worry about privacy; others about decreasing contributions if everyone's neighbors and employers can check up on political activity.

Category 38.2 *Trade in personal information*

2004-06-03 **data deceased ownership possession**

NewsScan

WHO GETS YOUR DATA WHEN YOU DIE?

When a deceased person's family members don't want to go to the time and effort of gaining access to the data on the person's computer, they simply erase the hard drive and get rid of the computer without ever knowing what was on it. The manager of one computer-repair service says, "We're probably wiping away a lot of memories. Most people want to give the computer away without worrying about someone else getting access to personal information. When they bring it in, they don't know what's on it and they don't seem to care." Of course, relatives may also be afraid that there may be e-mail messages or other things on the computer that they'd rather not see. Eric Thompson, founder of AccessData Corporation, suggests that sometimes it might be best to let some secrets go to the grave with the deceased: "When you break into computer files you're reconstructing a person's life, both the good and the bad." (New York Times 3 Jun 2004)

Category 38.2 *Trade in personal information*

2004-07-07 **private customer data privacy Hooked Phonics Federal Trade Commission FTC complaint settlement**

NewsScan

HOOKED FOR RENTING OUT PRIVATE CUSTOMER DATA

The Hooked on Phonics company, which markets learning systems, has settled a complaint by the Federal Trade Commission that the company rented out customer data to outside marketers even though it had promised on its Web site that it would keep the information private. The FTC's J. Howard Beales III says: "It's simple: If you collect information and promise not to share, you can't share unless the consumer agrees." But Chris Jay Hoofnagle of the Electronic Privacy Information Center criticizes the FTC on the grounds that the Agency is in effect pushing companies to have the fewest restrictions possible without alienating potential customers: "The obvious encouragement here is to not make promises. We think that approach is somewhat inflexible." (Washington Post 7 Jul 2004)

Category 38.2 *Trade in personal information*

2004-08-31 **ACLU American Civil Liberty Union Secret Service Website data sensitive**

NewsScan

ACLU DENIES MISCHIEF IN POSTING OF DELEGATE DATA

The Secret Service is investigating the posting on a Web site operated by an organization called the Independent Media Center of the personal information of delegates to the Republication National Convention in New York. The Center describes its activities as "passionate tellings of the
truth." The Secret Service, however, is concerned that posting of the delegate data could subject the delegates to harassment, acts of violence or identity theft. The American Civil Liberties Union is representing the Independent Media Center, and the ACLU's Ann Beeson says: "This type of
investigation is really a form of intimidation and a message to activists that they will pay a price for speaking out. The posting of publicly available information about people who are in the news should not trigger an investigation." (AP/USA Today 31 Aug 2004)

Category 38.2 *Trade in personal information*

2004-12-21 **wireless phone directory assistance Connecticut privacy consumer information**

NewsScan; http://www.usatoday.com/tech/wireless/phones/2004-12-21-mobile411_x.htm

CONTROVERSY OVER WIRELESS PHONE DIRECTORY

Connecticut Attorney General Richard Blumenthal wants the cellular phone industry to discard its plans to create a directory assistance system for wireless phone numbers because there are "too many unknowns and dangers and too few protections at this point." But Kathleen Pierz, a Michigan analyst specializing in directory assistance counseling, says there are plenty of safeguards: "This is so buttoned up from a customer point of view, people don't have to worry. Blumenthal fears that a list of wireless numbers would inevitably be sold to telemarketers: "If the lists are there, they will be sold. They are so valuable. No cell phone company will resist the temptation to sell those lists for the huge profits." Pierz, however, points out that there is no marketing value to such lists because of existing federal laws preventing entities from calling a cell phone. (AP/USA Today 21 Dec 2004)

Category 38.2 *Trade in personal information*

2005-03-15 **privacy central federal government database identification authentication sabotage corruption integrity**

RISKS 23 79

CENTRALIZED PRIVACY RIGHTS MECHANISM RAISES SECURITY QUESTIONS

Curt Sampson contributed useful pointers and serious questions about a proposal for a central registry for protecting information privacy:

>Bruce Schneier, on his blog recently, mentioned the paper "A Model Regime of Privacy Protection" by Daniel J. Solove & Chris Jay Hoofnagle. His link and discussion is at
http://www.schneier.com/blog/archives/2005/03/ideas_for_priva.html

The paper's abstract and a link to download it can be found at
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=681902

There are a lot of good ideas in this paper, but one in particular struck me as potentially unwise, and certainly underdeveloped:

In conjunction with the universal notice, the FTC shall develop a centralized mechanism for people to exercise their rights with respect to their personal information. Such a mechanism would mimic the Do Not Call website, which allows individuals to opt-out of telemarketing and verify their enrollment by visiting a single website.

Many interesting RISKS are raised by this. How do you identify the people in the opt-out registry? How do you authenticate requests to deny distribution of certain information? (A malicious person might try to cause difficulties for someone by forging a request to deny all credit data to potential lenders.) How do you determine who may or may not search the registry or read information in it? How do you keep this from acting as the "central key" to all the information on a person, effectively moving us closer to having One Central Database, with all of the problems that brings?

There's a huge can of worms here waiting to be opened.

Personally, my first instinct would be to avoid such a central registry and instead make it the responsibility of the data collectors to contact each individual with information about what they're collecting and how they're using it, and solicit permission to do so, as well as offer the ability to review the information. This avoids any centralized system, and also avoids certain types of error. For example, if I'm contact regarding a file that appears to have nothing to do with me, I can point that out, rather than have a company mistakenly believe that this file does correspond with my life. (Or I might just say it does, and use the information for identity theft. Who knows?)<

Category 38.2 *Trade in personal information*

2005-03-23 **US Department of Education national database college students criticism civil liberties privacy concerns Social Security Numbers**

EDUPAGE; http://www.insidehighered.com/news/2005/03/23/unit

CRITICISM MOUNTS FOR FEDERAL STUDENT DATABASE

The U.S. Department of Education has proposed creating a national database of college students, but the idea has drawn heavy criticism for its use of Social Security numbers to identify individuals. The current system for reporting student progress, the Integrated Postsecondary Education Data System, reports aggregate data for institutions and cannot accurately track students who start at one college or university and transfer to another. The proposed database would track individuals, offering more accurate data for graduation rates and other statistics, but some argue that those gains would come at the expense of student privacy. David Baime, vice president of government relations for the American Association of Community Colleges, said that despite the benefits to community colleges in particular from such a system, his organization opposes the plan "primarily due to privacy concerns, expressed to us by our members." David L. Warren, president of the National Association of Independent Colleges and Universities, said, "The proposal takes us down the slippery slope toward Big Brother oversight of college students, and of those same citizens beyond their college years." Inside Higher Ed, 23 March 2005

Category 38.2 *Trade in personal information*

2005-06-23 **privacy Social Security Numbers SSN database recruitment privacy security safety system design**

RISKS 23 93

DoD MILITARY RECRUITMENT DATABASE INCLUDES SSN

The Defense Department has begun working with BeNow Inc, a private marketing firm, to create a database of high school students ages 16 to 18 and all college students to help the military identify potential recruits in a time of dwindling enlistment in some branches.

The program is provoking a furor among privacy advocates. The new database will include personal information including birth dates, Social Security numbers, e-mail addresses, grade-point averages, ethnicity and what subjects the students are studying.

Chris Jay Hoofnagle, West Coast director of the Electronic Privacy Information Center, called the system "an audacious plan to target-market kids, as young as 16, for military solicitation." He added that collecting Social Security numbers was not only unnecessary but posed a needless risk of identity fraud. Theft of Social Security numbers and other personal information from data brokers, government agencies, financial institutions and other companies is rampant. "What's ironic is that the private sector has ways of uniquely identifying individuals without using Social Security numbers for marketing."

The Pentagon statements said the military is "acutely aware of the substantial security required to protect personal data," and that Social Security numbers will be used only to "provide a higher degree of accuracy in matching duplicate data records."

[Abstract by Peter G. Neumann]

Category 38.2 *Trade in personal information*

2005-06-23 **Department of Defense DoD student database EPIC civil liberties privacy concerns trade in consumer information**

EDUPAGE; http://www.insidehighered.com/news/2005/06/23/database

DEFENSE DEPARTMENT TO CREATE VAST STUDENT DATABASE

Officials at the U.S. Department of Defense (DoD) have proposed the creation of a database containing information on virtually every college student in the country, as well as many high school students. Intended as a tool to aid recruitment efforts, the database would include names, phone numbers, Social Security numbers, addresses, birth dates, ethnicities, grade point averages, and other data. The DoD's database bears similarities to another database proposed by the Department of Education. That database would track individual students through their college careers, providing a clearer picture of graduation rates than current records, which track only aggregate rates from institutions. The Education Department's proposed database has drawn criticism from privacy advocates, who see it as a potential risk to privacy. The DoD proposal has similarly elicited complaints from groups such as the Electronic Privacy Information Center (EPIC). According to EPIC, the database would be a "bad idea," putting tools of direct marketers in the hands of government officials but without affording consumers the same protections from government that they enjoy from marketers. Inside Higher Ed, 23 June 2005

Category 38.2 *Trade in personal information*

2005-07-08 **EPIC data broker investigation FTC cell phone records trade in personal information**

EDUPAGE; http://online.wsj.com/article/0,,SB112077534843280100,00.html

EPIC CALLS FOR INVESTIGATION OF DATA BROKERS

The Electronic Privacy Information Center (EPIC) this week filed a complaint with the Federal Trade Commission (FTC) asking the agency to investigate the business practices of companies that sell information such as cell phone records. The complaint focuses on a company called Intelligent e-Commerce Inc., which sells information including cell phone records and the identities of holders of post office boxes. In its complaint, EPIC contends that the collection and sale of such information likely violates federal regulations or statutes and asks the FTC to force Intelligent e-Commerce to discontinue the sale of such information pending a full investigation. According to EPIC, some data brokers obtain information fraudulently by pretending to be someone who is authorized to access that information. A spokesperson for Intelligent e-Commerce Inc. said company officials and attorneys are not aware of any laws that they are breaking. Wall Street Journal, 8 July 2005 (sub. req'd)

Category 38.2 *Trade in personal information*

2005-09-09 **civil liberties privacy organization United Kingdom UK EFF Open Rights Group ORG**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4225938.stm

DIGITAL RIGHTS ORGANIZATION OPENS IN UK

Modeled on the Electronic Frontier Foundation (EFF) in the United States, a new organization is being launched in the United Kingdom to protect the rights of users of digital resources. According to the Web site of the Open Rights Group (ORG), the group will work to "vigorously defend our digital civil liberties, ensuring that the our hard-won freedoms are not taken away simply because they've moved to the digital world." Suw Charman, one of the group's co-founders, said that ORG intends not to replace but to work alongside organizations with similar goals, of which several already exist in the United Kingdom and Europe, including the Campaign for Digital Rights, the Foundation for Information Policy Research, and the Foundation for a Free Information Infrastructure. Officials from the rights group Citizens Online expressed skepticism that ORG efforts would be appropriately inclusive. Citizens Online worried that ORG's focus would be "middle class" issues, ignoring technology issues concerning people with disabilities and the digital divide. BBC, 9 September 2005

Category 38.2 *Trade in personal information*

2006-01-12 **surveillance privacy law enforcement cell mobile phone records logs**

RISKS 24 15

CELL PHONE CALL RECORDS FOR SALE TO ANYONE

Locatecell.com seems to have a good thing going. According to this Chicago Sun Times story:

To test the service, the FBI paid Locatecell.com $160 to buy the records for an agent's cell phone and received the list within three hours, the police bulletin said.

Representatives of Data Find Solutions Inc., the Tennessee-based operator of Locatecell.com, could not be reached for comment.

Frank Bochte, a spokesman for the FBI in Chicago, said he was aware of the Web site.

"Not only in Chicago, but nationwide, the FBI notified its field offices of this potential threat to the security of our agents, and especially our undercover agents," Bochte said.

Funny how the FBI's first reaction is to go on the defensive. Funny how this is a big surprise to the FBI.

The Chicago Sun-Times paid $110 to Locatecell.com to purchase a one-month record of calls for this reporter's company cell phone. It was as simple as e-mailing the telephone number to the service along with a credit card number.

Locatecell.com e-mailed a list of 78 telephone numbers this reporter called on his cell phone between Nov. 19 and Dec. 17. The list included calls to law enforcement sources, story subjects and other Sun-Times reporters and editors.

Cheating spouse? Disloyal employees? Need to find out what your competition is doing? Hey, no problem. Telecom services are just information services these days.

[Contributed by Lauren Weinstein]

Category 38.2 *Trade in personal information*

2006-01-27 **ChoicePoint FTC settlement sensitive personal data disclosure**

EDUPAGE; http://www.nytimes.com/2006/01/27/business/27choice.html 23

CHOICEPOINT SETTLES WITH FTC

Data broker ChoicePoint has reached a $15 million settlement with the Federal Trade Commission (FTC) following the company's disclosure a year ago that it had turned over sensitive personal data for about 150,000 people to bogus customers. The FTC alleged that ChoicePoint did not have adequate procedures in place to prevent such fraud and that the company ignored what should have been red flags about the identity of the customers requesting data, including credit reports. ChoicePoint, which has over the past year taken steps to address the problems that led to the incident, said it disagrees with some of the FTC's findings but supports the settlement. The settlement covers a $10 million fine, the largest ever meted out by the FTC, and $5 million that will be held in an account and used to reimburse consumers who can demonstrate losses due to the ChoicePoint incident. Sen. Charles Schumer (D-N.Y.), who introduced tough legislation to regulate the data-brokerage industry after the ChoicePoint scandal, said he thinks the fine was too low and will encourage others to see such penalties as "just the cost of doing business."

Category 38.2 *Trade in personal information*

2006-02-08 **privacy protection private phone record Website shut down FTC EPIC**

DHS IAIP Daily; http://www.nytimes.com/aponline/technology/AP−Phone− Records. html?_r=1&oref=slogin 23

WEBSITES HAWKING PHONE RECORDS SHUT DOWN.

Following a wave of negative publicity and pressure from the government, several Websites that peddled people's private phone records are calling it quits. "We are no longer accepting new orders" was the announcement posted Wednesday, February 8, on two such sites, locatecell.com and celltolls.com. The Federal Trade Commission (FTC) this week conducted a sweep of 40 sites known to have been selling private phone records. According to the FTC's Lydia Parnes, more than 20 sites have recently shut down or stopped advertising for new business. The agency has sent letters to about 20 other sites, warning them that they may be violating the law and should review their business practices, said Parnes, director of the FTC's Bureau of Consumer Protection. While some sites appear to be closing up shop, others have seen a boom in business with the recent media attention, said Marc Rotenberg, executive director of the Electronic Privacy Information Center. Rotenberg urged lawmakers to ban a practice known as "pretexting," in which data brokers or others call a phone company, impersonate a customer and then persuade the company to release the calling records.

Category 38.2 *Trade in personal information*

2006-03-21 **IRS Internal Revenue Service tax information brokers marketers privacy confidentiality control opt-in sharing liability responsibility**

RISKS; Philadelphia Inquirer http://tinyurl.com/puqul ; MediaMatters http://tinyurl.com/k2t29 24 21

IRS PLANS TO ALLOW TAX-PREPARERS TO SELL CLIENT DATA

Chris Hoofnagle reported in RISKS on news that the IRS was pushing for new rules allowing commercial tax preparers to sell information from tax returns. "If consent is given, the FULL RETURN can be given to other entities for marketing purposes, and the tax preparer does not have to even ensure that these other entities are legit or following the preparer's privacy policy."

Jeff Gelles of the Philadelphia Inquirer wrote, "The change is raising alarm among consumer and privacy-rights advocates. It was included in a set of proposed rules that the Treasury Department and the IRS published in the Dec. 8 Federal Register, where the official notice labeled them 'not a significant regulatory action.' IRS officials portray the changes as housecleaning to update outmoded regulations adopted before it began accepting returns electronically. The proposed rules, which would become effective 30 days after a final version is published, would require a tax preparer to obtain written consent before selling tax information. Critics call the changes a dangerous breach in personal and financial privacy. They say the requirement for signed consent would prove meaningless for many taxpayers, especially those hurriedly reviewing stacks of documents before a filing deadline."

Media watchdog MediMatters For America reported that "On the CBS Evening News, Washington correspondent Bob Orr characterized a recent Internal Revenue Service (IRS) regulations proposal allowing tax return preparers to sell information from returns to third parties as spelling out a 'loophole of sorts' that has 'been around for more than 30 years.' In fact, in permitting sales to third parties, the new proposal would allow tax preparers to do something they are not currently permitted to do; under current law, they can pass on such information only to affiliates."

The US Public Interest Research Group (U.S. PIRG) established a Web site to cover this developing issue. < http://www.uspirg.org/uspirg.asp?id2=24620 >

38.3 Industry efforts for individual privacy protection

Category 38.3 *Industry efforts for individual privacy protection*

1997-07-21 **bank privacy policy ABA**

AP

The American Bankers Association promulgated a set of principles governing client privacy at its directors' meeting in Colorado Springs in late July. The principles included the following good ideas:
— Recognition of a customer's expectation of privacy.
— Customer information should be used, collected and retained only if the bank believes the customer would benefit.
— Maintenance of accurate information.
— Limiting bank employee access to customer information.
— Information should be protected by established security procedures.
— Disclosure of account information should be restricted.
— Customer privacy should be maintained in dealings with third parties.
— A bank should make its privacy policies known to its customers.

Category 38.3 *Industry efforts for individual privacy protection*

1999-04-21 **privacy seal certification online Internet Web credit report**

CNET News.com http://www.news.com/News/Item/0,4,35487,00.html

A firestorm erupted when the Better Business Bureau Online granted a seal of approval to Equifax, a major credit-rating agency that has been the bête noire of the privacy lobby for years. Critics pointed out that both the BBB Online and Truste seals refer exclusively to Web sites and ignore privacy violations carried out by firms using other modalities.

Category 38.3 *Industry efforts for individual privacy protection*

1999-06-22 **advertising marketing privacy policy Web**

AP

MICROSOFT TO REQUIRE PRIVACY PACTS
Microsoft on Wednesday is expected to announce that it will no longer buy ads on Webs sites that fail to provide sufficent privacy safeguards for consumers. Microsoft, the leading Web advertiser, is following the lead of IBM, the Web's second largest advertiser, which less than three months ago made a similar announcement. Microsoft has lobbied against federal privacy legislation, and offers a free toolkit for users designed to limit the amount of information Web sites collect. Microsoft's new privacy policy will take effect beginning next year; the company spent about $30 million last year on Web ads, still a small fraction of the $2 billion that was spent overall on Web ads. Although recent surveys show a major improvement in the privacy practices of Web sites, the FTC is studying what recommendations it plans to make to Congress regarding new privacy laws. (Associated Press 06/22/99)

Category 38.3 *Industry efforts for individual privacy protection*

2000-03-31 **Web privacy consumer profiling FTC investigation**

NewsScan

Yahoo Inc. has notified the Securities and Exchange Commission that it had volunteered to cooperate with an inquiry by the Federal Trade Commission into how Web sites gather and use personal information. Insisting that it takes its privacy policies seriously, the company says that the discussions have "nothing to do with advertising profiling" but has declined to elaborate on the scope of those discussions. Most Web sites gather personal data about their visitors not to collect information about individuals but to determine broad demographic characteristics that will attract advertisers who want to target their messages to prescreened audiences. (New York Times 31 Mar 2000)

Category 38.3 *Industry efforts for individual privacy protection*

2000-04-16 **data privacy children kids identification**

NewsScan, San Jose Mercury News
http://www.sjmercury.com/svtech/news/breaking/ap/docs/432874l.htm

Eric Shen, a policy analyst with the Electronic Privacy Information Center in the capitol, calls the new federal privacy law requiring that Web sites get parental permission before collecting personal information on kids, is "a serious first step" but says it also has a serious defect, because sites can evade the law merely by not asking hold old users are. But Mozelle Thompson of the Federal Trade Commission argues: "Sure, there are ways around it. But that doesn't mean you don't put a few speed bumps in." (AP/San Jose Mercury News 16 Apr 2000)

Category 38.3 *Industry efforts for individual privacy protection*

2000-06-07 **privacy consortium industry self-regulation organization consortium**

NewsScan, Los Angeles Times
http://www.latimes.com/business/20000607/t000053796

A seven-member coalition of leading high-tech companies . . . [proposed] a new system aimed at protecting consumers from online fraud and privacy intrusions in cyberspace. The group, which includes America Online, AT&T, Dell, IBM and Microsoft, has developed voluntary guidelines that would require merchants to clearly spell out the terms and conditions of a sale, make reasonable efforts to protect consumer privacy, and provide for "fair, timely and affordable" dispute resolution. The move is seen as a strategy to allay consumers' fears and ward off further intervention by government regulators at a time when the Federal Trade Commission is pushing for expanded powers to regulate industry Web sites, and several bills in Congress seek to increase consumer protections against cyberscams and privacy abuses. Although . . . [fewer] than 20% of Web sites post privacy policies, polls have found that privacy is the No. 1 concern of online users. (Los Angeles Times 7 Jun 2000)

Category 38.3 *Industry efforts for individual privacy protection*

2000-07-20 **cookies privacy monitoring consumer profiling Web software countermeasures**

NewsScan, San Jose Mercury News
http://www.sjmercury.com/svtech/news/breaking/internet/docs/218367l.htm

Microsoft is about to begin testing new software to allow users of its Internet Explorer software to receive alerts when there is an attempt to place "cookies" on their hard disks by Web sites they visit. Cookie trails are used by many sites to follow the travels of Web surfers in order to provide them with personalized content and/or targeted advertising. The new Microsoft software, which will be released to the public for beta testing within the next month, is also intended to give consumers an easy way to manage and delete cookies. (Reuters/San Jose Mercury News 20 Jul 2000)

Category 38.3 *Industry efforts for individual privacy protection*

2001-09-23 **national identification systems ID card terrorism surveillance**

NewsScan

ELLISON PROPOSES NATIONAL IDENTIFICATION SYSTEM [23 Sep 2001]

Oracle chief executive Larry Ellison says that America needs to create a national identification card system, and is offering to donate Oracle's database software to make such a system possible: "We need a national ID card with our photograph and thumbprint digitized and embedded in the ID card. We need a database behind that, so when you're walking into an airport and you say that you are Larry Ellison, you take that card and put it in a reader and you put your thumb down and that system confirms that this is Larry Ellison." Asked about privacy concerns, he responded: "Well, this privacy you're concerned about is largely an illusion. All you have to give up is your illusions, not any of your privacy. Right now, you can go onto the Internet and get a credit report about your neighbor and find out where your neighbor works, how much they earn and if they had a late mortgage payment and tons of other information." Ellison argues that shoppers now have to disclose more information to make a purchase at a shopping mail than they do to get on an airplane, and poses the following question: "Let me ask you. There are two different airlines. Airline A says before you board that airplane you prove you are who you say you are. Airline B, no problem. Anyone who wants the price of a ticket, they can go on that airline. Which airplane do you get on?" (San Jose Mercury News 23 Sep 2001)
http://www.siliconvalley.com/docs/news/svfront/ellsn092301.htm

---

Category 38.3 *Industry efforts for individual privacy protection*

2001-12-10 **corporate privacy policy P3P Platform for Privacy Preferences legal liability Microsoft MS browser IE6 Internet Explorer**

RISKS 21 82

Attorney Ben Wright noted in RISKS that the new defaults in MS Internet Explorer version 6 may pose a problem for corporations:

"The filters force administrators to post new privacy policies for their Web sites, coded in a technical language called P3P. The filters punish administrators who fail to publish properly coded P3P privacy policies by blocking or impeding their cookies.

The P3P coding language raises, for any corporation, government agency or other institution that uses it, a lawsuit danger. A privacy policy written in it exposes the organization to liability, with little or no escape.

A privacy policy, even one written in computer codes, can be legally enforceable like a contract. In lawsuits filed in 1999, plaintiffs forced US Bancorp to pay $7.5 million for misstatements in a privacy policy posted on its Web site.

Web administrators face a dilemma. They want to satisfy IE 6's technical requirement for P3P codes, but they also want to sidestep liability. See Webserver Online Magazine article: < http://webserver.cpg.com/news/6.12/n5.shtml>

One solution is to deploy dummy P3P codes, with an extra legal code that disavows any liability for the codes, as explained at < http://www.disavowp3p.com>."

Category 38.3 *Industry efforts for individual privacy protection*

2002-02-05 **e-commerce trust certification reliability credibility fraud online shopping**

NewsScan

BETTER BUSINESS BUREAU TARGETS ONLINE PRIVACY WITH NEW SITE
The Better Business Bureau has launched a new Safe Shopping Web site that enables consumers to locate online companies that have met BBB standards for privacy in e-commerce. Visitors to http://www.bbbonline.org/consumer/ will find nearly 11,000 Web sites that have earned one or both of the BBBOnline Privacy and Reliability seals. A recent survey showed that almost 90% of consumers would feel safer making a purchase from an online company that displays one of the seals than from a company that does not, according to Greenfield Online. "The BBB system will encourage the business community to step up to the plate and meet consumer expectations regarding online privacy," says Ken Hunter, president and CEO of the Council of Better Business Bureaus and BBBOnline. (E-Commerce Times 4 Feb 2002)
http://www.ecommercetimes.com/perl/story/16149.html

Category 38.3 *Industry efforts for individual privacy protection*

2002-03-05 **anonymizer quality assurance QA compromise vulnerability design flaw analysis**

RISKS, http://www.cs.bu.edu/techreports/pdf/2002-003-deanonymizing-safeweb.pdf 21 93

David Martin of Boston University reported on his group's analysis of the SafeWeb anonymizer service (which went out of business in December 2001 but whose technology was licensed to other firms). The analysis showed that the service did protect anonymity. However, despite the company's assurances about security, in fact the service opened users to serious compromise through errors in the service's design.

The simplicity of the errors is startling. Martin summarizes the situation as follows (quoting):
>First a quick SafeWeb overview: a SafeWeb user types in a URL. It goes to safeweb.com within an SSL connection; SafeWeb sanitizes the requested content and delivers it back to the browser. The origin server Web site only sees a connection from safeweb.com, and eavesdroppers near the user only see an encrypted connection to safeweb.com On-screen, SafeWeb uses frames to separate the SafeWeb controls from the requested content. Let's call them the "control" and "content" frames.

Now let's meet the protections:
(1) simultaneously open windows or frames can only communicate with each other if they're from the same domain,
(2) scripts stop running when a new page is displayed, and
(3) cookies are available only to the domain that set them.

The problem is that both of SafeWeb's frames are served from the same tunnel (https://www.safeweb.com/) even though their content comes from radically different sources: the trusted SafeWeb site on the one hand, and the untrusted third party site on the other. Since both frames come from the same domain, the Web browser exposes each Document Object Model to the other: protection #1 is gone.

Since the control frame is basically static, it's a great place for an attacker to tuck away any code that needs to persist throughout the browsing session -- like spyware. So protection #2 is gone too.

SafeWeb also wanted to support pseudonymous persistent cookies. Since the content frame is always associated with a single privacy domain, they aggregated all of the pseudonymous cookies from sites a user might visit through SafeWeb into one "master cookie" associated with the fixed domain safeweb.com. That way, the individual cookies all get stored on the user's computer in a slightly different form, and SafeWeb doesn't have to maintain any persistent state on their servers (and users don't have to log in to SafeWeb, etc.). But this approach discards protection #3 as well.

To exploit these lost protections, an attacker has to take control of one of the frames: the content frame is the obvious choice. That turns out to be not too hard. SafeWeb *requires* that JavaScript be enabled in the browser. Recognizing the risk, SafeWeb tried to sanitize scripts delivered to the content frame, but they didn't go nearly far enough. The result? By choosing to use this privacy enhancing system, users become vulnerable to having their IP address revealed, *all* of their cookies stolen, and the remainder of their privacy-"enhanced" browsing session silently transmitted to an attacker in spite of the layer of SSL protection. This is not speculation; we have tested several effective exploits against the system.<

[MK comments: You would think that the designers would have asked for outside analysis before implementing these designs, no?

MORAL #1: Challenge your own security models.

MORAL #2: Don't assume that vendors have challenged their own security models.]

Category 38.3 *Industry efforts for individual privacy protection*

2002-04-04 **privacy policy interpretation tool translation alert freeware**

NewsScan

IBM AND AT&T GIVE AWAY WEB PRIVACY SOFTWARE
IBM is now giving away its Tivoli Privacy Wizard software, which transforms a Web [site's] written privacy policies into electronic guidelines for its own employees, and AT&T is giving away software that will alert Web surfers to different privacy settings on sites they visit. Internet users have consistently have consistently rated privacy issues high on their list of concerns about the Web. IBM acknowledges the skepticism of some privacy advocates and admits that the donated software won't deter deliberate privacy violations, but insists that it "may help reduce the all-too-frequent accidents in privacy" caused by a company's employees failing to understand or follow the company's written privacy policies. (Reuters/San Jose Mercury News 4 Apr 2002)
http://www.siliconvalley.com/mld/siliconvalley/2997058.htm

Category 38.3 *Industry efforts for individual privacy protection*

2003-06-25 **bill gates orwell 1984 security homeland computers**

NewsScan

GATES: ORWELL GOT IT BACKWARDS
"Orwell's vision didn't come true, and I don't believe it will," Microsoft chairman Bill Gates said this week in a speech commemorating the 100th anniversary of the birth of George Orwell, the English author whose works included the dystopian novel "1984." That novel described a repressive society of the future dominated by a figure called Big Brother, whose image was displayed on screens throughout the land. Gates said that, contrary to Orwell's fears, "This technology can make our country more secure and prevent the nightmare vision of George Orwell at the same time... At a time of increased uncertainty about homeland security, computers must be available wherever and whenever we need them... Not so long ago, most people paid little attention to cybercrime, but today there's a broader recognition that IT security is vital to homeland security. We must build higher walls and stronger vaults, and government must continue to step up the priority given to this kind of crime while protecting the privacy of consumers." (AP/Los Angeles Times 25 Jun 2003)

Category 38.3 *Industry efforts for individual privacy protection*

2003-10-28 **Orbitz security breaches online travel agency customers junk e-mail unauthorized spammers**

NIPC/DHS

October 28, CNET News.com — Orbitz investigates security breach.

Online travel agency Orbitz has notified law enforcement authorities about a recent security breach that has resulted in its customers' e-mail addresses falling into the hands of spammers, an Orbitz representative confirmed Tuesday, October 28. "A small number of customers have informed us that they have received spam or junk e-mail from an unknown party that apparently used unauthorized and/or illegal means to obtain their e-mail addresses used with Orbitz," spokeswoman Carol Jouzaitis said in a statement. "There is no evidence that customer password or account information has been compromised," she said. Orbitz found no indication that credit card information had been compromised, Jouzaitis added. Orbitz became aware of the problem "in the last day or so," Jouzaitis said.

Category 38.3 *Industry efforts for individual privacy protection*

2003-12-19 **RIAA music dowloaders Verizon copyrighted privacy**

NewsScan

APPEALS COURT STRIKES DOWN RIAA STRONGARM TACTICS
A U.S. appeals court has ruled that the strongarm tactics used by the Recording Industry Association of America to track down music downloaders are illegal. The RIAA had sought to force Internet service providers, including Verizon, to divulge the names of subscribers suspected of downloading copyrighted music files without permission. Verizon argued that existing copyright law does not give the recording industry the authority to enforce its subpoenas and said the RIAA's actions violated Verizon customers' privacy. A lower court had earlier upheld the RIAA's actions, but this latest ruling sided with Verizon: "In sum, we agree with Verizon that [the 1998 copyright law] does not by its terms authorize the subpoenas issued here," wrote Chief Judge Douglas Ginsburg. (Reuters/CNN.com 19 Dec 2003)

Category 38.3 *Industry efforts for individual privacy protection*

2004-06-09 **Ohio interstate scanning system license plate recognition**

NewsScan

OHIO'S TURNPIKE SCANNING SYSTEM

The Ohio State Highway Patrol will be using two scanners on turnpike gates and two scanners in patrol cars for four months, as they test a new system that recognizes license plates and matches them with a national crime database. The scanner company, Elsaq SpA, is based in Genoa, Italy. Jeff
Gamso of the Ohio ACLU worries that the scanners will invade the privacy of ordinary citizens: "It's a free society, and we're supposed to move as we like without the government tracking us everywhere." State Highway Patrol superintendent Paul McClellan says that if the scanners had been in place earlier this year, they might have detected the individual responsible for a number of sniper shootings on state highways. (AP/USA Today 9 Jun 2004)

Category 38.3 *Industry efforts for individual privacy protection*

2005-01-01 **eBay passport auction personal information names addresses credit card numbers**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=7217100

EBAY TO DISCONTINUE PASSPORT

Online auction site eBay has announced it will discontinue support of Microsoft's Passport service later this month. The service offers registered users a single location to store personal information including names, addresses, and credit card numbers. When shopping at online vendors participating in the service, users can access their profiles for transactions with just a single login. Since its debut in 1999, however, Passport has failed to live up to expectations, in part due to competition as well as to security concerns among consumers. In addition, retailers were slow to sign up for fear that Microsoft might begin charging fees to retailers for the service. A spokesperson from eBay said that the percentage of its customers who regularly signed in using Passport was "very small." Despite losing one of the largest online retailers in eBay, Microsoft said the Passport service will continue.

Category 38.3 *Industry efforts for individual privacy protection*

2005-03-25 **intellectual property entertainment policy initiative cooperation**

RISKS; http://www.eepi.org 23 81

EEPI - ELECTRONIC ENTERTAINMENT POLICY INITIATIVE

Long-time privacy advocate Lauren Weinstein wrote:

I'm pleased to announce "EEPI" (http://www.eepi.org), a new initiative aimed at fostering cooperation in the areas of electronic entertainment and its many related issues, problems, and impacts.

I've teamed with 30+ year recording industry veteran Thane Tierney in this effort to find cooperative solutions to technical, legal, policy, and other issues relating to the vast and growing range of electronic technologies that are crucial to the entertainment industry, but that also impact other industries, interest groups, individuals, and society in major ways.

There are many interested parties, including record labels, film studios, the RIAA, the MPAA, artists, consumers, intellectual freedom advocates, broadcasters, manufacturers, legislators, regulators, and a multitude of others.

The issues cover an enormous gamut from DVDs, CDs, and piracy issues to multimedia cell phones, from digital video recorders to Internet file sharing/P2P, from digital TV and the "broadcast flag" to the Digital Millennium Copyright Act (DMCA) and "fair use" controversies.

Working together, rather than fighting each other, perhaps we can all find some broadly acceptable paths that will be of benefit to everyone.

For more information, please see the EEPI Web site at:

http://www.eepi.org

A moderated public discussion list and an EEPI announcement list are now available at the site.

Public participation is cordially invited. Thank you very much.

Lauren Weinstein lauren@pfir.org or lauren@vortex.com or lauren@eepi.org +1 (818) 225-2800
http://www.eepi.org
http://www.pfir.org/lauren
http://lauren.vortex.com
http://www.pfir.org
http://www.vortex.com

Category 38.3 *Industry efforts for individual privacy protection*

2005-10-04 **client server model remote processing history merger policy privacy officer searches records copyright intellectual property**

RISKS 24 06

GOOGLE PRIVACY POLICIES NEED REFINEMENT

Lauren Weinstein published an open letter berating Google (and Sun Microsystems) for Google's lack of privacy policies. Among other sins, he cited these [MK quoting liberally from LW's letter]:

* Google keeps records of your searches, and can tie them to other activities via cookies. Google scans the e-mail you send and receive through Gmail. Google collects a variety of information on your other browsing activities through various optional toolbars and services.

* Google wants to make copies of copyrighted books without paying for them. Arguments about how they might make "snippets" of such materials available in "Google Print" aside, the internal R&D value alone of that collection to Google would presumably be immense, and all without sending a dime to the copyright holders.

* When CNET ran a story using Google to research data on Google's chief exec, Google reacted like an enraged and petulant child.

* Now, with the new Sun Micro deal, if hosted versions of word processing and related applications are developed and deployed by the joint Google and Sun team, Google could quite possibly be tied into your document editing and other Office-like activities if you use such services.

* Google refuses to hire a privacy officer (after all, they're the "Trust us -- First do no evil" company, and they're smarter than everyone else about… well… everything, right?)

* Google refuses to detail their data retention policies or the extent to which they make that growing corpus of data available to outside entities.

*…Sun's Scott McNealy … has famously said: "You have no privacy, get over it" and … suggested that consumer privacy is a "red herring" issue.

Weinstein urged Google and Sun to consult with the privacy community and personally offered to help. However, he wrote, "I won't be holding my breath waiting for their call."

Category 38.3 *Industry efforts for individual privacy protection*

2006-01-30 **industry vendor effort anti-spyware TrendMicro Symantec McAfee ICSA Thompson Cyber Security Lab sharing**

DHS IAIP Daily; http://www.theregister.co.uk/2006/01/30/spyware_testing/ 23

SECURITY VENDORS OPEN ANOTHER FRONT AGAINST SPYWARE.

The three biggest anti-virus vendors have teamed up with testing labs to develop standards for spyware detection. Trend Micro, Symantec and McAfee are joining forces with ICSA Labs and Thompson Cyber Security Labs in a bid to standardize methods for sharing spyware samples and testing anti-spyware products and services. The effort is aimed at curtailing a possible source of user confusion before it becomes a problem, as well as driving up standards for detection across the anti-spyware industry. Spyware testing, modeled on schemes the anti-virus industry has been running for years, will also make it easier to compare the efficacy of various anti-spyware products, at least in theory. The group's anti-spyware testing methodology and best practices can be viewed at Spywaretesting.org. The initiative is one of a number of cross industry efforts aimed at coordinating the fight against spyware -- the invasive programs that track user's surfing habits or, in the worst cases, steal their personal information, such as credit card or Social Security numbers. Spywaretesting Website: http://www.spywaretesting.org/metadot/index.pl

---

Category 38.3 *Industry efforts for individual privacy protection*

2006-02-10 **EFF warning Google Desktop remote information file storage hacker target**

DHS IAIP Daily; 23
http://security.ithub.com/article/EFF+Dont+Use+Google+Desktop/171267_1.aspx

EFF: DON'T USE GOOGLE DESKTOP.

A high-profile privacy watchdog group has a terse warning for business and consumer users: Do not use the new version of Google Desktop. The nonprofit Electronic Frontier Foundation (EFF) said a new feature added to Google Desktop on Thursday, February 9, is a serious privacy and security risk because of the way a user's data is stored on Google's servers. The new "Share Across Computers" feature stores Web browsing history, Microsoft Office documents, PDF and text files on Google's servers to allow a user to run remote searches from multiple computers, but, according to the EFF, this presents a lucrative target to malicious hackers. Google said users can use a "Clear my Files" button to manually remove all files from its servers or a "Don't Search These Items" preference to remove specific files and folders from the software's index.

38.4 International agreements on security, individual privacy, Net law

Category 38.4 *International agreements on security, individual privacy, Net law*

2000-01-12 **international negotiations discussion conflict regulations European Privacy Directive USA**

Edupage, Financial Times, EPIC Alert

The US government met with European Union officials in mid-January 2000 to discuss the ongoing conflict over the strict EU Privacy Directive. Back on November 15, 1999, the US delegation released the latest in a two-year series of proposals called the Safe Harbor Principles, designed to allay privacy concerns of the Europeans. US negotiators hoped to convince the more government-tolerant Europeans that industry self-regulation would be a reasonable method for protecting citizen privacy.

Category 38.4 *International agreements on security, individual privacy, Net law*

2000-03-14 **EC European Commission Privacy Directive international agreement Safe Harbor**

NewsScan, CNet http://news.cnet.com/news/0-1007-200-1571726.htm

The European Union and the U.S. have agreed on regulations covering personal data collected electronically, following months of negotiations aimed at reconciling the disparity in privacy protection laws in the two regions, and giving a boost to trans-Atlantic e-commerce. The new regulations, which require U.S. companies to comply with European rules, are expected to go into effect in June or July. Failure to comply will be considered a deceptive business practice and a prosecutable offense. U.S. companies can cooperate in one of four ways: by reporting to a data authority in Europe, by agreeing to be monitored by U.S. authorities; by joining a self-regulatory body, which will be monitored by the FTC; or by agreeing to rules set by a European panel of data privacy officials. The U.S. Commerce Department will keep a list of industry self-regulators and will provide oversight to ensure they comply with privacy rules. (Bloomberg/CNet 14 Mar 2000)

Category 38.4 *International agreements on security, individual privacy, Net law*

2000-06-22 **privacy monitoring surveillance organization industry grouping standard protocol P3P**

NewsScan

Though derided by some of its critics as "too little, too late" and as "complex and confusing," a new protocol for protecting individual privacy on the Web has been introduced by the World Wide Web Consortium (W3C), a standards organization, along with AT&T labs, major companies that include IBM, Microsoft and AOL, and the online civil liberties group Center for Democracy and Technology. The new standard, called Platform for Privacy Preferences (P3P), sets standards to allow your browser to automatically read the posted privacy policies of Web sites and alert you before going to any Web site that collects more information about you than you are willing to give. (New York Times 22 Jun 2000)

Category 38.4 *International agreements on security, individual privacy, Net law*

2000-10-17 **spying eavesdropping industrial espionage network monitoring international wiretapping artificial intelligence AI lawsuit European surveillance covert action**

NewsScan, USA Today http://www.usatoday.com/life/cyber/nb/nb4.htm

[In February, there was news that France would sue the British and US governments over the use of Echelon.] In October, a Green Party member of the European Parliament has filed criminal charges in Germany against "Echelon," the secret international computer surveillance system that monitors most voice and data traffic circulating in Western countries. In 1997 the Covert Action Quarterly, an intelligence newsletter, said: "Unlike many of the electronic spy systems developed during the Cold War, Echelon is designed primarily for non-military targets: governments, organizations, businesses, and individuals in virtually every country. It potentially affects every person communicating between (and sometimes within) countries anywhere in the world." (Newsbytes/USA Today 17 Oct 2000)

Category 38.4 *International agreements on security, individual privacy, Net law*

2001-08-16 **international privacy guidelines Web standards audit failure study**

NewsScan

U.S. WEB SITES FALL SHORT OF GLOBAL PRIVACY STANDARDS
A survey of 75 U.S. corporate Web sites found that none were in compliance with a set of international privacy guidelines developed by the U.S. and the European Union last year. The guidelines require companies to: notify consumers how their personal data is used; use the information only for its stated purpose; allow consumers to examine and correct data collected about them; give consumers an option to forbid sharing that data for marketing purposes; store the data in a secure manner; and provide recourse for consumers whose privacy has been violated. The survey, conducted by Andersen, found that travel and leisure companies scored the best on notice and security provisions, while financial services firms were most likely to offer adequate choice. U.S. companies must make progress on revamping their Web privacy standards or "Disruption to the conduct of business is a real risk," says Andersen principal Kerry Shackelford. (Reuters 16 Aug 2001)
http://news.excite.com/news/r/010816/11/net-tech-privacy-dc

Category 38.4 *International agreements on security, individual privacy, Net law*

2003-02-12 **European cybersecurity agency proposal cope cyber crime co-ordination**

NIPC/DHS

February 10, IDG News Service — European cybersecurity agency proposed.

The European Commission Monday proposed the creation of a Europe-wide network and information security agency. The European Network and Information Security Agency is to serve as an advice center for the fifteen member states on matters relating to cybersecurity, such as computer viruses, Erkki Liikanen, commissioner for the information society, said. Until now, viruses have largely been propagated by young individuals and amateurs, but in the post-September 11 era there is a risk of worse attacks, he said. Mobile Internet connections, through mobile phones in particular, are expected to increase the risk of serious attacks, Liikanen said. The Commission has earmarked a ï¿½24.3 million ($26.3 million) budget for the agency over a five-year period, with an additional $9 million planned to include the 10 new member states, mainly from Central Europe, in May 2004. Individual member states have already established crisis units (known as Computer Emergency Response Teams) in an effort to cope with increasing cyber crime. However, the current system lacks central coordination. The agency is due to start operating next January. The governments of the 15 member states will decide on a location later this year, Liikanen said.

Category 38.4 *International agreements on security, individual privacy, Net law*

2003-09-16 **internet management ICANN international body UN intergovernmental organizations**

NewsScan

BATTLE IS BREWING OVER NET MANAGEMENT
Two camps with opposing views on Internet management are emerging, setting the stage for discord at the upcoming UN-backed World Summit on the Information Society in December. "Some governments are arguing that the management of things like (Internet protocol) addressing, global domain names and privacy should be done by an intergovernmental organization because the feel the Internet is a public resource, and they have responsibility over public resources," says Mohammed Sharil, chairman of the government advisory committee for ICANN (the Internet Corporation for Assigned Names and Numbers). "Then there are some governments who feel that the Internet should be managed by an international body. International by definition means everyone is involved, from governments to private sector and civil society. Whereas intergovernmental gives an indication that only governments are involved and not necessarily people." Sharil says many countries in the Asia-Pacific region prefer an independent international managing body, whereas some in Europe and the Middle East favor an intergovernmental organization. The issue is currently under debate as the wording of a key article to be adopted at the summit is hammered out. "Positions are shifting all the time," says Sharil, who adds that ICANN will not take a position on the subject. (Reuters/CNet 16 Sep 2003)

Category 38.4 *International agreements on security, individual privacy, Net law*

2003-11-14 **windows media player europe commission brad smith audiovisual software**

NewsScan

MICROSOFT TO EUROPE: 'WE CAN WORK THINGS OUT'
After concluding Microsoft's defense in the antitrust case brought against it by the European Commission, Microsoft general counsel Brad Smith told reporters: "I do really want to underscore one thing, which is that we come to Brussels not only to discuss the issues but to work things out." The Commission has threatened to fine Microsoft as much as 10% of its global sales and force the company to remove its Media Player audiovisual software from Windows. But Microsoft seems to be hoping to work out a deal similar to the out-of-court settlement it reached with the U.S. Justice Department in November 2001. (Los Angeles Times 14 Nov 2003)

Category 38.4 *International agreements on security, individual privacy, Net law*

2003-12-09 **international computer crime cooperating fighting cyberspace**

NIPC/DHS

December 07, — Cybercops and robbers growing trickier on World Wide Web.

When the World Summit on the Information Society convenes in Geneva, Switzerland, December 10 to 12, leaders will seek to build on their success in developing better cross-border guidelines to fight online crime. Investigators say organized crime rings and terror groups are using the Internet to expand their reach and exploit the Web's anonymity to stay one step ahead of the law. Internet experts are particularly concerned about the potential for "cyber terrorism" in which the Internet is used to shut down computer networks, potentially disabling vital infrastructure at banks, airports and emergency services. "It is not at all unusual for a regional conflict to have a cyber dimension, where the battles are fought by self-appointed hackers operating under their own rules of engagement," said Dorothy Denning, a cyber terrorism expert at the Naval Postgraduate School in Monterey, CA. "A rash of cyber attacks have accompanied the conflict between Israel and the Palestinians, the conflict over Kashmir, and the Kosovo conflict, among others." Denning said that for now, at least, studies indicated that anything more than irritating cyber attacks were still difficult for most extremists to mount — although the future could hold more technically savvy terrorists.

Category 38.4 *International agreements on security, individual privacy, Net law*

2004-02-02 **Federal Trade Commission FTC server secure e-mail open proxy spam relay routing**

DHS IAIP Daily; http://www.ftc.gov/opa/2004/01/opsecure.htm

February 02, Federal Trade Commission — FTC and international agencies announce "Operation Secure Your Server".

The United States Federal Trade Commission (FTC) and 36 agencies in 26 countries announced "Operation Secure Your Server " on Thursday, January 29, an international effort to reduce the flow of unsolicited commercial e-mail by urging organizations to close "open relays" and "open proxies." As part of the initiative, the participating agencies have identified tens of thousands of owners or operators of potentially open relay or open proxy servers around the world, and the agencies are sending letters urging the owners and operators to protect themselves from becoming unwitting sources of spam. Open relays and open proxies are servers that allow any computer in the world to "bounce" or route e-mail through servers of other organizations, thereby disguising the real origin of the e-mail. Spammers often abuse these servers to flood the Internet with unwanted e-mail. Their abuses not only overload servers, but also could damage an unwitting business' reputation if it appears that the business sent the spam. The FTC and 10 agencies in Albania, Argentina, Australia, Canada, Brazil, Bulgaria, Canada, Chile, Colombia, Denmark, Ecuador, Finland, Hungary, Jamaica, Japan, Lithuania, Norway, Panama, Peru, Romania, Serbia, Singapore, South Korea, Switzerland, Taiwan, and the United Kingdom are sponsoring this initiative.

Category 38.4 *International agreements on security, individual privacy, Net law*

2006-04-19 **Russia call unity Internet crime fight**

DHS IAIP Daily; http://www.informationweek.com/showArticle.jhtml;jsessionid= 23
D0MGLIXG0NEWAQSNDBECKHSCJUMEKJVN?articleID=186100209

RUSSIA CALLS FOR UNITY TO FIGHT INTERNET CRIME.

The world should unite against online criminals because they could cause as much harm as deadly weapons, Russia's interior minister said on Wednesday, April 19. Russian hackers are notorious, and the country is often identified as a center for extortion from Internet bookmakers, banks and other businesses. Several damaging viruses are believed to have originated in Russia. Interior Minister Rashid Nurgaliyev said the frequency of such attacks was increasing, with potentially catastrophic consequences.

38.5 EU case law, legislation & regulation concerning individual privacy (not govt surveillance)

Category 38.5 *EU case law, legislation & regulation concerning individual privacy (not govt s*

1997-01-21 **e-commerce smart card universal ID privacy EU**

PA News

The European Union floated a proposal for a smart card that would double as a bank card and as a universal identity document. Some anti-EU British politicians immediately branded the proposal as a threat to British sovereignty and a threat to civil liberties.

Category 38.5 *EU case law, legislation & regulation concerning individual privacy (not govt s*

1998-03-01 **privacy Europe government US laws legal**

EDUPAGE

EUROPEAN PRIVACY RULES WILL CHALLENGE U.S. PRACTICES
The European Union Data Protection Directive, which takes effect October 1998, will force U.S. companies doing business in Europe to change the way they handle routine data collection procedures. For instance, companies will need to get consent from their European employees before including them in corporate e-mail or phone directories, and in extreme cases, it may become illegal to carry a laptop computer containing a database with personal information on Europeans to the U.S. or other countries that are deemed to lack "adequate" guarantees of privacy protection. The directive mandates that any personal data obtained by a company may be used only for the purposes for which it was collected unless consent is granted by the consumer for broader usage. If the data is misused in any way, governments will be able to seek injunctions, fines, and even criminal sanctions, and the individuals affected may sue for damages. (CIO Enterprise 15 Feb 98

Category 38.5 *EU case law, legislation & regulation concerning individual privacy (not govt s*

1998-07-02 **privacy ISPs Europe P3P OPS standards W3C**

EDUPAGE

EUROPE, U.S. CLASH OVER INTERNET PRIVACY ISSUES
Disagreement between European and U.S. government officials over how online consumers divulge information about themselves and how that information is used has led to a stalemate over technical standards now under consideration by the World Wide Web Consortium. The Privacy Preferences Project (P3P) and the Open Profiling Standard (OPS) both enable computer users to determine how much personal information they are willing to make available to Web sites, but are not stringent enough in their controls to comply with the European Privacy Directive, which restricts the ability of businesses to collect information from individuals without their permission. A European Union technical committee issued a draft opinion June 16 criticizing the technologies, and saying that "a technical platform for privacy protection will not in itself be sufficient to protect privacy on the Web." The EU is pushing for a new set of laws protecting privacy and worries that if either standard is adopted, it will mislead European companies and individuals into thinking that they have adequate privacy protection on the Web. (New York Times 2 Jul 98)

Category 38.5 *EU case law, legislation & regulation concerning individual privacy (not govt s*

1999-04-29 **corporate privacy policy requirements EU directive compliant**

Computer Weekly (UK)

David Bicknell, writing in the UK's _Computer Weekly_, urged IT directors to study the new European Data Privacy Directive and implement privacy-compliance changes to prevent expensive fines and loss of business for their employers. The deadline for compliance in the UK is the end of 2000, so experts are advising Y2K teams to attack privacy as soon as the Y2K issue is solved.

Category 38.5 *EU case law, legislation & regulation concerning individual privacy (not govt s*

2000-04-14 **data privacy legislation government regulation international EC European Common EU European Union**

NewsScan, Wall Street Journal
http://interactive.wsj.com/articles/SB955657595353654 5.htm

The latest European Union data privacy legislation is in the process of being ratified, and will change the way that companies doing business in Europe collect information on their customers. At issue is the EU's opt-in principle, which requires that each customer give permission for personal data to be shared — in contrast, the U.S. relies on an opt-out policy, which means personal information can be gathered and passed on unless specifically prohibited by a customer. " Before, processing was authorized unless forbidden," says a lawyer for Belgium's Sabena Airlines. "Now it will be forbidden unless authorized." The EU law also gives individuals the right to correct inaccurate data, to delete any information to which they object, and to collect damages for suffering caused by illegal data processing. A number of U.S. companies are objecting to the new law, saying that little consideration was given to the cost of compliance or the technological feasibility of implementing EU privacy standards. (Wall Street Journal 14 Apr 2000)

[In May,] The European Union . . . passed a landmark e-commerce directive that it hopes will streamline member country decision-making and pave the way for agreement on further initiatives, including ones on copyright, online financial services, and revision of the Brussels convention on contractual law. The new directive spells out rules governing electronic contracts, the information an online merchant must give a customer, what e-mail ads must disclose about the sender, discounts and other promotions, as well as the limits on the liability of intermediaries for unlawful material on their Web sites. Analysts predict that the European e-commerce market will top US$300 billion by 2003, out of a world total of US$1.25 trillion. "If we hesitate too long, we will never be able to make up the digital divide, notably with the U.S.," says Frits Bolkestein, internal market commissioner. "Member states need to follow up their words with concrete measures to facilitate the growth of e-commerce." (Financial Times 5 May 2000)

Category 38.5 *EU case law, legislation & regulation concerning individual privacy (not govt s*

2001-04-10 **music copyright intellectual property legislation law proposal**

NewsScan

EU PROPOSES NEW DIGITAL COPYRIGHT LAWS
Ministers from the 15 European Union member nations adopted a copyright directive yesterday aimed at updating copyright laws for the digital age. Member nations now have 18 months to ratify and implement the new regulations, which, according to the EC, will provide a "secure environment for cross-border trade in copyright protected goods and services, and will facilitate the development of electronic commerce in the field of new and multimedia products and services." Under the proposed law, online swapping of copyrighted music files for free would be outlawed, but consumers would be allowed to make a limited number of copies for private use. The EU directive is comparable to the 1998 U.S. Digital Millennium Copyright Act, but differs in that it does not provide for "fair use" of copyrighted material for the purposes of scholarship and research. In contrast, the EU doctrine includes a laundry list of optional exceptions that allow copying for technical reasons, personal use and archival purposes. Member states may make their own decisions as to which exceptions to adopt. (E-Commerce Times 10 Apr 2001)
http://www.ecommercetimes.com/perl/story/8826.html

Category 38.5 *EU case law, legislation & regulation concerning individual privacy (not govt s*

2001-11-30 **Internet service providers ISPs logging user traffic data monitoring privacy law enforcement police investigation evidence**

NewsScan

EUROPEANS DEBATE PRIVACY RIGHTS ON THE INTERNET [30 Nov 2001]
Two different institutions, the European Parliament and the Council of Ministries, are in disagreement over a proposed Europe-wide law requiring Internet service providers to extend the length of the time customer "traffic data" be kept available for use in investigations by law enforcement officials. The Council's pro-law-enforcement position has hardened since the terrorist attacks of September 11, but the European Parliament is resisting changes that would make it easier for authorities to gain access to personal data. Erkki Liikanen, the Finnish commissioner who has the job of revising Europe's data-protection laws for the digital age, says: "We must look at the world differently after September 11. We must be careful to ensure that law enforcement officials do have the powers they need, but I believe it is possible to reach a balance between this and citizens' rights to privacy." (New York Times 30 Nov 2001)
http://partners.nytimes.com/2001/11/30/technology/30DATA.html

---

Category 38.5 *EU case law, legislation & regulation concerning individual privacy (not govt s*

2002-05-28 **privacy international concerns .NET e-commerce access**

NewsScan

EUROPEAN COMMISSION HAS PRIVACY CONCERNS ABOUT MICROSOFT
The European Commission says Microsoft's .NET Passport system may be in violation of the Commission's data protection law. Passport stores a user's ID information on company servers so it doesn't have to be reentered as the user moves from site to site on the Web. The EU is fearful both that personal data might be passed to unknown parties and also that failure to register with Passport could exclude people from visiting some sites. (New York Times 28 May 2002)
http://partners.nytimes.com/2002/05/28/technology/28SOFT.html

---

Category 38.5 *EU case law, legislation & regulation concerning individual privacy (not govt s*

2002-05-28 **consumer data privacy Europe directive e-payment penalties fines**

FindLaw Download This 87

In May 2002, the European Union warned that Microsoft faced possible fines for violating the EC Data Protection Directive. Microsoft's .NET Passport service may have failed to protect consumer privacy at the standards required in Europe.

Category 38.5 *EU case law, legislation & regulation concerning individual privacy (not govt s*

2002-06-04 **homeland security international Europe privacy data protection terrorism surveillance privacy**

FindLaw Download This 88

EU PANEL OKS PRIVACY RULES
The European Union Parliament passed weakened data protection and privacy rules Thursday, bowing to pressure from EU governments eager to boost controls in its fight against terrorism. The new legislation, which still faces final approval by the 15 EU governments, will give anti-terrorist investigators greater powers to eavesdrop on private data on the Internet and other electronic records like people's phone calls.
http://news.findlaw.com/ap_stories/high_tech/1700/5-30-2002/20020530060005_11.html

Cyberspace Privacy Resources
http://www.findlaw.com/01topics/10cyberspace/privacy/

Category 38.5 *EU case law, legislation & regulation concerning individual privacy (not govt s*

2002-06-06 **privacy international Europe e-mail cookies surveillance permission opt-in**

Security Wire Digest 4 44

*E.U. PARLIAMENT RESTRICTS COMMERCIAL USE OF PERSONAL DATA
Companies will need permission to send unsolicited commercial e-mail or use cookies in Internet browser software under a series of amendments to the European Union's data privacy law. E.U. Parliament members last week ignored a committee's recommendations against the restrictions, choosing instead to require companies to get permission from users before they can send unsolicited e-mail, or spam. The Citizens' Rights Committee wanted member states to dictate opt-in policies for including users on third-party mailing lists. The amendment is expected to become law by the end of the year.. Member states still can adopt their own laws on how to use personal information, rather than be forced to delete customer data within a specific time frame.

Category 38.5 *EU case law, legislation & regulation concerning individual privacy (not govt s*

2002-06-06 **expectation privacy covert surveillance law moral obligations rights duties secrecy**

RISKS 22 11

In France, a worried father installed a hidden camera in his own home to check on the behavior of his babysitter's boyfriend. The camera found no abuse, but it did record the baby sitter and her boyfriend having sex while the three-year-old slept in the next room. The father was arrested and fined for violating the couple's privacy. In a thoughtful analysis published in the Los Angeles Times, author Gary T. Marx commented that although such an outcome was unlikely in the USA because of less stringent privacy laws, "The fact that there is still a legal right to secretly record images in the U.S. does not mean that it is the right thing to do. We would do well to learn from the French the general principle of respect for private life, a principle that holds no matter what new technologies are offered to us that allow us to spy on others."

Category 38.5 *EU case law, legislation & regulation concerning individual privacy (not govt s*

2002-08-20 **surveillance spying privacy Europe regulations legislation e-mail phone**

NewsScan

GROUP WARNS OF EU SURVEILLANCE
Statewatch, a U.K. group dedicated to protecting civil liberties on the Internet, is warning that European governments are planning changes to the 1997 EU Directive on privacy in telecommunications that would require phone companies, mobile network operators and ISPs to store details of their customers' Web use, e-mails and phone calls for between one to two years. Current law states that traffic data may be retained for billing purposes only and then must be deleted. "EU governments claimed that changes to 1997 EC Directive on privacy in telecommunications to allow for data retention and access by the law enforcement agencies would not be binding on member states -- each national parliament would have to decide. Now we know that all along they were intending to make it binding, compulsory across Europe," says Tony Bunyan, editor of Statewatch. The changes may include the provision that police would need a judicial order before accessing traffic data, but Statewatch warns that such conditions have been sidestepped before. (CNet News.com 20 Aug 2002)
http://news.com.com/2100-1023-954487.html

Category 38.5 *EU case law, legislation & regulation concerning individual privacy (not govt s*

2002-08-30 **consumer individual privacy Europe USA Web data subject directive online e-commerce**

NewsScan

TOUGH EU PRIVACY RULES INFLUENCE U.S. WEB PRACTICES
Europe's strict approach to consumer data protection is forcing many U.S.-based companies to follow suit in order to continue serving their European customers. "Europeans are extremely concerned about the use of data about people," says Rockwell Schnabel, the U.S. ambassador to the European Union. "The data privacy issue is a huge issue over there. American partners have to live with those rules, and they can't do with it what they can with American data." A case in point is Microsoft's Passport online ID service that enables users to log in once and then move from one secure Web site to another. Consumer and privacy groups had accused Microsoft of not taking adequate steps to protect consumers' personal information and in a settlement earlier this month, Microsoft admitted no wrongdoing, but agreed to government oversight of its consumer privacy policies for the next 20 years. A separate Passport investigation by the EU is still pending. "The EU directive raised the bar on the practices by U.S. companies for U.S. consumers," says Marc Rotenberg, head of the Electronic Privacy Information Center. "Passport is a good example of that, because Microsoft is very much aware that its products are going to have to meet EU privacy standards." EU standards specify that data may be collected only for "specified, explicit and legitimate purposes, and to be held only if it is relevant, accurate and up to date." Citizens may access any data about themselves, find out its source, correct inaccuracies, and pursue legal recourse for misuse. (San Jose Mercury News 29 Aug 2002)

Category 38.5 *EU case law, legislation & regulation concerning individual privacy (not govt s*

2004-01-18 **UK data protection act unintended consequences privacy disclosure**

RISKS; http://news.bbc.co.uk/1/hi/uk/3395071.stm 23 14

UK DATA PROTECTION LAWS AND THE LAW OF UNINTENDED CONSEQUENCES

Contributor Richard Pennington notes two cases of loss of life resulting from misunderstanding and misapplication of the UK Data Protection Act. In the first case, a school in Cambridgeshire hired an applicant from Humberside for a janitor's job. Background checks with Humberside police had shown the applicant to be 'clean'. Later, this new janitor murdered two schoolchildren. An inquiry showed that the janitor had been investigated in Humberside for indecent assualt. Humberside police stated that they were forced by the UK Data Protection Act to destroy the suspect's records when "investations ended without a trial." So, the suspect's history was not circulated in Humerside, and never reached Cambridgeshire. In the second case, in August 2003, British Gas stopped supplying an elderly couple gas due to bill nonpayment. This couple was discovered to have perished from hypothermia during the winter. British Gas cited the UK Data Protection Act for not contacting local Social Services because "they did not have the written permission of the couple to disclose their financial records." In a follow-up article, the same contributor noted that, at that time, the Data Protection Registrar had been renamed the Information Commissioner. In another follow-up article, contributor Dave Harris, referring to the first case above, said that the killer Ian Huntley had not actually worked at the school where the two children were murdered. Huntley had come "into contact with them through his girlfriend (who did work at their school)."

Category 38.5 *EU case law, legislation & regulation concerning individual privacy (not govt s*

2004-07-01 **did-they-read-it e-mail Web bug online service privacy France litigation illegal**

NewsScan

FRENCH AUTHORITY FORBIDS "DIDTHEYREADIT?" SERVICE

CNIL, the French data protection authority, has declared Rampell Software's new mail-service 'Did they read it?' to be illegal. (Subscribers to "DidTheyReadIt?" get a report about the exact time their e-mail was opened, for how long, on what kind of operating system and if the mail was forwarded to other people.) The CNIL finds the service unacceptable under French privacy Legislation; as a result, any French subscriber to this service risks a prison sentence of 5 years plus a substantial fine. (EDRIgram 1 Jul 2004) Rec'd from Jim Sterne via Mark Gibbs

---

Category 38.5 *EU case law, legislation & regulation concerning individual privacy (not govt s*

2004-08-19 **data debate privacy Lloyds Britain jurisdiction outsourcing India**

NewsScan

DATA DEBATE STIRS IN BRITAIN

A customer of Lloyds TSB bank has complained to Britain's Information Commissioner arguing that data should not be transferred outside Europe without the consent of individual customers. The complaint by an unidentified Lloyds customer, filed in July, argues that Indian workers would not be subject to the same data protection standards applicable in Europe, according to the Lloyds TSB union, which has been campaigning against outsourcing of work to India and other countries. The Information Commissioner's office said British companies are still bound by European standards when data is transferred overseas: "There are various bases in law which can be used to legitimize the transfer overseas of personal data, consent from the individual is just one of them." (The Australian 19 Aug 2004) Rec'd from J. Lamp

---

Category 38.5 *EU case law, legislation & regulation concerning individual privacy (not govt s*

2005-09-15 **Holland Netherlands Dutch Ministry of Health citizen tracking permanent government agencies**

EDUPAGE; http://www.wired.com/news/privacy/0,1848,68866,00.html

DUTCH TO TRACK ALL CITIZENS, FOREVER

Beginning in 2007, the Dutch Ministry of Health will begin tracking all citizens of the country in a single database from their births to their deaths. Each person will be added to the database at birth, with health and family information included. As people in the database age, information from schools, doctors, and the police will be added. In an effort to protect privacy, no individual will be permitted to see any person's complete file. Various governmental agencies, however, will be able to add "red flags" to a file if they notice something that might be cause for concern, according to Jan Brouwer, spokesperson for the Health Ministry. Brouwer suggested that someone at child protection services might find that for an individual, red flags had been added by the police, the school, and a doctor, which would likely indicate a problem that should be addressed. Truancy is often correlated with criminality, for example, and the new database will allow tracking such patterns. Wired News, 15 September 2005

Category 38.5 *EU case law, legislation & regulation concerning individual privacy (not govt s*

2005-09-26 **Europe EU data retention plans criticism terrorism anti-terrorism Convention on Human rights civil liberties Internet phone logging**

EDUPAGE; http://www.siliconvalley.com/mld/siliconvalley/12746814.htm

EU DATA-RETENTION PLANS DRAW CRITICISM

Peter Hustinx, data protection supervisor for the European Union (EU), has voiced his criticism of two antiterrorism proposals for their stance on data retention. Neither the proposal by the European Commission nor one drafted by EU governments makes a compelling case for holding on to sensitive data as part of antiterrorism efforts, said Hustinx. The EU proposal, he noted, would allow for the retention of information such as times of phone calls for up to three years. Hustinx said that any measures put forth should comply with the European Convention on Human Rights. Those that do not are "not just unacceptable but illegal." The chair of the EU negotiations, British Home Secretary Charles Clarke, is urging European governments to forgo some measure of civil liberties in return for broader authority for law enforcement to investigate suspected terrorists. San Jose Mercury News, 26 September 2005

Category 38.5 *EU case law, legislation & regulation concerning individual privacy (not govt s*

2006-02-09 **Europe Web security improvement urge EU media commissioner online threats**

DHS IAIP Daily; 23
http://news.yahoo.com/s/ap/20060209/ap_on_hi_te/eu_internet_security;_ylt=AqJsTFxWQORMKXpiJ5yFMsAjtBAF;_ylu=X3oDMTA5aHJvMDdwBHNlYwN5bmNhdA−−

EUROPE URGED TO IMPROVE WEB SECURITY.

Europe must work harder to make the Internet more secure as the nature of online threats becomes increasingly criminal across the 25-nation bloc, a senior EU official warned Thursday, February 9. "We are still far from achieving the goal of secure and reliable networks that protect confidential and reliable information," said Viviane Reding, the EU's media commissioner, at a conference on trust in the Internet. Almost 80 percent of EU citizens are concerned about Internet security and half do not engage in electronic commerce because they worry about having their personal financial data stolen on the Web, she said. Speaking via video link from Brussels, Reding stressed the importance of international cooperation in promoting user trust in the Web and said she would soon announce a "strategy for enhanced security."

38.6 US case law, legislation & regulation concerning individual privacy (not govt surveillance)

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

1997-01-07 **privacy**

AP

The FTC declared in January that consumers ought to be given control over whether personal information can be gathered and used on the Internet.

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

1997-04-17 **privacy law**

EDUPAGE

PRIVACY LEGISLATION
Senators Dianne Feinstein (D, California) and Charles Grassley (R, Iowa) . . . Introduced legislation that would bar commercial use of Social Security numbers and make it illegal for credit bureaus to disseminate Social Security numbers, unlisted phone numbers, birthdates, or individuals' mothers' maiden names. In the House of Representatives, Congressman Paul E. Kanjorski (D, Pennsylvania.) submitted legislation that would create a Commission on Privacy of Government Records and ban Social Security or Internal Revenue Service records from being posted on the Internet without an individual's written permission. (Washington Post 17 Apr 97)

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

1997-05-07 **privacy medical online**

Wired

In California, Rep. Liz Figueroa (D -San Francisco Bay Area) moved ahead with her proposal to put physicians' professional records online. She agreed to remove the controversial inclusion of malpractice settlements (often agreed to simply to prevent costly legal fees). Other sensitive matters, however, continue to be included in the public information: doctors' education, malpractice, and disciplinary history in hospitals, especially if based in alcohol or other drug abuse.

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

1997-07-29 **privacy eavesdropping cellular Web**

AP

The Chair of the House Commerce Committee's Telecommunications Subcommittee, Rep. Billy Tauzin (R-LA), introduced legislation to stop companies from disclosing or using without consent people's medical and financial records, as well as government information such as social security numbers that are available online. In a separate measure, he proposed to increase penalties against eavesdropping on cellular phone communications and to forbid tampering with radio equipment for the purpose of such interception.

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

1998-05-14 **privacy law politics information warfare**

EDUPAGE

The most technologically-savvy Vice President of the United States in history, Al Gore, called for an Electronic Bill of Rights (echoing long-standing calls by Winn Schwartau and other supporters of privacy rights). The United States, unlike most other developed countries, has no formal office dedicated to protecting the privacy of its citizens, so Gore's announcement of a privacy conference in June to be sponsored by the Department of Commerce was good news for privacy advocates. Now if we could just convince the administration that encryption is important for privacy. . . . In August, VP Gore formally endorsed several privacy bills making their way through the HR and the Senate.

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

1998-05-19 **high technology policing FBI BATF DoE cell-phone fraud**

EDUPAGE

DOE WILL SHARE TECHNOLOGY WITH FBI, BATF
In a speech [in May 1998], Vice President Al Gore ...[announced] that the Energy Department will share some of its valuable technology, which up to now has been used only for Cold War espionage, with the Federal Bureau of Investigation and the Bureau of Alcohol, Tobacco and Firearms. The technology includes: portable chemical analysis machines to gather forensic crime-scene data; software used to track cell-phone fraud, online copyright violations and Internet fraud; hand-held GPS devices to record video and audio notes; and nuclear-detection technology and drug-analysis labs. "This new partnership will help law enforcement across the country deploy the cutting-edge technologies of our national labs to fight drugs, violent crime and terrorism," says Gore. (Wall Street Journal 19 May 98)

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

1998-06-04 **child pornography Internet Web filtering abuse privacy**

EDUPAGE

The Federal Trade Commission of the US severely criticized ISPs for failing to protect children from cyber-abuse. In a study of Web-site privacy policies, the FTC found that although 92% of 1400 studied sites collected personal information, only 14% of the 1400 had posted any information at all about their intended applications for these data. Only 2% had any privacy policy available. Predictably, ISPs fired off salvos of lobbying to persuade the government to "allow self-regulation to work." Um, did they mean, "allow self-regulation to begin?" In a related development, FTC Commissioner Mozelle Thompson criticized Web sites for allowing children to reveal person information without parental involvement. In June, the Administration stated that they would delay proposals for government regulation on privacy for at least several more months. Privacy advocates groaned. In July, the FTC announced that it was working on formal privacy guidelines and asked the House Commerce Committee to provide the FTC with additional enforcement powers.

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

1998-11-11 **P3P Platform Privacy Preferences labeling Web site patent**

Wired http://www.wired.com/news/print_version/technology/story/16180.html

P3P, the Platform for Privacy Preferences, was developed by the World Wide Web Consortium (W3C), a standards group that included Drummond Reed, CEO of the Intermind company. The P3P allows a Web user to specify a privacy profile that can be read automatically by Web sites and thereby adjust the site's handling of the visitor's privacy. In July, word leaked that Intermind had filed for and was expected to receive a patent from the U.S. government on the very idea behind P3P. Reaction was shock and horror; Reed admitted that the group members mostly want "to just crucify us." According to an article in Wired by Chris Oakes, Intermind's Web site specified "a minimum royalty of US$50,000 per year to a maximum of $2.5 million from companies implementing P3P, plus 1 percent of all revenues directly associated with the technology."

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

1998-12-07 **privacy international Europe standards US conflict different**

TechWeb http://www.techweb.com/se/directlink.cgi?INW19981207S0035

The U.S. refusal to draft privacy standards consistent with the European Data Protection Directive drafted in 1996 will lead to increasing difficulties for firms trying to do business with European clients. Nick Evans, technical director of PricewaterhouseCoopers' national Internet practice, warned in an article published on the TechWeb site that online businesses could suffer as a refusal of the legislators to progress on this issue.

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

1998-12-09 **privacy ISP Internet service providers initiative proposal**

Network Week (UK)

According to an article by Alex Straunik in Network Week in December, the UK Cyber Rights & Cyber Liberties association "called on Internet users to demand clear answers from their service providers as to what privacy policies they had in place and what co-operation they had agreed to with the Association of Chief Police Officers in Britain." The Secretary General of the Internet Service Providers Association (ISPA), Nicholas Lansman, reportedly told the ISPA members to ignore the letter, but others in ISPA said they would respond. The problem identified by the privacy advocates was rooted in British laws allowing police to obtain detailed information about telephone and ISP subscribers without a court-issued warrant. However, wire-tapping or surveillance of e-mail still required a warrant.

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

1998-12-19 **privacy watchdog group survey Web sites consumers**

New York Times
http://www.nytimes.com/techweb/TW_Privacy_Group_Unveils_Watchdog.html

In December, the Center for Democracy and Technology <http://www.cdt.org> announced their new project for a Web site where consumers would be able to evaluate the privacy policy of any online business.

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

1998-12-29 **privacy federal government study evaluation survey Web sites**

New York Times
http://www.nytimes.com/library/tech/98/12/cyber/articles/29privacy.html

The Federal Trade Commission of the U.S. announced in December that it would work with the Direct Marketing Association to survey the state of privacy on the World Wide Web. Online privacy groups such as the Better Business Bureau, Direct Marketing Association, TRUSTe and the Online Privacy Alliance were scurrying to meet the January 1999 deadline for proposed legislation if they failed to establish viable private-sector controls on the use and abuse of personal information provided by consumers using the Web.

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

1999-03-03 **privacy wireless communications eavesdropping law**

EDUPAGE; tele.com

CONGRESS EXTENDS PRIVACY PROTECTION TO DIGITAL WIRELESS
The U.S. House of Representatives last week passed The Wireless Privacy Enhancement Act of 1999, which extends the privacy protection afforded to analog wireless devices to digital ones. The bill, which passed on a vote of 403 to 3, closes some loopholes in an earlier Privacy Act, which excluded digital technology. It also cracks down on eavesdropping on a cellular phone call, stipulating punitive measures such as fines, warnings, and possible imprisonment for such actions. In addition, the bill requires the Federal Communications Commission to ban scanners that can intercept cellular and digital calls and asks the FCC to evaluate the idea of requiring warning labels to be placed on such scanning receivers. (tele.com 3 Mar 99)

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

1999-04-08 **privacy legislation bill proposal US law regulation**

PC WORLD DAILY

In April, Congressional Rep. Ed Markey (D—MA) announced his bill to establish a national privacy policy, bringing the US up at last with nations around the world who established such policies — and Privacy Commissioners or Privacy Ombudsmen — years ago. Writing in _PC WORLD DAILY_, Niala Boodhoo summarized the issues as follows: "The proposed policy boils down to three basic principles: the individual's right to know what personal information is being gathered; the right to know whether gathered information may be used for other purposes; and the right to refuse to provide information."

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

1999-04-16 **privacy policy Web federal government agencies browsers**

Wired

The Center for Democracy and Technology published a study in April 1999 showing that only about a third of US Federal Government agencies actually publish detailed privacy policies showing visitors exactly what kind of data their Web sites collect.

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

1999-04-20 **Internet privacy law legislation bill children FTC Web**

ZDNN

The Federal Trade Commission announced a notice of proposed rulemaking implementing the Children's Online Privacy Protection Act of 1998. The law takes effect in 2001. The proposed implementation would require all Web sites soliciting or collecting information from children under 13 years of age to obtain explicit permission from the children's parents or guardians. How exactly such a scheme could possibly be implemented without strong identification and authentication and verifiable digital signatures remained a complete mystery.

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

1999-04-29 **EU data privacy directive US compliance government law**

COMPUTING (UK)

At the end of April, the US Department of Commerce announced principles for US companies to comply with the European Union Data Privacy Directive. An article in the British magazine _Computing_ said, "Under the principles, organisations are required to tell individuals about the information held on them; allow individuals to choose how that information is used, including onward transfer; and maintain secure systems to ensure data integrity, allowing access to their systems for enforcement of these principles. Organisations will be permitted to use private sector programs to ensure compliancy with the agreement. However, these must include effective enforcement and dispute resolution with either supervisory authorities, or via co-operation with data privacy organisations in the EU."

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

1999-05-04 **privacy proposal bill Administration fraud banking transactions sharing**

Washington Post http://www.washingtonpost.com/wp-srv/business/daily/may99/privacy4.htm

PRIVACY PROPOSAL
A Clinton Administration proposal to protect individual financial and medical records includes a request for more than $5 million to fund an increase in online surveillance and to train law enforcement officials in ways to combat security fraud. Congressman Jay Inslee (D-Wash.) explained the problem to his colleagues by writing: "Do you believe your banking transaction experiences are private? You may be surprised to learn that with certain exceptions, financial institutions may legally share all of the information about you and your bank account activity with affiliated businesses or even third parties." (Washington Post 4 May 99)
http://www.washingtonpost.com/wp-srv/business/daily/may99/privacy4.htm

WHITE HOUSE TARGETS ONLINE TRADING FRAUD
The Clinton administration has pledged to crack down on fraudulent Internet stock trading, with Securities and Exchange Commission Chairman Arthur Levitt announcing plans to double the number of SEC Cyberforce attorneys to 250 in the coming year. He also plans to ask for a "significant" increase in funding for the agency's fraud unit in next year's budget. More than 7 million Americans now trade stocks online, and their trades make up 25% of all trades made by individual investors. (Financial Times 5 May 99)
http://www.ft.com/hippocampus/qc5f86.htm

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

1999-10-07 **online privacy seals certification complaints investigation Web**

ZDNet

FTC WILL BACK ONLINE PRIVACY GROUPS
The FTC announced at Internet World that it will take the consumer complaints it receives from online privacy seal groups and send them directly to investigators, bypassing the normal channels of complaint. The new policy will give stronger support to third-party privacy seals and will help ensure compliance with privacy policies, according to David Medine, associate director for financial practices at the FTC's bureau of consumer protection. Still, Medine questioned whether companies are "doing the right thing" in terms of protecting user privacy. Former FTC Commissioner Christine Varney was among the participants in an online privacy panel. The panelists called on businesses to spell out their privacy policies, give users greater control over their data, and provide Web site visitors with a plan of recourse to resolve privacy violations. Varney says Congress is unlikely to pass wide-ranging privacy laws any time soon. "Without a specific catastrophe, I'd say it's unlikely you'll see specific broad-based privacy legislation." (ZDNet 10/07/99)

FTC ACCUSED OF WITHHOLDING PRIVACY DATA
The Electronic Privacy Information Center, a nonprofit that favors stiff privacy laws, has filed a lawsuit against the Federal Trade Commission in an effort to win the release of hundreds of consumer complaints about possible privacy violations. The center's director, Marc Rotenberg, says the group will analyze the records to test how thorough the FTC has been in enforcing consumer privacy complaints. Rotenberg says he expects to find that the FTC has been negligent in effectively dealing with thousands of privacy complaints. The Electronic Privacy Information Center asked for the records June 10, but the FTC failed to respond in a timely manner, according to Rotenberg. The FTC disputes Rotenberg's assessment of the situation. "All of the complaints we get are either responded to by staff members or forwarded to the appropriate people," says the FTC's Victoria Streitfeld. The FTC must first ensure that it strips away data that could be used to identify users before releasing the complaints, Streitfeld says. (Los Angeles Times 10/13/99)

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

1999-10-21 **children privacy parental approval authorization data collection Web**

New York Times

NEW PRIVACY RULES FOR CHILDREN'S WEB SITES
Privacy advocates are giving high marks to the FTC for passing new rules governing Web sites' collection of personal information from children. The FTC voted 4-0 to implement the rules, which complement the Children's Online Privacy Protection Act and will become effective in April. All Web sites must receive "verifiable parental consent" before collecting personal data from children, according to terms of the law. The FTC rules define parental consent on a "sliding scale" that permits Web sites to use postal mail, fax, credit card, or digital signatures to get consent when children will be using chat rooms or parting with personal data that will be made available to affiliates. The rules also state that an e-mail from parents, and a follow up confirmation by the online company, is sufficient enough consent to collect data from children — so long as that data is only used internally. (New York Times 10/21/99)

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

1999-11-03 **privacy financial services banking customer confidentiality legislation law bill**

EPIC Alert 6 18

At the beginning of November, the Financial Services Modernization Bill of 1999 (S. 900) obliged financial institutions to disclose their privacy policies to consumers and restricted release of account numbers and access codes to third parties. However, the bill did not require explicit consent before allowing disclosure of a customer's financial information to third parties such as marketing agencies. The legislation did not override better privacy protection at the state level.

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2000-01-13 **privacy government states driving license personal data sale**

Edupage, Washington Post, EPIC Alert 7 01

The Supreme Court of the United States upheld the 1994 Drivers' Privacy Protection Act and refused to allow states to sell drivers' personal information without permission. Several states had opposed the Act because their bureaucrats and politicians saw the sale of drivers' information as a lucrative source of revenue for their governments. Edupage editors wrote, "Privacy and civil liberties advocates reacted with joy yesterday after the Supreme Court decided to uphold the 1994 Driver's Privacy Protection Act, which bars states from selling drivers' personal data without their knowledge. The ruling came as some surprise, as recent court decisions have favored states' authority over such laws. The ruling could establish a precedent that encourages federal lawmakers to pass laws restraining the widespread dissemination of personal data over the Internet, privacy advocates and members of the direct-marketing industry said. In making its decision, the Supreme Court reversed the ruling of the U.S. Court of Appeals for the 4th Circuit, which found the law unconstitutional because it forced states to enforce a federal regulation. The Supreme Court ruled differently, stating that the law `does not require state officials to assist in the enforcement of federal statutes regulating private individuals.' "

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2000-02-24 **privacy law regulation proposal Safe Harbor EC European Commission Data Protection Directive international agreements**

NewsScan

The Federal Trade Commission . . . [proposed] legislation that will require department stores, automakers, car-rental firms, and other companies to protect the financial privacy of consumers who do business with them. Financial firms will have to create a privacy policy and clear state it to consumers, and give consumers the right to forbid the sharing of their personal financial information with unaffiliated third parties.

* * *

The move by the FTC to impose privacy protection rules on U.S. businesses [was] heralded as a breakthrough by U.S. and European negotiators who have been seeking a way for U.S. firms to do business in Europe without eroding Europeans' privacy rights. In the compromise, the FTC will maintain a list of companies that agree to comply with at least one of four ways of implementing privacy protections: 1) By subjecting themselves to the data-protection authority in one of the 15 EU countries; 2) By showing that they comply with similar U.S. privacy laws; 3) By signing up with a self-regulatory organization such as BBBOnline, which is subject to FTC oversight; or 4) By agreeing to refer privacy disputes to a European regulatory panel. European officials say that resolving the disparities between U.S. and European privacy protections will be key to the success of e-commerce on the continent. (Wall Street Journal 24 Feb 2000)

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2000-05-22 **identity anonymity privacy intellectual property copyright infringement policy proposal report think-tank law legislation government**

NewsScan, Los Angeles Times
http://www.latimes.com/business/20000522/t000048299.html

The Progressive Policy Institute is expected to meet with Congress on Wednesday to deliver its proposed remedy for the current legal wranglings over copyright infringements via the Internet. The changes include: requiring Internet companies to collect personally identifiable and verifiable information from their users, rather than allowing them to sign on anonymously; setting a specific time frame for removing copyright-infringing materials off the Net; and allowing judges to grant injunctions against companies such as Napster whose services are substantially used for exchanging pirated material. (Los Angeles Times 22 May 2000)

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2000-06-12 **privacy lawsuit regulation state law prosecution**

NewsScan. USA Today http://www.usatoday.com/life/cyber/tech/cti085.htm

Michigan Attorney General Jennifer Granholm is threatening lawsuits against four Web sites for failing to tell consumers whether their privacy rights are being protected under state law, even though the sites sold personal products designed for expectant mothers and small children, AIDS patients, sexual voyeurs and stock market investors. "We picked four areas we thought would be of interest and might contain sensitive information. They are examples of how completely inadequate so many privacy policies are." The sites targeted were Johnson & Johnson's www.procrit.com, children's retailer AmericasBaby.com, the voyeuristic Intimate Friends Network and the Stockpoint financial site. (USA Today 12 Jun 2000)

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2000-06-20 **privacy law legislation state regulation federal survey**

NewsScan, USA Today http://www.usatoday.com/life/cyber/tech/cti125.htm

Internet privacy will be the central topic of the summer meeting of the National Association of Attorneys General, beginning today in Seattle. Citing a recent survey showing that only 20% of the busiest Internet sites offer consumers adequate privacy protections, New York Attorney General Elliott Spitzer sees an opportunity for action at the state level: "There is a void that has been created by the failure of Washington to act. In the absence of any forward movement, it may be time to pursue litigation." (USA Today 20 Jun 2000)

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2000-10-03 **privacy opt-in ISP government committee legislation**

NewsScan, San Jose Mercury News
http://www.sjmercury.com/svtech/news/breaking/reuters/docs/472958l.htm

America Online says consumers certainly should be able to choose to withhold their personal data from being shared among online companies, but urged lawmakers not to change the equation to require that consumers "opt in" — make an informed decision — before data collected about them online could be used for purposes other than the transaction at hand. "In the diverse online marketplace, we believe it is impossible to mandate a 'one-size-fits-all' solution to consumer choice," said AOL senior VP George Vradenburg in testimony to the Senate Commerce Committee. Meanwhile, privacy advocates maintain that an "opt-in" system is more in keeping with U.S. notions of civil liberties. "This is the same sort of 'informed consent' system that has become the standard in medicine, banking and other areas," testified Simson Garfinkel, author of "Database Nation: The Death of Privacy in the 21st Century." (Reuters/San Jose Mercury News 3 Oct 2000)

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2000-11-29 **privacy corporate policy position officer progress**

NewsScan, San Jose Mercury News
http://www.mercurycenter.com/svtech/news/breaking/merc/docs/076752.htm

IBM has named Harriet Pearson its first Chief Privacy Officer, responsible for coordinating privacy programs throughout the company. IBM chief executive Lou Gerstner explained: "We know that one of the great conundrums of e-business is that it gives enterprises a powerful new capability to capture and analyze massive amounts of customer information so they can serve individual customers more effectively. Yet this very capability troubles some people, who see it as a means to disclose or exploit their personal information. These are legitimate and very real concerns, and they must be addressed if the world of e-business is to reach its full potential." (Reuters/San Jose Mercury News 29 Nov 2000)

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2001-01-15 **HIPAA privacy illness health records solicitation marketing**

NewsScan

LOOPHOLES IN NEW HEALTH RECORD PRIVACY REGULATIONS
The Clinton administration's new federal privacy regulations explicitly allow doctors, hospitals, health services, and their business associates to use patient records for marketing and fundraising. People with a certain disease could receive unsolicited telephone calls touting relevant health products or asking for donations for research to find a cure for that disease. Consumer and privacy advocates are charging that these provisions of the privacy law violate its basic intent, and medical ethicist Thomas Murray says: "Your medical record was meant for your medical care. Now your medical record becomes a marketing tool." But Health and Human Services official Gary Claxton defended the law: "It's the best we could do and we think we did a good job. There's going to be a lot of discussion as this is implemented. If changes need to be made, they should be made." (Washington Post 16 Jan 2001)
http://washingtonpost.com/wp-dyn/articles/A63303-2001Jan15.html

---

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2001-01-24 **privacy Web data collection regulation investigation advertising**

NewsScan

FTC CLEARS DOUBLECLICK
The Federal Trade Commission has ended its investigation into the data collection practices of Internet advertising firm DoubleClick, concluding that "DoubleClick never used or disclosed" consumers' personal information "for purposes other than those disclosed in its privacy policy." The inquiry was initiated in response to complaints that DoubleClick's $1.7-billion purchase of direct marketer Abacus would enable it to cross-reference its records of consumers' online habits with Abacus's database including names and other identifying information. DoubleClick eventually scrapped those plans and has now promised the FTC that it will provide consumers an "opt out" option and will clarify its privacy policy. (AP/USAToday 24 Jan 2001)
http://www.usatoday.com/life/cyber/tech/2001-01-23-doubleclick.htm#more

---

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2001-01-24 **Web privacy personal information opt out legislation**

NewsScan

CONGRESS TACKLES INTERNET PRIVACY LEGISLATION
Two U.S. Representatives -- Chris Cannon (R-Utah) and Anna Eshoo (D-Calif.) -- have introduced legislation that would require Web sites to notify visitors how personal data such as telephone numbers and ZIP codes are used, and allow visitors to "opt out" of that use. "Consumers shouldn't have to reveal their life story every time they surf the Web," said Eshoo. The bill mirrors legislation introduced in the Senate last year by Sen. John McCain (R-Ariz.) and Sen. John Kerry (D-Mass.), and lawmakers agree that Congress will probably pass some type of Internet privacy bill this year. (Reuters/San Jose Mercury News 24 Jan 2001)
http://www0.mercurycenter.com/svtech/news/breaking/internet/docs/792207l.htm

---

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2001-02-12 **privacy policy government organization coalition**

NewsScan

GROUP ASKS FEDERAL OFFICIALS TO MAKE PRIVACY PLEDGE"
The Privacy Coalition, a group of national organizations that include the liberal ACLU, conservative Eagle Forum, the Electronic Privacy Information Center, the American Library Association, the United Auto Workers union, and nine other member organizations, is asking federal officials to make a "privacy pledge" to set "strong, basic privacy standards" to ensure that companies will inform consumers how their personal data is used, protect that data from hackers, and give them power over that data. (AP/USA Today 12 Feb 2001)
http://www.usatoday.com/life/cyber/tech/2001-02-12-privacy-challenge.htm

---

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2001-03-14 **privacy government regulation activists**

NewsScan

FTC HEARS FROM PRIVACY GROUPS
In a Federal Trade Commission workshop held yesterday focused on how companies exchange information about their customers, privacy groups told the agency that companies should do a better job explaining how they share such information with other firms and should let consumers decide whether or not they want their names and addresses shared like that. However, House Majority Leader Dick Armey says he's just as worried about how the government itself treats information about its citizens: "If the government is going to monitor the information sharing practices of the private sector, I'd like to know who's going to monitor the government." A number of companies gather information about the purchasing preferences of their customers. (USA Today 14 Mar 2001)
http://www.usatoday.com/life/cyber/tech/2001-03-13-privacy.htm

---

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2001-04-23 **privacy laws legislators legislation proposals lawmakers amateurs**

NewsScan

PLEA FOR CAUTION WHEN WRITING NEW PRIVACY LAWS [9 Apr 2001]
House Majority Leader Dick Armey (R-Texas) has written a letter to his fellow lawmakers urging them not to let the current prominence of privacy issues stampede them into writing careless laws. "I don't want strangers poking around in my business any more than they want me poking around in theirs," the letter said, but emphasized the need for proceeding cautiously before writing laws for a new and unpredictable technology-based economy: "Congress is an inexperienced and amateur mechanic trying to tinker with the supercharged, high-tech engine of our economy. We need to be careful not to let our good intentions get in the way of common sense." An official of the United States Public Interest Research Group criticized Armey's letter as an attempt to promote an "anti-privacy agenda." (New York Times 9 Apr 2001)
http://www.nytimes.com/2001/04/09/technology/09PRIV.html

WHAT PRICE PRIVACY? [23 Apr 2001]
A new study by the Progressive Policy Institute, a moderate Democrat research group, is warning that any proposed privacy legislation that would significantly restrict Web sites from collecting personal information about their visitors will endanger the viability of sites whose advertising support allows them to disseminate information for free. Progressive Policy Institute president Robert Atkinson says, "If we pass draconian privacy legislation we're going to seriously damage the economics of the Internet." (San Jose Mercury News 23 Apr 2001)
http://www.siliconvalley.com/docs/news/svfront/priv042301.htm

---

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2002-02-19 **sex offender public list privacy anonymity constitutionality judicial review lawsuit**

NewsScan

ONLINE SEX-OFFENDER LISTS TO BE GIVEN CONSTITUTIONAL SCRUTINY [19 Feb 2002]
The U.S. Supreme Court will decide the question of whether the Constitution allows states to pass legislation enabling the use of Internet registries of convicted sex offenders who have served their time in jail and been released back into society. All states have some version of a sex-offender law, which typically allows publication of a convicted offender's name, address, and other personal information. Such laws are deemed to conform to the Constitution if they are narrowly focused on public safety and not used to extend the punishment of someone beyond what was prescribed by the sentence given to him by the courts, because it is unconstitutional to punish someone twice for the same crime. (AP/USA Today 19 Feb 2002)
http://www.usatoday.com/life/cyber/tech/2002/02/19/scotus-sex-offender-registries.htm

---

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2002-04-19 **privacy legislation proposal bill personal information EU directive opt-in**

NewsScan; http://news.com.com/2100-1023-886679.html

INTERNET PRIVACY
Sen. Ernest Hollings (D-S.C.) has introduced an online privacy bill that would require companies to obtain explicit permission from people before collecting and sharing their personal information. The Online Personal Privacy Act reflects some components of the recently ratified European Union privacy directive, requiring that individuals "opt-in" to any collection, use or disclosure of "sensitive information." Sensitive information is defined as relating to any financial, medical, ethnic or religious affiliation, sexual orientation or political data. In addition, the bill would require businesses to provide an "opt-out" option when collecting nonsensitive information, such as that related to online clothing purchases. "Privacy fears are stifling the development and expansion of the Internet as an engine of economic growth," says Hollings. (CNet News.com 18 Apr 2002)

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2002-05-03 **identify theft proposed legislation bill penalties**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A24368-2002May2.html

ASHCROFT WANTS STIFFER PENALTIES FOR IDENTITY THEFT
U.S. Attorney General John D. Ashcroft is proposing legislation increasing by 2 to 5 years the jail time for persons convicted of aggravated identity theft a crime . "The Department of Justice is committed to seeing to it that criminals and terrorists cannot find refuge in the identities of law-abiding citizens of this country." Since October 1998, 2,223 criminal cases have been filed against 2,899 defendants. The call for tougher penalties won immediate support from Democrat Sen. Dianne Feinstein of California, who chairs the Senate Judiciary subcommittee on technology, terrorism and government . (Washington Post 3 May 2002)

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2002-05-17 **data collection Web privacy commercial information proposed law legislation bill**

NewsScan

ONLINE PRIVACY BILL DELAYED
Parliamentary maneuvering has delayed consideration of a Senate bill that would protect individual privacy on the Internet and regulate how businesses may use customer e-mail addresses and other personal data. The proposed legislation would also limit how businesses may use phone numbers, purchase records, and other data collected through their Web sites, and would require online businesses to get customer permission before collecting or sharing sensitive personal information. "What we are proposing simply codifies businesses' best practices on the Internet," Hollings says Senator Ernest Hollings (D-SC), who sponsored the bill. (Reuters/USA Today 16 May 2002)
http://www.usatoday.com/life/cyber/tech/2002/05/16/privacy-bill.htm

---

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2002-05-21 **Internet privacy proposed law legislation bill**

FindLaw Download This 86

VENTURA MULLS INTERNET PRIVACY BILL
Minnesota's Senate and House overwhelmingly approved a bill that backers say would make the state the first to give Internet users control over whether service providers disclose their personal information. Gov. Jesse Ventura will now decide its fate. He has not indicated a position on the bill. . . Under the bill, ISPs would have to tell Minnesota consumers whenever they plan to disclose such personal information about them as which Web sites they've visited, their e-mail or home addresses or telephone numbers. They also would have to say how the information would be used.
http://news.findlaw.com/ap/ht/1700/5-20-2002/20020520050002_6.html

"The Body" Ponders His Next Move
http://www.canoe.ca/SlamWrestlingVentura/venturap1.html

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2002-05-28 **Internet privacy surveillance**

FindLaw Download This 87

GOVERNOR SIGNS INTERNET PRIVACY BILL
Internet users will be able to control whether their service providers disclose their personal information under a new Minnesota law that could speed federal action on Internet privacy. National Internet companies fought the bill, signed by Gov. Jesse Ventura on Wednesday, and its authors described it as the most comprehensive state Internet privacy law. It won't take effect until March. The law requires ISPs to tell Minnesota consumers whenever they plan to disclose such personal information as which Web sites users have visited, their e-mail or home addresses or their telephone numbers. They also would have to say what the information would be used for.
http://news.findlaw.com/ap/ht/1700/5-22-2002/20020522210004_13.html

FindLaw's Minnesota Legal Resources
http://www.findlaw.com/11stategov/mn/index.html

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2002-06-12 **privacy opt-in financial information confidentiality political activism**

PoliTech, http://www.aclu.org/news/2002/n061202a.html

An ACLU press release began as follows in June 2002:

NEW YORK--The American Civil Liberties Union today congratulated the people of North Dakota for defending their privacy by rejecting a ballot measure that would have allowed banks to share customers' information without their permission. "This vote was a stunning defeat for the powerful financial companies who were trying to bamboozle the citizens of North Dakota into acting against their own interests," said Jennifer Ring, Executive Director of the ACLU of the Dakotas. ...

"The results in North Dakota are significant not just in that state but nationally," said Barry Steinhardt, Director of the ACLU's Technology and Liberty Program. "If the voters in a small midwestern state vote for privacy by more than a three-to-one margin despite an intense media campaign urging them not to, then politicians in Washington and Sacramento and Albany ought to be listening."

"The pro-privacy campaign was waged by a group of citizen-volunteers led by Charlene Nelson, a homemaker and mother of three working out of her home in Casselton. Until a last-minute $25,000 contribution by the ACLU for radio ads, the privacy forces had reported donations of just $2,450."

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2002-06-17 **university campus e-mail government employees freedom-of-information laws FOIA public records**

EDUPAGE

CAMPUS E-MAIL EXPOSED TO PUBLIC SCRUTINY

Many states identify administrators and professors at public colleges as state employees, potentially exposing their letters, documents, and e-mail to public scrutiny under freedom-of-information laws. Some institutions have begun to update policies to safeguard personal e-mail or warn professors to be careful what they write. Open-records laws don't specify clearly whether professors' research notes, lecture notes, or regular mail would qualify as public records, but most states assume that state employees' e-mail messages are public records, even when the law is ambiguous. Employees at private colleges can be exposed as well, although not through open-records laws; a person would need to obtain a court order or a subpoena, requiring involvement in litigation against the college. Chronicle of Higher Education, 17 June 2002 (sub. req'd) http://chronicle.com/free/v48/i41/41a03101.htm

---

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2003-08-28 **privacy law Californai information collection**

NewsScan

CALIFORNIA GETS NEW PRIVACY LAW

California has just passed privacy legislation aimed at preventing banks, insurance companies and other institutions from sharing their personal information, and Gov. Gray Davis said: "Most Californians are stunned to learn that financial corporations trade their names for money. That is wrong, and when I sign this bill, that practice will stop." The law will require permission from a customer before financial institutions share any information on that customer with an unaffiliated company or an affiliated firm in a different line of business. (AP/USA Today 28 Aug 2003)

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2003-09-27 **speech privacy Do-Not-Call list first amendment telemarketers supreme court FTC**

NewsScan

SPEECH, PRIVACY, AND DO-NOT-CALL: 'I WANT TO BE ALONE'
Privacy and free speech are conflicting values in the current controversy over "Do Not Call" legislation aimed at curtailer commercial telemarketing calls (while continuing to allow calls made for political or philanthropic purposes). David Sobel, general counsel for the Electronic Privacy Information Center, says: "The telemarketers have some First Amendment rights to disseminate information. But the consumer also has some rights to control unwanted information coming into the home." Telemarketers argue that their own free-speech rights are being violated by the FTC's attempt to establish a Do-Not-Call list, and UCLA law professor Eugene Volokh explains: "When it comes to residential privacy, the Supreme Court has suggested that content-based discrimination is illegal. The FTC is setting up content-based discrimination." Some legal experts think the government could legally expand the registry to all telemarketers, with a registry that just says, like Greta Garbo, "I want to be alone." Attorney Bruce Johnson, an expert in First Amendment law, says: "I don't think it's restricting political or religious speech. The registry just says that I don't want to hear from anybody." (San Jose Mercury News 27 Sep 2003)

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2004-01-08 **email privacy U.S Treasury TTB violation**

NewsBits; http://news.com.com/2100-1028_3-5137488.html

Treasury breaks word on e-mail anonymity

The U.S. Treasury Department plans to publish nearly 10,000 e-mail addresses on the Web, violating its privacy promise to Americans who used e-mail to comment on a government proceeding. In March 2003, the Treasury Department's Alcohol and Tobacco Tax and Trade Bureau (TTB) asked for e-mail comments about a proposal that could raise the price of malt beverages like Bacardi Breezer and Smirnoff Ice. At the time, the department said that the text of comments would be made public--but assured people that e-mail addresses, home addresses and other personal information of individuals would be removed first.

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2004-05-17 **privacy protection data mining Donald Rumsfeld Pentagon DoD**

NewsScan

PANEL URGES MORE PRIVACY PROTECTIONS IN FEDERAL 'DATA-MINING'

The Technology and Privacy Advisory Committee, a panel created by U.S. Defense Secretary Donald Rumsfeld to scrutinize Pentagon programs in the wake of criticism over the ill-fated "Total/Terrorism Information Awareness" program, is urging Congress to pass laws protecting citizens' civil liberties from overly intrusive federal data mining activities. "The Department of Defense should safeguard the privacy of U.S. persons when using data mining to fight terrorism," says the panel's report, which notes that privacy laws lag far behind current capabilities in information and communications technology. A key recommendation suggests federal agencies should be required to obtain approval from a special federal court "before engaging in data mining with personally identifiable information concerning U.S. persons." Former FCC Chairman Newton Minow, who headed up the panel, acknowledges that the proposals would "impose additional burdens on government officials," but maintains that the requirements would improve national security while enhancing personal privacy: "Good privacy protection in the context of data mining is often consistent with more efficient investigation." (New York Times 17 May 2004)

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2004-06-30 **e-mail eavesdropping OK litigation court ruling privacy surveillance law enforcement anti-terrorism Homeland Security**

NewsScan

COURT RULES E-MAIL EAVESDROPPING OKAY

In a surprise decision, a federal appeals court has ruled that it was acceptable for a company that offered e-mail service to peruse messages sent by its subscribers. The case stems from 1998 when it was discovered that Interloc, a now-defunct literary clearinghouse, surreptitiously copied messages sent to its subscribers by rival Amazon in order to "develop a list of books, learn about competitors and attain a commercial advantage." An Interloc executive was later indicted on an illegal wiretapping charge, but yesterday's ruling upheld a federal judge's dismissal of that charge on the
grounds that the e-mails were copied while in "electronic storage" (during the process of being routed through a network of servers to recipients). The Wiretap Act prohibits unauthorized eavesdropping on messages that are not stored -- such as a real-time telephone conversation -- but does not afford the same protection to stored messages. In a dissenting opinion, Appeals Court Judge Kermit Lipez wrote that the ruling unravels "decades of practice and precedent regarding the scope of the Wiretap Act" and essentially renders the act "irrelevant to the protection of wire and electronic privacy." In a concurring statement, the Electronic Frontier Foundation said that yesterday's ruling "dealt a grave blow to the privacy of Internet communications." (AP 30 Jun 2004)

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2004-08-28 **Federal Communications Commission FCC telephone outage information kept private**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/articles/A40329−2004Aug 27.html

August 28, Washington Post — FCC cuts public line to phone outage data.

The Federal Communications Commission (FCC), citing concerns about national security, has abandoned a 10-year-old policy and will no longer give the public access to information about past telephone network outages. The decision has angered consumer advocates and some state regulators who say the data are a critical tool in evaluating phone service reliability around the country. Large companies use the information to make decisions about where they build their own networks and to plan for key facilities such as data centers. While the FCC limited the amount of information it is making public, it has expanded the amount of information it collects from the wireless and satellite industries. Under the new rules, wired, mobile and satellite carriers must report an outage that affects 900,000 user minutes or more. Although the FCC will not make the information it collects about the outages public, the companies are free to keep the public informed about outages as they are occurring.

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2004-10-01 **clickwrap agreements tiny print examination study privacy security operability utility usability legal mumbo-jumbo privacy**

NewsScan; http://www.wired.com/wired/archive/12.10/view.html?pg=2

WHAT THE WORLD NEEDS IS MORE LAWYER-BOTS

Mark Rasch, founder and former head of the U.S. Justice Department's computer crimes unit, says that the increasing trend toward lengthy, tiny-font policy "agreements" that users must click on before they can access a Web site are generating the need for more legal oversight. "Increasingly, companies have been putting some pretty nasty things into their clickwrap agreements -- such as that they can collect and sell your detailed personal information or install software that will capture your every keystroke … This is not legal boilerplate, the kind that everybody assents to when renting a car or buying a ticket to a ball game. It affects the privacy, security, and operability of all of the information you access online." Rasch says what's desperately needed is a law robot -- "a browser-based automaton that could be adjusted to match your tolerance for legal mumbo-jumbo… Once you establish privacy settings, your browser would transfer personal data (after prompting you) only to sites that conform with your privacy requirements." Rasch says such technology would go a long way toward eradicating such online nuisances as porn spam and spyware. "We will never fully automate the reading of contracts or agreements online. Nor would we want to -- after all, Internet lawyers need jobs, too. But by automating the vetting of clickwraps or implied agreements we could make everybody sleep a little easier."

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2004-10-05 **spyware legislation US House Representatives**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A9558-2004Oct5.html

HOUSE PUNISHES SPYWARE PERPETRATORS

The U.S. House of Representatives has voted 399-1 to pass the "Spy Act," which imposes heavy federal fines on those who secretly install "spyware" programs on people's computers to surreptitiously monitor their Internet activities. The bill was introduced by Rep. Mary Bono (R-Calif.).

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2005-02-02 **blogs weblog Apple Tiger EFF journalism privacy rights sources**

NewsScan; http://www.usatoday.com/tech/news/techpolicy/2005-02-02-about-a-blog_x.htm

WHO GETS TO DECIDE WHAT JOURNALISM IS?

A California court will soon decide whether bloggers have the same legal protections as journalists under "shield" laws that protect reporters from revealing their sources. Electronic Frontier Foundation attorney Kurt Opsahl, who represents two bloggers targeted by Apple for leaking information about new company products, maintains that if the bloggers are forced to give up their sources "the public will lose out on a vital outlet for independent news, analysis, and commentary." An opposing view is offered by University of Iowa law professor Randall Bezanson, who says that simply expressing opinions to a tiny audience isn't journalism -- because if it were "then I'm a journalist when I write a letter to my mother reporting on what I'm doing. I don't think the free-press clause [of the U.S. Constitution] was intended to extend its protections to letters to mothers from sons." (USA Today 2 Feb 2005)

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2005-02-08 **voyeur state law legal privacy**

NewsScan; http://www.usatoday.com/tech/news/2005-02-08-video-voyeur_x.htm

VIDEO VOYEURS

Prosecutors across the country have been finding that loopholes in state laws make it difficult to convict individuals who shoot voyeuristic "upskirting" or "downblousing" videos of teenagers at public places like the local mall. Most states with video voyeurism laws prohibit unauthorized videotaping or photographing of people who are in private areas, such as dressing rooms, or in situations where they have "a reasonable expectation of privacy" -- but public places pose a different problem. One Virginia state delegate says, "It's certainly immoral, it's certainly wrong, but under the code, it's just not a written offense. We're trying to tighten the code so some pervert isn't able to do that." But attorney Lawrence Walters counters: "Certainly it's a good idea to stop perverts from filming down women's blouses or up little girls' skirts. But we have to step back as a society once we get past that visceral reaction and think this through." Mary Lou Leary of the National Center for Victims of Crime suggests that the problem is the public's diminished expectation of a right to privacy: "We're used to the notion that if you're in a public place, you can take pictures and you can be photographed." (AP/USA Today 8 Feb 2005)

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2005-02-15 **law legal spyware Florida wiretapping**

NewsScan; http://news.com.com/Court+Wife+broke+law+with+spyware/2100-1030_3-5577979.html

WIFE BROKE LAW IN USING SPYWARE

A Florida appeals court has ruled that a suspicious wife, who installed spyware on her husband's computer to secretly monitor and record his electronic interactions with another woman, violated Florida's wiretapping law. The law says anyone who "intentionally intercepts" any "electronic communication" commits a criminal act. The wife had argued that her use of Spector spyware should be viewed as similar to reading a stored file on her husband's computer. But Judge Donald Grincewicz wrote that "because the spyware installed by the wife intercepted the electronic communication contemporaneously with transmission, copied it and routed the copy to a file in the computer's hard drive, the electronic communications were intercepted in violation of the Florida Act." (CNet News.com 15 Feb 2005)

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2005-03-15 **privacy concerns data information disclosure identity ID theft Social Security Number use restrictions lawmakers laws**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=7911154

U.S. CONSIDERS RESTRICTIONS ON SOCIAL SECURITY NUMBERS

Following recent incidents that exposed personal information on more than 175,000 individuals, U.S. lawmakers are considering placing new restrictions on companies that gather and sell such information. Relatively few regulations apply to companies such as ChoicePoint and LexisNexis that collect data about driving records, financial records, and other sensitive information. Social Security numbers appear to be at the crux of the issue: because they are unique, data companies rely on Social Security numbers to distinguish individuals, but the numbers are also a powerful weapon in the hands of identity thieves, who can use them to access confidential records, open new accounts, and wreak havoc with a person's privacy. At separate hearings in the House and the Senate, legislators discussed laws that would require data companies to notify any individual before they sell that person's Social Security number. Other suggestions included requiring disclosure of any incident that exposes sensitive information. Don McGuffey, vice president of ChoicePoint, which recently sold 145,000 records to identity thieves, told a Senate hearing that personal information had been compromised by his company in "a handful" of other incidents that were not made public. Reuters, 15 March 2005

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2005-03-24 **federal agencies bank security breach customer disclosure Fair and Accurate Credit Transactions Act FACT**

EDUPAGE; http://www.pcworld.com/news/article/0,aid,120168,00.asp

FEDS ORDER BANKS TO DISCLOSE BREACHES

Four federal agencies have released regulations requiring banks and other financial institutions to notify customers when a security breach presents a risk that their personal information may be misused. The Federal Reserve, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision deliberated for 18 months on how federal legislation, including the Fair and Accurate Credit Transactions (FACT) Act, should be interpreted. The resulting "guidance" stipulates that when personal information is accessed without authorization and misuse of that information has occurred or is reasonably possible, institutions must notify affected customers "as soon as possible." In all cases, even those that do not meet the standard set for notifying customers, institutions must notify their primary federal regulators of the breach. Delays in notifying customers are permissible if such notification is determined to jeopardize an investigation into the breach. PCWorld, 24 March 2005

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2005-04-29 **civil liberties privacy concerns USA PATRIOT Act renewal House Senate ACLU critical litigation**

EDUPAGE; http://chronicle.com/prm/daily/2005/04/2005042901t.htm

HEARINGS FOCUS ON LIBRARY PROVISIONS OF USA PATRIOT ACT

Amid both House and Senate hearings on whether to renew certain portions of the USA PATRIOT Act, supporters and critics of Section 215, which authorizes law enforcement to obtain records from libraries and other institutions, have lined up to voice their opinions. Section 215 allows gaining access to various types of records with only the approval of a secret court. Further, those whose information has been collected are barred from disclosing that fact, even to attorneys. Representatives of the American Civil Liberties Union (ACLU), which has been highly critical of the legislation, said they could support its renewal if several concessions were made, including limiting the authority to investigate only "agent[s] of a foreign power" and eliminating the gag order for those under investigation. Groups including the American Library Association said they supported the ACLU's recommendations. Rep. Howard Coble (R-N.C.) defended the law as it stands, saying there has been much "misinformation" about Section 215 and how it has been used. Kenneth L. Wainstein, U.S. attorney for the District of Columbia, said that the law has not been used to obtain records from libraries, though he acknowledged that it could be used that way in the future. Chronicle of Higher Education, 29 April 2005 (sub. req'd)

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2005-06-15 **civil liberties privacy concerns USA PATRIOT Act powers limited US House of Representatives patron information disclosure**

EDUPAGE; http://www.wired.com/news/privacy/0,1848,67880,00.html

HOUSE VOTES TO LIMIT PATRIOT ACT

The U.S. House of Representatives has voted 238-187 to impose limits on the powers of the U.S.A.P.A.T.R.I.O.T. Act. Sponsored by Rep. Bernard Sanders (I-Vt.), the measure would eliminate federal authority granted by the U.S.A.P.A.T.R.I.O.T. Act to compel libraries and bookstores to disclose information about books their patrons have checked out or bought, without first obtaining a search warrant; the measure would preserve the right for government officials to obtain Internet search records from libraries.
Although Attorney General Alberto Gonzales recently told Congress that federal authorities have never invoked the power, a number of libraries have begun deleting patron records to preempt the possibility of having to turn them over. Sanders called the vote "a tremendous victory that restores important constitutional rights to the American people." Rep. Tom Feeney (R-Fla.) defended the powers, saying that federal authorities need tools to help them identify planned terrorist activities and prevent attacks before they happen. The measure has not been introduced by the Senate, and President Bush has promised to veto the bill if it passes. Wired News, 15 June 2005

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2005-07-15 **GAO Information Security rely tampering disruptions operations fraud disclosure account FISMA GAO**

DHS IAIP Daily; http://www.gao.gov/cgi−bin/getrpt?GAO−05−552

INFORMATION SECURITY: WEAKNESSES PERSIST AT FEDERAL AGENCIES DESPITE PROGRESS MADE IN IMPLEMENTING RELATED STATUTORY REQUIREMENTS (REPORT)

Federal agencies rely extensively on computerized information systems and electronic data to carry out their missions. The security of these systems and data is essential to prevent data tampering, disruptions in critical operations, fraud, and inappropriate disclosure of sensitive information. Concerned with accounts of attacks on systems via the Internet and reports of significant weaknesses in federal computer systems that make them vulnerable to attack, Congress passed the Federal Information Security Management Act (FISMA) in 2002. In accordance with FISMA requirements that the Comptroller General report periodically to the Congress, GAO's objectives in this report are to evaluate (1) the adequacy and effectiveness of agencies' information security policies and practices and (2) the federal government's implementation of FISMA requirements. GAO recommends that the Director of the Office of Management and Budget (OMB) implement improvements in the annual FISMA reporting guidance. In commenting on a draft of this report, OMB agreed with GAO's overall assessment of information security at agencies but disagreed with aspects of our recommendations to enhance its FISMA reporting guidance.

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2005-07-28 **Congress measures Personal Data Privacy and Security Act FTC Social Security Number sale**

EDUPAGE; http://news.com.com/2100-7348_3-5808894.html

CONGRESS GETS SERIOUS ABOUT DATA PRIVACY

Ahead of its August recess, Congress moved data-security measures to the top of its agenda, with various House and Senate committees considering three different bills dealing with the protection of sensitive information. The broadest legislation being considered is the Personal Data Privacy and Security Act, which would place new restrictions on how personal information may be used and imposes criminal penalties for those found to have violated it. The bill would limit the sale and publication of Social Security numbers, require notification of consumers in the event their personal data is compromised, and restrict the authority of the states in writing their own regulations for data protection. Other bills working their way through the Senate include similar requirements that consumers be notified of data breaches, but they only include civil penalties. The other measures, including one passed by the Senate Commerce Committee, place oversight and enforcement authority with the Federal Trade Commission (FTC). Critics of the proposed legislation argue that it is being rushed through without proper discussion. CNET, 28 July 2005

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2005-08-26 **civil liberties privacy concerns USA PATRIOT Act government surveillance Supreme Court decision Connecticut library FBI investigation ACLU lawsuit litigation**

EDUPAGE; http://www.nytimes.com/2005/08/26/politics/26patriot.html

FBI SEEKS LIBRARY RECORDS

According to the American Civil Liberties Union (ACLU), the FBI is using one of the powers granted by the USA PATRIOT Act to demand the records of a library in Connecticut. Because the USA PATRIOT Act also forbids disclosure of details surrounding such investigations, the name of the library in question is being kept confidential, though it is known to be a member of the American Library Association. At issue is the authority to subpoena library records using something called a national security letter, which does not require a judge's approval. The ACLU has filed a federal lawsuit on behalf of the library, saying "it should not be forced to disclose such records without a showing of compelling need and approval by a judge." Anthony D. Romero, executive director of the ACLU, said, "This is a prime example of the government using its U.S.A.P.A.T.R.I.O.T. Act powers without any judicial oversight to get sensitive information on law-abiding Americans." The FBI did not comment on the lawsuit, but the agency's national security letter noted that it was seeking the library records as part of an investigation "to protect against internal terrorism or clandestine intelligence activities." New York Times, 26 August 2005 (registration req'd)

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2005-09-01 **civil liberties privacy concerns USA PATRIOT Act government surveillance Supreme Court decision Connecticut library FBI investigation ACLU lawsuit litigation**

EDUPAGE; http://chronicle.com/daily/2005/09/2005090102t.htm

NO DECISION YET FROM JUDGE ON PATRIOT ACT CASE

U.S. District Court Judge Janet C. Hall has postponed deciding whether a Connecticut library may publicly disclose its identity as the institution whose records have been sought by the FBI under the PATRIOT Act. The act forces any organization whose records have been subpoenaed to be silent about the investigation, but the library in question and the American Civil Liberties Union have filed a suit, alleging that such restrictions are unconstitutional. Hall heard arguments from both sides this week but declined to issue a ruling until she hears more from the FBI. Observers noted that Hall seemed dubious of the government's claim that identifying the library would threaten the investigation. She said the FBI must demonstrate that risk, which it so far has not done. Pointing out that controversial provisions of the PATRIOT Act are under review by Congress, Hall suggested that allowing the public to see how the law is being applied could be an important factor in deciding whether the act will be extended. Chronicle of Higher Education, 1 September 2005 (sub. req'd)

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2005-09-21 **information technology association America ITAA Congress law data security breach**

EDUPAGE; http://www.fcw.com/article90869-09-21-05-Web

ITAA CALLS FOR NATIONAL DATA-BREACH NOTIFICATION LAW

The Information Technology Association of America (ITAA) has called on Congress to pass federal legislation that would specify the conditions under which companies and government agencies would be required to notify consumers regarding breaches of data security. According to Greg Garcia, vice president of information security programs and policy at the ITAA, 17 states have passed such laws, 8 of which have gone into effect. The ITAA recommends a federal law that would provide clear definitions of data breaches, identify circumstances under which notification would be required, and detail the ways in which notification must take place. Furthermore, the ITAA said a federal data-breach law should take precedence over state laws that might otherwise weaken the federal law. Both houses of Congress have taken up the topic of requiring notification, but so far only one bill, sponsored by Sen. Dianne Feinstein (D-Calif.), has been introduced. Federal Computer Week, 21 September 2005

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2005-11-11 **privacy concerns USA PATRIOT Act US government surveillance bill law Congress terrorism anti-terrorism**

EDUPAGE; http://chronicle.com/daily/2005/11/2005111101t.htm

CONGRESS EXAMINES CONTROVERSIAL PORTIONS OF PATRIOT ACT

Members of a Congressional committee this week took up discussions of the USA PATRIOT Act, including two highly controversial sections of the law. Several provisions of the law are scheduled to expire this year, and the committee is charged with reconciling House and Senate proposals to extend those provisions. Expected to be the focus of the discussions are Sections 215 and 505, which greatly expand federal authority to obtain information such as phone and library records on individuals and which prevent those under investigation from revealing, even to their attorneys, that they are under investigation. Advocates for civil liberties have been pressing federal officials for details on how these key sections of the law have been applied, including a letter recently sent by five U.S. Senators to Attorney General Alberto Gonzales, demanding data on how many so-called national security letters have been issued since the PATRIOT Act was enacted. Although federal officials have revealed few specifics, supporters of the legislation argue that "vigorous oversight by congressional committees has uncovered no instances of abuse," according to Sen. Pat Roberts (R-Kans.). Rep. John Conyers (D-Mich.) noted, "The very act of surveilling citizens who aren't even suspected of wrongdoing is an abuse in itself." Chronicle of Higher Education, 11 November 2005 (sub. req'd)

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2005-11-18 **privacy concerns USA PATRIOT Act extension opposition US government surveillance bill law House Senate terrorism anti-terrorism**

EDUPAGE; http://chronicle.com/daily/2005/11/2005111801t.htm

REACTION TO EXPECTED EXTENSION OF PATRIOT ACT PROVISIONS

Groups opposed to two provisions of the USA PATRIOT Act up for review expressed disappointment at a tentative plan to extend both. The proposed extension was written by a conference committee charged with reconciling House and Senate versions of a bill covering the parts of the act that will otherwise expire at the end of the year. Under the plan, the provision that allows the government to issue so-called national security letters without a judge's approval would be made permanent and would allow for criminal prosecutions of individuals who reveal that they have received such a letter. The plan does not make changes to the second section of the act at issue, the library provision, that were included in the Senate bill. Those changes included requiring the government to demonstrate a connection between terrorists and individuals whose records were sought. The Senate bill also called for another review of the library provision in four years; under the proposal, it would not be reviewed for seven years. The plan does include limited concessions. Those who receive national security letters would be allowed to discuss them with their attorneys, and the government would be required to disclose certain details about how the national security letters are used. Chronicle of Higher Education, 18 November 2005 (sub. Req'd)

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2005-12-06 **California law bill data security standards privacy protection state government efforts**

EDUPAGE; http://chronicle.com/daily/2005/12/2005120601t.htm

CALIFORNIA LAW SETS NEW DATA-SECURITY STANDARDS

California has passed a new data-protection law that may serve as a model for other states, despite the reaction of academic researchers, many of whom see it as an obstacle to their efforts at conducting research efficiently. The new law is intended to safeguard individuals' personal information when it is used by any research organization. Under the law, before any state agency may release personal data, the state's Committee for the Protection of Human Subjects must assess the research and determine whether it would adequately protect the requested data. Researchers seeking data from state agencies must show that the data are necessary; ensure that data are destroyed or returned when the project is completed; and, when possible, use information other than Social Security numbers as unique identifiers for subjects. Academic researchers largely object to the new law, saying it will impede some aspects of their research. Chronicle of Higher Education, 6 December 2005 (sub. req'd)

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2005-12-11 **cell mobile phone tracking privacy surveillance law enforcement probable cause court case lawsuit litigation**

RISKS; http://tinyurl.com/b4fhk 24 12

CELLPHONE TRACKING AND PRIVACY

Cellular operators know, within about 300 yards, the location of their subscribers whenever a phone is turned on. The operators have said that they turn over location information when presented with a court order to do so. However, in the last four months, three federal judges have denied prosecutors the right to get cellphone tracking information from wireless companies without first showing "probable cause" to believe that a crime has been or is being committed. That is the same standard applied to requests for search warrants.

[Abstract by Peter G. Neumann]

Dr Neumann notes: "Missouri has granted a contract for statewide cell-phone tracking."

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2005-12-15 **Internet policing privacy FTC act spam control foreign governments**

DHS IAIP Daily; http://news.zdnet.com/2100−9588_22−5996703.html

SENATE PANEL APPROVES MORE INTERNET-POLICING POWERS

The Federal Trade Commission (FTC) would gain expanded policing powers and could share information about spammers and other miscreants with foreign governments under a bill approved Thursday, December 15, by a U.S. Senate panel. Called the Undertaking Spam, Spyware, and Fraud Enforcement with Enforcers Beyond Borders Act of 2005, the proposal is nearly identical to legislation pushed by the FTC itself two years ago that drew concerns from civil liberties groups and was never enacted. In essence, the bill would expand existing FTC powers so that the agency could go after any "unfair or deceptive practices" that are likely to cause "foreseeable injury" on U.S. soil or involve conduct in the United States. Intended by its sponsors to help combat such menaces as spam, spyware and telemarketing fraud carried out on international turf, the bill would allow the FTC to collaborate with foreign law enforcement agencies and swap information on a reciprocal basis. Further detail on this Act can be found at: http://thomas.loc.gov/cgi-bin/bdquery/z?d109:s.01608:

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2005-12-15 **US government surveillance FTC policing bill Undertaking Spam Spyware Fraud Enforcement Enforcers Beyond Borders Act 2005**

EDUPAGE; http://news.zdnet.com/2100-9588_22-5996703.html

SENATE PANEL PROPOSES NEW FTC POLICING POWERS

A bill approved by a U.S. Senate panel would give the Federal Trade Commission (FTC) increased policing power and the authority to share with foreign governments information about spammers and others suspected of illegal acts. Called the Undertaking Spam, Spyware, and Fraud Enforcement with Enforcers Beyond Borders Act of 2005, the proposal mimics legislation requested by the FTC two years ago that roused objections from civil liberties groups and was not enacted. Collaboration with foreign law enforcement agencies would permit the commission to address problems such as spyware and telemarketing fraud that cross national borders. It has yet to be debated by the full Senate and U.S. House of Representatives. ZDNet, 15 December 2005

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2006-01-26 **phone record privacy politician plea regulation FCC**

DHS IAIP Daily; 23
http://news.com.com/Politicians+call+for+better+phone+record +privacy/2100−1036_3−6031916.html?tag=cd.top

POLITICIANS CALL FOR BETTER PHONE RECORD PRIVACY.

In response to disclosures about phone records being sold on the Internet, politicians want federal regulators to verify that the biggest service providers are adequately protecting their customers' information. According to a letter sent by the chairmen of the U.S. House of Representatives Energy and Commerce Committee, all telecommunications providers must "certify annually" with the Federal Communications Commission (FCC) that they are in compliance with the federal rules. The politicians asked the FCC to turn over the latest certifications from the five largest wireless and wireline providers, along with statements from the companies describing "how their internal procedures protect the confidentiality of consumer information." Citing their ongoing investigation about the matter, the legislators imposed a Monday, January 30, deadline. The House returns from its winter recess Tuesday, January 31. The issue of the illicit brokering of phone records has drawn attention recently, with carriers such as T-Mobile, Verizon Wireless and Cingular Wireless and also the state of Illinois filing suits against third-party brokers accused of the practice. On Monday, January 23, T-Mobile landed a temporary restraining order, which prohibits at least two companies from directly or indirectly obtaining its customers' information. Letter sent by the chairman of the U.S. House of Representatives Energy and Commerce Committee: http://markey.house.gov/docs/privacy/iss_privacy_ltr060123.pdf

---

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2006-02-01 **Congress hearing cell-phone customer privacy wiretapping data disclosure theft**

EDUPAGE; http://news.zdnet.com/2100-1035_22-6033688.html 23

CONGRESS HOLDS HEARINGS ON CELL-PHONE CUSTOMER PRIVACY

A Congressional hearing this week will address cell phone companies' efforts to protect the privacy of their customers. The hearing comes after recent revelations that a number of data brokers have been able to con cell phone companies into disclosing data about customers and their calling habits, which was then sold to third parties. The premise is that certain individuals, such as attorneys, might want details of cell phone calls, and data brokers supply that data. Cell phone companies and some members of Congress, however, object to the methods that data brokers use to obtain that information, including posing as people they are not and using information such as Social Security numbers without authorization. Some critics have pointed to weak policies and practices among cell phone companies for protecting such data as the root of the problem. Rep. Joe L. Barton (R-Tex.), chairman of the House Energy and Commerce Committee, said in a statement that he intends to make the practice of fraudulently obtaining such data "very illegal."

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2006-02-06 **Microsoft Washington state lawsuit anti-spyware company Secure Company Spyware Cleaner ineffective dangerous charge**

DHS IAIP Daily; 23
http://computerworld.co.nz/news.nsf/scrt/F03EF851B098CED6CC25710900776B50

MICROSOFT AND WASHINGTON STATE SUE SPYWARE COMPANY.

Microsoft and the Washington state attorney general have filed lawsuits against antispyware software vendor Secure Computer, alleging that the company's Spyware Cleaner software not only fails to remove spyware as advertised, but makes changes to users ' computers that make them less secure. The attorney general's lawsuit is the state's first to be filed under Washington's 2005 Computer Spyware Act. Washington's 16-count lawsuit was filed in U.S. District Court in Seattle and follows investigations by both Microsoft and the Attorney General's high tech fraud unit. The state's lawsuit also names Secure Computer president Paul Burke and Web domain owner Gary Preston, both of New York state, as defendants. It further charges Zhijian Chen, of Portland, OR; Seth Traub, of Portsmouth, NH; and Manoj Kumar, of Maharashtra, India, in connection with the advertising of the product. Microsoft has also sued Secure Computer, alleging that the company's Spyware Cleaner e-mail and pop-up advertisements falsely suggested that Microsoft endorsed the product, says Nancy Anderson, vice president and deputy general counsel with Microsoft.

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2006-02-14 **court ruling unencrypted data okay negligence lawsuit rejection GLB Act compliance**

EDUPAGE; http://news.com.com/2100-1030_3-6039645.html 23

COURT SAYS UNENCRYPTED DATA OKAY

A federal judge in Minnesota has dismissed a case alleging that a student loan company was negligent in not encrypting customer data. The case was filed by Stacy Lawton Guin after a laptop containing unencrypted data on about 550,000 customers of Brazos Higher Education Service was stolen from an employee's home in 2004. Although he was not harmed by the loss of his personal information--indeed, there have been no reports of any fraud committed with the stolen information--Guin argued that the Gramm-Leach-Bliley (GLB) Act required Brazos to encrypt the data. Judge Richard Kyle rejected that claim, noting that the legislation does not specifically require encryption. The law states that financial services companies must "protect the security and confidentiality of customers' nonpublic personal information," but, according to Kyle's decision, "The GLB Act does not prohibit someone from working with sensitive data on a laptop computer in a home office."

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2006-03-06 **anonymity Internet Web USENET BBS postings prohibition law bill proposal**

RISKS; Slashdot http://yro.slashdot.org/article.pl?sid=06/03/06/1736234 24 18

NEW JERSEY BILL WOULD HAVE BANNED ANONYMOUS POSTINGS

A firestorm broke out on Slashdot and other Internet-centric discussion sites after someone posted the following announcement: "The New Jersey legislature is considering a bill that would require operators of public forums to collect users' legal names and addresses, and effectively disallow anonymous speech on online forums. This raises some serious issues, such as to what extent local and state governments can go in enacting and enforcing Internet legislation."

Vigorous discussion ensued, including this cogent posting by "orthogonal":

MR. JUSTICE Hugo Black, writing for the Supreme Court of the United States in Talley v. California, 362 U.S. 60 (1960), declaring unconstitutional a California ordinance requiring that handbills and pamphlets be signed:

>Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all. The obnoxious press licensing law of England, which was also enforced on the Colonies was due in part to the knowledge that exposure of the names of printers, writers and distributors would lessen the circulation of literature critical of the government. The old seditious libel cases in England show the lengths to which government had to go to find out who was responsible for books that were obnoxious [362 U.S. 60, 65] to the rulers. John Lilburne was whipped, pilloried and fined for refusing to answer questions designed to get evidence to convict him or someone else for the secret distribution of books in England. Two Puritan Ministers, John Penry and John Udal, were sentenced to death on charges that they were responsible for writing, printing or publishing books…. Before the Revolutionary War colonial patriots frequently had to conceal their authorship or distribution of literature that easily could have brought down on them prosecutions by English-controlled courts. Along about that time the Letters of Junius were written and the identity of their author is unknown to this day. Even the Federalist Papers, written in favor of the adoption of our Constitution, were published under fictitious names. It is plain that anonymity has sometimes been assumed for the most constructive purposes.

We have recently had occasion to hold in two cases that there are times and circumstances when States may not compel members of groups engaged in the dissemination of ideas to be publicly identified. Bates v. Little Rock, 361 U.S. 516 ; N. A. A. C. P. v. Alabama, 357 U.S. 449, 462 . The reason for those holdings was that identification and fear of reprisal might deter perfectly peaceful discussions of public matters of importance. This broad Los Angeles ordinance is subject to the same infirmity. We hold that it, like the Griffin, Georgia, ordinance, is void on its face. [362 U.S. 60, 66]<

[MK notes that by June 2006, the NJ legislature's Web site no longer had any reference to the proposed bill.]

Category 38.6 US case law, legislation & regulation concerning individual privacy (not govt s

2006-03-24 **US legislation data-protection bill DATA identity theft**

EDUPAGE; http://www.internetnews.com/bus-news/article.php/3594136 23

LEGISLATORS AGREE ON DATA-BREACH TERMS

Members of a House committee have agreed on compromise language in a data-protection bill intended to provide increased protections for sensitive consumer information. The Data Accountability and Trust Act (DATA) includes definitions of when organizations must report a data breach to customers and requires companies that handle such information to meet minimum standards for protecting sensitive data. In its original form, the bill only required disclosure if an event carried a "significant risk" of identity theft. The compromise language mandates notification if a "reasonable threat" exists. The bill requires data stewards to take "reasonable" precautions against data theft and to perform periodic assessments to verify that data has not been compromised. Rep. Joe Barton (R-Tex.), chair of the Energy and Commerce Committee, said the existing statutes for data protection "are so flimsy they're laughable." Rep. John Dingell (D-Mich.) said the DATA bill "focuses on strong security systems, notice to consumers of breaches, and tough enforcement."

Category 38.6 US case law, legislation & regulation concerning individual privacy (not govt s

2006-03-31 **US Senate phone record privacy bill legislation protection penalties violation**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1944817,00.asp 23

U.S. SENATE PANEL BACKS PHONE RECORD PRIVACY BILL.

The U.S. Senate Commerce Committee Thursday, March 30, approved legislation to protect consumers' telephone records by making it illegal to sell such information without consent. The measure would boost penalties to as much as $30,000 per incident and up to $3 million for continuing violations by telephone companies that fail to properly safeguard consumer information. The bill would also require carriers to inform consumers if their information was accessed without permission.

Category 38.6 US case law, legislation & regulation concerning individual privacy (not govt s

2006-05-11 **Congress debate SSN restrictions identity theft fraud detection**

EDUPAGE; http://news.com.com/2100-7348_3-6071441.html 23

CONGRESS DEBATES SSN RESTRICTIONS

Members of Congress have vowed to enact legislation by the end of the year that will restrict use of Social Security numbers (SSNs), which have become a prime target of identity thieves. Several bills are before Congress now, including one introduced by Edward Markey (D-Mass.) and another by Clay Shaw (R-Fla.). Joe Barton (R-Tex.) said the current practice of allowing data brokers to sell SSNs to anyone able to pay for them should be banned outright. Federal Trade Commissioner Jon Leibowitz said SSNs are "overused" and "underprotected." Officials from financial services institutions cautioned, however, that appropriate use of SSNs is invaluable for sectors such as theirs. Oliver Ireland, representing the Financial Services Coordinating Council, said SSNs "are critical for fraud detection."

Category 38.6 US case law, legislation & regulation concerning individual privacy (not govt s

2006-05-12 **data breach legislation discuss Consumer Data Protection Act**

EDUPAGE; http://www.internetnews.com/bus-news/article.php/3605666 23

DATA-BREACH LEGISLATION ON THE AGENDA

Rep. James Sensenbrenner (R-Wis.), chairman of the House Judiciary Committee, has introduced the Cybersecurity Enhancement and Consumer Data Protection Act of 2006, which would require notification of government officials--but not of those affected--any time a computer breach exposes data for 10,000 or more individuals. Data-breach bills have previously been introduced by the House Financial Services Committee and the House Commerce Committee, with varying requirements for notification. In the Senate, two bills have been introduced in the Judiciary Committee and a third in the Commerce Committee. Some observers are concerned that the competing federal legislation, which would likely supersede any state laws concerning data-breach disclosure, risks being reconciled into a law that would be worse than if no law were passed. Susanna Montezemolo of the Consumers Union expressed support for one of the Senate bills, the Personal Data Privacy and Security Act, which has been approved by committee and is waiting for a vote in the full Senate.

Category 38.6 *US case law, legislation & regulation concerning individual privacy (not govt s*

2006-05-16 **identification authentication Social Security Number SSN theory misunderstanding politicians Congress laws mistake problem design flaw error misunderstanding ignorance**

RISKS 24 29

SSNs AS BOTH IDENTIFICATION AND AUTHENTICATION

Jeremy Epstein noted in RISKS that politicians do not necessarily understand security fundamentals. In congressional testimony from the American Financial Services Association, the spokesperson said, ""The Social Security number is the only unique identifier in our country that enables a credit grantor, or a credit bureau, or a bank, or an insurance company, or an investment firm to be sure that the consumer they are doing business with [is legitimate]." Epstein explained, "In other words, they're using it as both an identifier and an authenticator." He also wrote, "Switching to a different number … that is used for both purposes will have the same problem."

His final words were important: "Until Congress understands the problem, there's not much hope of solving it through legislation."

38.7 Other case law, legislation & regulation concerning individual privacy (not govt surveillance)

Category 38.7 *Other case law, legislation & regulation concerning individual privacy (not govt*

1998-01-29 **privacy government e-commerce Internet Web**

EDUPAGE

CANADIAN EFFORTS TO ENSURE PRIVACY ON NET
The Canadian government says it will introduce legislation this fall to protect the privacy of individuals who conduct business on the Internet. The law, which the government wants to have in place by 2000, will also apply to other forms of computer-based e-commerce and personal data transfer in sectors under federal jurisdiction, including the banking sector. The law will try to ensure that personal data collected by businesses for one purpose are not used for other purposes without the consent of the individual, and will prohibit managers of medical databases from notifying insurance companies that a person had down-loaded fact sheets about AIDS or other diseases. (Toronto Globe & Mail 27 Jan 98)

Category 38.7 *Other case law, legislation & regulation concerning individual privacy (not govt*

1999-01-12 **digitised signature driver's license**

THE DOMINION (New Zealand)

The New Zealand government announced that new driver's licenses would bear a digitised signature. An opposition member of the legislature, Neal King, protested that storing such signatures in insecure databases would lead to disaster.

Category 38.7 *Other case law, legislation & regulation concerning individual privacy (not govt*

1999-04-20 **privacy personal information protection law bill act Europe**

Wired

Canadian legislators moved quickly to conform to the European Union Data Privacy Directive. The Personal Information Protection and Electronic Documents Act C-54 would provide consumers with considerably more control over the way data about themselves could be collected and used. US delays in conforming to the Directive threatened international trade with Europe and other collaborators in the effort to increase privacy.

Category 38.7 *Other case law, legislation & regulation concerning individual privacy (not govt*

1999-04-22 **privacy law Canada European Privacy Directive bill proposal**

National Post (Canada) editorial

An editorial by Richard C. Owens in Canada's right-wing, business-oriented _National Post_ newspaper criticized Bill C-54, the Personal Information Protection and Electronic Documents Act, claiming that "If passed and enforced, this law will impede transactions and lower asset values across the country." The writer argued that restrictions on sale of customer or prospect databases as part of the assets of a company would lower the value of companies; that inability to exchange information would harm outsourcing; and that the law addresses a problem that looms large in the public mind but is in fact a minor issue in practice.

Category 38.7 *Other case law, legislation & regulation concerning individual privacy (not govt*

2000-01-27 **censorship privacy international regulation Internet chat**

NewsScan, New York Times
http://www.nytimes.com/library/tech/00/01/biztech/articles/27china.html

The mainland Chinese government announced yet more of its usual stream of draconian prohibitions against free speech and free thought when it barred anyone from posting "state secrets" on the Internet or via e-mail. A state secret in the People's Republic of China is any information that has not been officially approved for distribution; examples include but are not limited to news of natural disasters, reports of bureaucratic corruption, outbreaks of disease, and worker protests. However, experts predicted that the regulations would ultimately be futile; even now, the sheer volume of e-mail and chat-room communications precludes monitoring more than a tiny percentage of the traffic. As the number of Internet users in China rises, the task will be even greater for the tyrants attempting to control the most popular country in the world.

Category 38.7 *Other case law, legislation & regulation concerning individual privacy (not govt*

2000-03-27 **Canada legislation privacy standards enforcement law regulation**

Government of Canada
http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_3/C-6_cover-E.html

In Canada, the Parliament continued consideration of Bill C-6, which Chris Wood described in correspondence published in POLITECH as follows: "a major piece of legislation that will extend Euro-style definitions and obligations of privacy protection to federally regulated businesses and to health providers in Canada. It will also enable e-filing of legal documents . . . and permit (with tech definitions to come) e-signatures. It will oblige companies collecting personal data to get informed consent for the collection and allow complaints about abuse of personal information to be submitted for investigation to Canada's Privacy Commissioner."

Category 38.7 *Other case law, legislation & regulation concerning individual privacy (not govt*

2000-04-17 **privacy standard proposal**

NewsScan

In April, Microsoft's Director of Corporate Privacy, Richard Purcell, announced that Microsoft would provide free tools to support P3P, the Platform for Privacy Preferences Project. P3P, under development by the World Wide Web Consortium (W3C), allows a browser to signal violation of minimum standards of privacy selected by a user.

Category 38.7 *Other case law, legislation & regulation concerning individual privacy (not govt*

2002-03-12 **privacy warnings disclaimers UK law legislation legal requirements monitoring surveillance workplace e-mail communicaitons**

RISKS 21 95ff

Michael Bacon noted in RISKS the logical difficulties of warnings such as the BBC's e-mail disclaimer, "Please note that the BBC monitors e-mails sent or received. Further communication will signify your consent to this." If you reply to indicate that you don't consent, have you consented nonetheless? Is there any way to avoid consent and monitoring?

Further discussion in RISKS explained that the disclaimer was required for compliance with UK privacy laws. J. F. Hitches explained, >That sort of statement will be seen more widely on messages coming from the UK because it is part of a requirement of an Act of Parliament called the "Regulation of Investigatory Powers Act". This is combined with a Statutory instrument called "The Telecommunications (Lawful Business Practice Regulations) 2000" .

The requirement is that monitoring may only be carried out "if the controller of the telecommunications system on which they are effected has made all reasonable efforts to inform potential users that interceptions may be made".<

Category 38.7 *Other case law, legislation & regulation concerning individual privacy (not govt*

2002-04-08 **privacy e-mail monitoring surveillance policies UK regulations international**

NewsScan

ROUTINE E-MAIL MONITORING BANNED IN UK OFFICES
A new code defining workers' privacy rights prohibits British employers from routinely monitoring e-mail and Internet usage in UK offices, even when there is "reason to believe" that they are personal and sent or received on a work computer during business hours. The code reflects the standards on monitoring that the Information Commission, the UK's data protection watchdog, says must be met in order to comply with the country's Data Protection Act. The commission has threatened to take action against companies that violate the new code. Industry groups have protested the code, with one human resources manager saying that "It's overly concerned with the employee's privacy it is still far too prescriptive and just not realistic." (Financial Times 7 Apr 2002)
http://news.ft.com/news/industries/internet&e-commerce

Category 38.7 *Other case law, legislation & regulation concerning individual privacy (not govt*

2002-06-18 **International UK Britain privacy e-mail cellular mobile telephone surveillance law law enforcement government agencies Internet eavesdropping**

FindLaw Download This 90

BRITAIN RETHINKS NET SURVEILLANCE
The British government said Tuesday it was withdrawing a heavily criticized plan to give more bureaucrats and local authorities the power to monitor private e-mail and mobile telephone records. Civil liberties groups and opposition politicians had condemned the proposed changes to the Regulation of Investigatory Powers Act, which they dubbed a "snoopers' charter." Under the act, passed by Parliament two years ago, the police, intelligence agencies, Customs and Excise and the Inland Revenue Service have the authority to demand records of e-mail, mobile phone and Internet traffic.
http://news.findlaw.com/ap/ht/1700/6-18-2002/20020618084502_01.html

UK Legal Resources
http://www.findlaw.com/12international/countries/uk/index.html

---

Category 38.7 *Other case law, legislation & regulation concerning individual privacy (not govt*

2002-08-06 **universal identifier citizen international privacy identity**

NewsScan

JAPANESE SAY THEY DON'T WANT TO BECOME NUMBERS
Japan's creation of a new citizen database has caused widespread concern that there has not been enough attention paid to privacy issues. Every citizen, starting at birth, will be assigned a unique 11-digit number. At present it will be used only to retrieve basic information (name, address, sex, and birth date), but many people think the system will be expanded to include other personal data. The new system has prompted widespread disobedience in the country, and half a dozen cities have refused to have any part of it. Nobuo Hoshino, mayor of Yokubunji, presiding over a "disconnecting ceremony," said: "Residents are sending us their views by e-mail, fax and various other ways, and almost all of them support us." One critic says that the project will grow and grow into "a bigger project, named 'E-Government,' that will have 16,000 administrative uses." (New York Times 5 Aug 2002)

Category 38.7 *Other case law, legislation & regulation concerning individual privacy (not govt*

2003-05-23 **privacy japan personal information databases e-mail**

NewsScan

NEW PRIVACY PROTECTION LAW IN JAPAN
In response to complaints that personal information about consumers is circulating without their permission in databases and e-mail communications, the Japanese parliament has passed legislation that will give individuals the right to obtain information collected about them and will put restrictions on both governmental and corporate entities who maintain such databases. Critics of the new legislation are worrying that Internet operators will be inundated with information requests from individuals, and privacy advocates are saying the legislation will impede freedom of speech. (APOnline/USA Today 23 May 2003)

Category 38.7 *Other case law, legislation & regulation concerning individual privacy (not govt*

2004-02-12 **privacy Australian Federal Privacy Commissioner warning**

NewsScan

AUSTRALIA WARNS ON PRIVACY

The Australian Federal Privacy Commissioner has warned companies about Web sites that don't adhere to security practices that protect the privacy of customers or visitors. The Commissioner said he was disappointed that businesses are still making fundamental errors and said there is no longer any excuse for not having privacy built into IT system re-design and or upgrades. (Office of the Federal Privacy Commissioner — News Release 12 Feb 2004)

Category 38.7 *Other case law, legislation & regulation concerning individual privacy (not govt*

2004-11-09 **New Zealand mobile phone voyeur crime photographs nudity prviacy legislation law**

NewsScan; http://theage.com.au/articles/2004/11/09/1099781374972.html

KIWIS COMBAT MOBILE PHONE VOYEURS

A New Zealand law being debated will impose a three-year jail sentence on mobile phone voyeurs who take intimate photographs of people without their knowledge. The law will make it an offense to surreptitiously film intimate situations involving nudity or partial nudity where people would have a reasonable expectation of privacy. (The Age 9 Nov 2004)

Category 38.7 *Other case law, legislation & regulation concerning individual privacy (not govt*

2005-02-02 **Greece ban e-mail snooping DPA workers employee privacy remote control law legislation**

NewsScan; http://australianit.news.com.au/articles/0

GREECE BANS E-MAIL SNOOPING

Greece's personal data watchdog has ordered companies not to violate employee privacy by snooping into their private e-mail. The independent Data Protection Authority (DPA), whose decisions are binding, has barred firms from collecting and processing information on workers' communications, including e-mail. The decision did not include fines. The authority acted on a complaint by the workers' union of an unnamed company, alleging the company remote-controlled employees' computers through virtual network control, specialized software that transmits the screen and keyboard and mouse clicks between two computers on a network. (The Australian 2 Feb 2005)

Category 38.7 *Other case law, legislation & regulation concerning individual privacy (not govt*

2005-02-22 **Singapore coordinated cybersecurity effort Government officials Internet law monitoring activity networks threats United States Australia**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=7698536

SINGAPORE PLANS COORDINATED CYBERSECURITY EFFORT

Government officials in Singapore announced that the country will spend $23 million over three years on a centralized program to increase cybersecurity. Singapore is one of the world's most wired countries, with a residential Internet access rate of 50-60 percent. The country also has some of the strictest regulation of computer systems, including a law that allows government monitoring of all computer activity. The law also allows preemptive action by the government to prevent anticipated cybersecurity threats. The new initiative, the National Cyber-Threat Monitoring Center, will monitor networks, looking for evidence of hacking or other cyber threats. The center, which is expected to be running by the second half of 2006, will work with similar centers in countries including the United States and Australia. Deputy Prime Minister Tony Tan, who is also Singapore's Coordinating Minister for Security and Defense, said, "Infocomm security is as important in protecting Singapore as is physical security at our borders."

38.8 Law enforcement & privacy rights

Category 38.8 *Law enforcement & privacy rights*

2000-03-09 **law enforcement privacy anonymity accountability investigation**

NewsScan, Washington Post http://www.washingtonpost.com/wp-srv/business/feed/a39970-2000mar9.htm

A new Justice Department report, titled "The Electronic Frontier: The Challenge of Unlawful Conduct on the Internet," . . . put privacy activists on alert: "What the report amounts to is a law enforcement Internet wish list of ways in which they can strip away privacy and free-speech protections in order to get at what they claim is this criminal element online," says an ACLU spokeswoman. The most controversial part of the report is a passage that terms anonymous e-mail a "thorny issue": "Given the complexity of this issue, balancing the need for accountability with the need for anonymity may be one of the greatest policy challenges in the years ahead." A White House deputy press secretary attempted to reassure ACLU officials, saying the administration understands the importance of privacy, including the positive role anonymity can play in reporting crimes and war atrocities. (Washington Post 9 Mar 2000)

Category 38.8 *Law enforcement & privacy rights*

2000-03-28 **fraud monitoring privacy securities industry government watchdog surveillance controversy**

NewsScan, Wall Street Journal
http://interactive.wsj.com/articles/SB954197317969930664.htm

An automatic surveillance system that would monitor for online securities fraud is running into trouble before it gets off the ground. The system, which would be operated by the Securities and Exchange Commission, would employ a Web "crawler" to survey public Web sites, message boards and chat groups, looking for key phrases like "get rich quick" and "free stock," and then analyze and index the information for later retrieval by SEC investigators bringing civil proceedings against scam perpetrators. In addition to sparking privacy concerns, the SEC may find itself up against giant Internet operators who consider their chat rooms to be proprietary. AOL, for instance, says it routinely bans outsiders from harvesting information from its chat rooms and message boards, in order to protect its customers' privacy. In addition, the SEC announcement comes at a time when the Federal Trade Commission and many states are working to increase privacy protections for citizens. Congress recently awarded the SEC an additional $12.5 million this year, primarily for Internet enforcement activities. (Wall Street Journal 28 Mar 2000)

Category 38.8 *Law enforcement & privacy rights*

2000-11-07 **privacy keystroke monitoring software forensic logging audit trail investigation**

NewsScan, TechWeb http://www.techweb.com/wire/story/TWB20001106S0012

Privacy advocates are concerned about the latest version of WinWhatWhere's Investigator software, which tracks all computer activity, including incoming and outgoing e-mail, both sides of chat room conversations, Instant Message dialogues, Web surfing and all passwords. That information can then be conveyed without the computer user's knowledge to a company's IT administrator, human relations personnel, or even a private investigator. "A lot of things this program does cause me great consternation," says WinWhatWhere president Richard Eaton, who developed the Investigator program. "If you tab across a password field, it picks all that up. I haven't decided if that is good or bad." "It's a complete dragnet," says Beth Givens, director of Privacy Rights Clearinghouse. "Certainly, employees must make personal communications throughout the day, .. and this particular software would pick up those conversations as well. It's certainly ruthless in its pursuit." WinWhatWhere's clients have included major airlines, government agencies, research laboratories, pharmaceutical companies, a large aerospace company, a leading business consulting firm and private individuals. (TechWeb News 6 Nov 2000)

Category 38.8 *Law enforcement & privacy rights*

2001-09-17 **wiretap constitution fourth amendment search seizure warrant changes proposals terrorists**

NewsScan

DISCUSSIONS OF PLANS TO CHANGE WIRETAP RULES [17 Sep 2001]
U.S. Attorney General John Ashcroft met with Congressional leaders Sunday to begin a review of possible changes in the laws governing use of wiretapping techniques to fight terrorism. House Minority Leader Richard Gephardt (D-Mo.) called the meeting constructive and Sen. Patrick Leahy (D-Vt.) said he would be open to revising the wiretapping laws to keep pace with technology change. At a press conference, Ashcroft said: "It's easier to investigate someone involved in illegal gambling schemes than it is to investigate someone involved in terrorism. Telephone surveillance has been limited historically to specific telephones, rather than to people." Pointing out that we have entered an era of disposable phones and Internet cafes, Ashcroft added, "it simply doesn't make sense to have the surveillance authority associated with the hardware or with the phone instead of with the person or the terrorist." Privacy advocates are urging lawmakers to proceed with caution. (San Jose Mercury News 17 Sep 2001)
http://www.siliconvalley.com/docs/hottopics/attack/005143.htm

---

Category 38.8 *Law enforcement & privacy rights*

2001-09-24 **biometric face recognition identification authentication terrorism airports scanning privacy surveillance**

NewsScan

FACE-RECOGNITION SYSTEM RECOMMENDED FOR AIRPORT SECURITY [24 Sep 2001]
A government committee appointed to review airport security procedures will recommend to Transportation Secretary Norman Y. Mineta the employment of face-recognition systems that create a digital map of a person's face and translate it into mathematical formulas claimed to be as uniquely distinguishing as a fingerprint. Privacy advocates like David Sobel regard this as a "potentially invasive technology" whose use will eventually expand to other purposes and endanger the civil liberties of ordinary people. The president of FaceIt Systems, one of the best-known manufacturers of face-recognition systems, says he shares privacy concerns and asserts that the answer is to have rules governing whose photos can be included in a database of suspects or criminals for comparison with mere passers-by. (Washington Post 24 Sep 2001)
http://www.washingtonpost.com/wp-dyn/articles/A14273-2001Sep23.html

---

Category 38.8 *Law enforcement & privacy rights*

2002-02-13 **surveillance cameras law enforcement police crime prevention anonymity public expectation privacy**

NewsScan

WASHINGTON POLICE EXPAND USE OF SURVEILLANCE TECHNOLOGY [13 Feb 2002]
Noting that people in the United Kingdom have "easily adapted" to pervasive public surveillance and that "there has not been an outcry about privacy there," Washington, D.C. police officials are busy expanding the public use of surveillance cameras. A police department spokesman says, "In the context of September 11, we have no choice but to accept the greater use of this technology." MIT emeritus sociology professor Gary T. Marx concedes that "almost all of the surveillance innovations are easily justifiable" but worries that "the major concern is: where is it leading?" (Wall Street Journal 13 Feb 2002)
http://online.wsj.com/ (sub req'd)

Category 38.8 *Law enforcement & privacy rights*

2002-09-05 **surveillance law enforcement police database suspects associates**

NewsScan

GUILT-BY-ASSOCIATION?
Law enforcement officials in Wilmington, Delaware are being criticized by privacy advocates for putting digital photos and other information into a database of associates of suspected drug dealers rounded up in rough neighborhoods. A Wilmington public defender calls it "guilt by association" and Barry Steinhardt of the ACLU charges: "They are stopping, searching and putting into a database photographs of people whose only crime is being in the wrong place at the wrong time. It's bad law enforcement, and it's bad for civil liberties." Police Chief Michael Szczerba's response is: "If you come into our city to take in a ballgame or dine at a restaurant or go to a theater, you likely won't know about these corner patrols. But if you come to sell drugs or drink alcohol on the corner or just be a general nuisance, you're going to see us." (USA Today 4 Sep 2002)
http://www.usatoday.com/tech/news/2002-09-04-wilmington

Category 38.8 *Law enforcement & privacy rights*

2002-11-20 **infrastructure protection homeland security legislation law bill privacy surveillance wiretaps court order probable cause**

NewsScan

HOMELAND SECURITY GIVES GOV'T NEW POWERS
Provisions of the legislation to create the U.S. Department of Homeland Security bill would allow Internet service providers to give the government more information about their subscribers and give police new Internet wiretap powers. The Electronic Privacy Information Center and other civil liberties groups say the bill's language lets Internet providers reveal subscriber information to any government officials, not just investigators. Another section of the bill gives U.S. authorities new power to trace e-mails and other Internet traffic during cyber attacks without first obtaining even court approval in the event hat there occurs "an immediate threat to national security" or an attack against a "protected computer." (AP/New York Times 20 Nov 2002)

Category 38.8 *Law enforcement & privacy rights*

2003-07-07 **FTC personal information Federal Trade Commission cyberspace business privacy policy**

NIPC/DHS

July 07, The Register — FTC calls privacy claims to account.

Most online businesses promise they'll protect customer data as if it were their own. Now the government is holding them to it. United States Federal Trade Commission has indicated its intention to actively pursue companies that obtain personal information by promising a level of security, and then not delivering it. Almost every company that does business in cyberspace has a security and privacy policy, typically buried at the bottom of a home page, under "legal notice" or "privacy policy." The FTC concluded that data that is collected under false pretenses is a "deceptive trade practice."

Category 38.8 *Law enforcement & privacy rights*

2003-11-08 **personal private sensitive information citizen database law enforcement technology**

RISKS; http://www.twincities.com/mld/pioneerpress/news/ politics/7154217.htm 23 3

Minnesota CriMNet shutdown

Steven Hauser wrote the following report in RISKS:

Minnesota has a large database of millions of records of police activity and incident data compiled on its citizens. The data is not owned by the government but an extra-legal private entitity, the Minnesota Chiefs of Police Association. This alone is scary, no recourse for inaccuracy, no way to assure data is not leaked or used for political or commercial purposes. News articles show it may have been used in political demonstrations to target citizens. Good "death squad" database. It was also hacked by an unidentified whistleblower who gave State Representative Mary Liz Holberg supposedly private data about herself. The cops are pressuring the Representative to turn over the whistleblower for prosecution, but the Representative has not yet squealed. This incident caused the system to be shut down. Google search on CriMNet or MJNO to get more articles. [The Internetted system is of course thought to be secure because it is password protected! There's a LONG article by Patrick Howe. PGN] http://www.twincities.com/mld/pioneerpress/news/ politics/7154217.htm

---

Category 38.8 *Law enforcement & privacy rights*

2003-11-13 **privacy US American MATRIX Multistate Anti-Terrorist Information Exchange Florida terrorism anti-terrorism**

RISKS; http://www.usatoday.com/news/opinion/editorials/2003-11-10-campbell_x.htm 23 3

High-tech microscopes expose Americans' private lives

In USA Today, Don Campbell writes about a new threat to Americans' privacy: MATRIX, or Multistate Anti-Terrorist Information Exchange. This 20-billion-record database is said to be "the largest database on the planet" by its creator Seisint. With $12 million in federal funding, Seisint is collaborating with the Florida Department of Law Enforcement (FDLE) "with the objective of compiling an electronic dossier on every citizen in the nation." In addition to being used as an anti-terrorism tool, MATRIX is said to become useful "when it comes to catching kidnappers and child molesters."

Category 38.8 *Law enforcement & privacy rights*

2003-11-13 **Federal Bureau of Investigation FBI financial records judge jurisdiction warrant security terrorism anti-terrorism**

RISKS; http://www.nytimes.com/2003/11/12/politics/12RECO.html 23 3

FBI's reach into records is set to grow

Monty Solomon observes that the House and Senate have approved the FBI's power to get access to financial records, without a judge's approval, from anyone ranging from security brokers to pawnbrokers--any "institution doing cash transactions with "a high degree of usefulness in criminal, tax or regulatory matters.""

Category 38.8 *Law enforcement & privacy rights*

2003-12-23 **online music probe Pressplay MusicNet Roxio EMI digital services**

NewsScan

NO HARM, NO FOUL: U.S. DROPS ONLINE MUSIC PROBE
The U.S. Justice Department has closed its investigation of online music ventures Pressplay and MusicNet because investigators came to the conclusion that the two services have not actually hurt consumers. Pressplay is owned by Roxio Inc., and MusicNet is owned jointly by subsidiaries of Time Warner Inc., Bertelsmann AG and EMI Group Plc. Antitrust chief Hewitt Pate said: "None of the several theories of competitive harm that the Division considered were ultimately supported by the facts. Consumers now have available to them an increasing variety of authorized outlets from which they can purchase digital music, and consumers are using those services in growing numbers." (Reuters/Washington Post 23 Dec 2003)

Category 38.8 *Law enforcement & privacy rights*

2004-01-22 **ACLU states' crime database privacy threat**

NewsBits; http://www.usatoday.com/tech/news/2004-01-22-aclu-vs-matrix_x.htm
http://www.chron.com/cs/CDA/ssistory.mpl/business/2365475

ACLU: States' crime database a privacy threat

A seven-state crime database launched with $12 million in federal funds is a more powerful threat to privacy than its organizers acknowledge, theAmerican Civil Liberties Union alleged Wednesday after obtaining documents relating to the program. The law enforcement officials and private database company behind the Multistate Anti-Terrorism Information Exchange, or Matrix, contend it is merely an investigative tool that helps police quickly gather already- available information on suspects.

Category 38.8 *Law enforcement & privacy rights*

2004-02-11 **VoIP wiretaps privacy federal US government Bush administration CALEA**

DHS IAIP Daily; http://news.com.com/2100−7352_3−
5157282.html?tag=nefd_top

February 11, CNET News.com — Feds step up push to wiretap VoIP calls.

The Bush administration plans to ask the Federal Communications Commission to order Net telephony providers to comply with a law that would permit police to wiretap conversations carried over the Internet. In a series of letters made public Tuesday, February 11, the Justice Department said it is "currently drafting a request" that would invoke the 1994 Communications Assistance for Law Enforcement Act (CALEA). That law requires telecommunications carriers to rewire their networks to government specifications to provide police with guaranteed access for wiretaps. It is debatable whether CALEA's decade-old definition of "telecommunications carrier," crafted long before the Internet era, applies to Voice over Internet Protocol (VoIP) providers. If the FCC rules that CALEA's definitions are not a close enough fit for the fast-growing and somewhat amorphous VoIP sector, then the Bush administration could ask Congress to rewrite the law. Until earlier this month, the FBI had tried to block the FCC from considering VoIP's regulatory structure until the wiretap issue was resolved. But last week, the two agencies said they had reached an agreement allowing a vote on VoIP regulations to take place on Thursday.

Category 38.8 *Law enforcement & privacy rights*

2004-02-12 **privacy incident Australia sensitive documents files unauthorized access**

NewsScan

POLICE FACE SACK IN ONGOING PRIVACY INCIDENTS

Australian Police in Victoria are facing an embarrassing new privacy scandal after an internal audit found fresh evidence of improper access to confidential computer files. The audit has found up to 35 police have used the police Law Enforcement Assistance Program (LEAP) computer to check information on a security guard charged with manslaughter over the death of former Test cricketer David Hookes. All police who have accessed the files, other than homicide squad police investigating the death, are expected to be asked by ethical standards department police to justify their actions. Police who cannot give legitimate reasons face the sack. This incident comes in the wake of an investigation in 2003 into allegations that the files of 32 current and former Victorian Members of Parliament have been accessed without legitimate reason.

Category 38.8 *Law enforcement & privacy rights*

2004-05-21 **surveillance database integration crime terrorism homeland security**

http://query.nytimes.com/gst/abstract.html?res=F60A17F63A5B0C728EDDAC08 94DC404482

New details about criminal information project known as Matrix, which combines state records culled by database company Seisint to give investigators fast access to information on crime and terrorism suspects, raise questions about its potential power; records show Matrix gave federal and Florida authorities names of 120,000 people who showed statistical likelihood of being terrorists, before program actually began, resulting in investigations and arrests; objections were raised because system includes information on innocent people as well as known criminals; officials involved with Matrix say statistical method was removed from final product due to privacy concerns (M)

Category 38.8 *Law enforcement & privacy rights*

2004-08-04 **Internet Net telephone tapping voice-over-IP VoIP law enforcement FBI DEA DoJ Federal Communications Commission FCC**

DHS IAIP Daily;
http://www.reuters.com/newsArticle.jhtml?type=internetNews&s toryID=5873014

August 04, Reuters — FCC: Net phone calls must be able to be tapped.

Internet phone carriers such as Vonage should set up their systems so U.S. law enforcers can monitor suspicious calls, the Federal Communications Commission (FCC) tentatively ruled on 12 Wednesday, July 4. By a vote of 5-0, the FCC said "voice over Internet protocol," or VoIP, providers should be subject to the 1994 Communications Assistance for Law Enforcement Act, which ensures that law enforcers will be able to keep up with changing communications technologies. VoIP service is likely to replace much traditional phone service over the coming years, the commission said. The Justice Department, FBI and Drug Enforcement Administration have argued that they must be able to monitor suspicious calls no matter how they are made. Technology advocates have worried that the fast-growing service, which promises to slash costs by routing phone calls over the Internet, could be harmed by excessive regulation. The ruling does not affect other regulatory questions surrounding VoIP service, such as how it should be taxed, FCC Chairman Michael Powell said.

Category 38.8 *Law enforcement & privacy rights*

2005-01-18 **Internet broadcast court prediction online video privacy public broadcast trials**

NewsScan; http://www.usatoday.com/tech/news/2005-01-18-sentenced-online_x.htm

WILD WEB JUSTICE

Ohio trial court judge James L. Kimbler has set up a personal Sony digital camcorder in his courtroom and using it to post online video of people being sentenced for robbery, rape and other crimes. Kimbler says, "It's all public record anyway. If the general public and law students know what we do it increases their understanding." Lloyd Snyder, a professor of legal ethics, predicts: "This is coming. With 'Court TV' available, people are getting used to having things like this out there, and it's also entertainment. It is the right of the defendant to be tried in the open. There is no correlative right for a defendant to have a private trial." (AP/USA Today 18 Jan 2005)

Category 38.8 *Law enforcement & privacy rights*

2005-01-19 **Carnivore dead Congress FBI surveillance federal officials electronic communications privacy software**

EDUPAGE; http://news.com.com/2100-1028_3-5541483.html

CARNIVORE IS DEAD

According to two recent reports to Congress, the FBI has put an end to its electronic surveillance tool, known as Carnivore. Despite claims from federal officials that they need expanded access to electronic communications, the system was widely criticized by civil liberties groups as being overly invasive and for not respecting individuals' privacy. The reports, which the Electronic Privacy Information Center obtained under the Freedom of Information Act, note that the FBI did not use the system for fiscal years 2002 and 2003 and instead used commercially available monitoring software. According to the reports, the FBI engaged in court-ordered Internet surveillance 13 times during those years.

Category 38.8 *Law enforcement & privacy rights*

2005-02-25 **homeland security privacy committee bias corporate influence representation protests**

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/10991077.htm

PRIVACY ISSUES AND THE DEPARTMENT OF HOMELAND SECURITY

Privacy advocates are saying that a committee set up to advise the Homeland Security Department on privacy issues is skewed too heavily toward corporations such as Intel, Computer Associates, IBM, and Oracle. George Washington University Law School professor and privacy expert Daniel Solove says, "The strong privacy advocacy community seems underrepresented on this list." But Homeland Security Chief Privacy Officer Nuala O'Connor Kelly says the committee represents a cross-section of viewpoints, including people "who have gone to companies that have had challenges and tried to fix them." She pointed to several privacy advocates on the board: Tara Lemmey, former executive director of the Electronic Frontier Foundation; Lance Hoffman, a George Washington University professor; and James Harper, editor of Privacilla.org and a strong critic of government surveillance. (AP/San Jose Mercury News 25 Feb 2005)

Category 38.8 *Law enforcement & privacy rights*

2005-07-22 **GAO TSA privacy violations Secure Flight program terrorism anti-terrorism**

EDUPAGE; http://www.fcw.com/article89670-07-22-05-Web

GAO SAYS TSA CLEANING UP SECURE FLIGHT

According to the Government Accountability Office (GAO), the Transportation Security Administration (TSA) has adequately addressed concerns raised by the GAO over privacy violations in the Secure Flight program. The program is designed to safeguard the nation's air travel system by identifying suspected terrorists and preventing them from boarding planes. During a test of the program, TSA collected commercial information on air passengers, violating its privacy policy, according to the GAO. TSA used the commercial data in conjunction with passenger information to increase the reliability of the Secure Flight system, but the result was that air passengers were unable to know what information about them was being collected and how it was being used.
In a report, the GAO said that after being notified of the problems, TSA acted immediately to address the issues raised. Aside from not using commercial data in the Secure Flight program, TSA also said its chief privacy officer and general counsel would ensure that activities related to the Secure Flight program would be explicitly detailed in its privacy notices. Federal Computer Week, 22 July 2005

Category 38.8 *Law enforcement & privacy rights*

2005-10-06 **privacy concerns USA PATRIOT Act American Library Association ALA brief**

EDUPAGE; http://chronicle.com/daily/2005/10/2005100601t.htm

MORE HINTS POINT TO IDENTITY OF CONNECTICUT LIBRARY

The American Library Association (ALA) has filed a court brief in the ongoing wrangling over a provision of the USA PATRIOT Act that prevents organizations under investigation from publicly speaking about the investigation. Under the terms of that law, federal authorities had sought information from a Connecticut library group, which has been forced to keep its identity secret. An article in the New York Times, though, said the Library Connection Inc., of Windsor, Conn., is the probable target of the investigation. According to the ALA's brief, because the Library Connection has refused to confirm or deny the story in the Times, it is clear that the speculation is correct. Further, because the identity has been guessed, keeping the group from speaking about the investigation is pointless, according to the brief. The brief states: "If the reporting is accurate, the information the government seeks to suppress has already been revealed, and the gag order serves no interest but that of silencing a citizen." Last month a judge ordered that the gag order be lifted, but an appeals court has reimposed the gag order pending its review of the case. Chronicle of Higher Education, 6 October 2005 (sub. req'd)

Category 38.8 *Law enforcement & privacy rights*

2005-10-19 **Sleuths tacking code color printers serial EFF San Franisco Secret Service**

DHS IAIP Daily; http://www.washingtonpost.com/wp−dyn/content/article/2005/10/18/AR2005101801663.html?referrer=email

SLEUTHS CRACK TRACKING CODE DISCOVERED IN COLOR PRINTERS

An invisible bar code of sorts that contains the serial number of the printer as well as the date and time a document was printed has been cracked by the Electronic Frontier Foundation (EFF), a San Francisco consumer privacy group. According to U.S. Secret Service spokesperson Eric Zahren, "It's strictly a countermeasure to prevent illegal activity specific to counterfeiting. It's to protect our currency and to protect people's hard-earned money. "

Category 38.8 *Law enforcement & privacy rights*

2005-10-23 **Colleges upgrade Federal Communications Commission Internet networks law monitor Internet Philadelphia San Francisco**

DHS IAIP Daily; http://www.nytimes.com/2005/10/23/technology/23college.html

COLLEGES PROTEST CALL TO UPGRADE ONLINE SYSTEMS

The Federal Communications Commission is requiring hundreds of universities, online communications companies and cities to overhaul their Internet computer networks to make it easier for law enforcement authorities to monitor e-mail and other online communications. This order extends the provisions of a 1994 wiretap law to universities, libraries, airports providing wireless service and commercial Internet access providers and municipalities that provide Internet access to residents, such as Philadelphia and San Francisco. The action, which the government says is intended to help catch terrorists and other criminals, has unleashed protests and the threat of lawsuits from universities, which argue that it will cost them at least $7 billion while doing little to apprehend lawbreakers. The Justice Department requested the order last year, saying that new technologies like telephone service over the Internet were endangering law enforcement's ability to conduct wiretaps "in their fight against criminals, terrorists and spies."

38.9 Medical information & HIPAA

Category 38.9 *Medical information & HIPAA*

1997-08-01 **health privacy confidentiality medical records**

AP

U.S. Health and Human Services Secretary Donna Shalala said that a national system is needed to replace a patchwork of state laws governing privacy of health records. Speaking at the National Press Club, Shalala recommended that Congress prohibit use of personal information for anything other than health care and punish those who misuse it; require data keepers to keep the information secure; allow consumers to see what is in their health records; and give them a way to change incorrect data. she added, however, that privacy rights cannot be absolute; the public interest (e.g., public health, research, and fraud investigations) may require access to health data without permission.

Category 38.9 *Medical information & HIPAA*

1997-10-28 **health privacy medical law hospital records patient**

AP

The US Senate's Labor and Human Resources Committee heard in October from proponents of strict laws to restrict the use of medical information to medical applications. Legislation expected to be introduced in early 1998 by Sen. Robert Bennett (R-Utah) would provide federal protection for such records. Sen. Patrick Leahy (D-VT) was working on even stricter protections focusing in particular on access to medical records by law enforcement officials.

Category 38.9 *Medical information & HIPAA*

1999-10-12 **privacy medical information identification authentication I&A doctors Internet remote telemedicine HIPAA**

EDUPAGE; Wall Street Journal

INTEL AND AMA FORM SERVICE TO IMPROVE SECURITY OF ONLINE MEDICAL INFORMATION
Intel and the American Medical Association (AMA) are teaming to offer a service that will boost the online security of medical data. The service, which becomes available in the first quarter of 2000, will use "digital credentials" to prove the identities of doctors who are sending and accessing medical information over the Internet. The service launches Intel's "Internet Authentication Services" initiative, which permits the identification of parties at both ends of online transactions. The digital credential service, which is portable, is a big improvement over digital certificate security measures, according to Intel and the AMA. The use of the Internet for medical transactions will not reach mainstream levels unless security is improved. "This is important if the use of the Internet for health care is to go to the next level," says Jim Klein of the Gartner Group. (Wall Street Journal 10/12/99)

Category 38.9 *Medical information & HIPAA*

2003-10-06 **HIPAA medical information security privacy compliance regulation FBI**

NIPC/DHS

Contingency Plan For HIPAA Oct. 6, 2003

Message from Feds to all health-care companies that won't meet the Oct. 16 deadline to have their electronic transactions compliant with the Health Insurance Portability and Accountability Act: Stop sweating. You'll still get paid from Medicare and Medicaid, as long as you're making a good-faith effort to become compliant. That's the word from the Centers for Medicare and Medicaid Services, which has issued a contingency plan for the "thousands" of health providers it expects won't meet HIPAA's deadline. Among processes covered by HIPAA's regulations are claim-status tracking, remittance, and coverage eligibility; the most significant transaction is claims processing for Medicare and Medicaid patients. CMS had said Medicare and Medicaid wouldn't pay claims sent in electronic formats not compliant with HIPAA standards after Oct. 16. However, as of last week, fewer than 20% of claims being electronically sent to CMS were HIPAA compliant.

Category 38.9 Medical information & HIPAA

2003-12-15 **HIPAA medical information security privacy cost compliance**

http://www.informationweek.com/news/showArticle.jhtml?articleID=16700402

COMPLIANCE DRIVES HEALTH-CARE CHANGES

"Health-care costs are on the rise, but why? As companies in the health sector struggle to comply with stringent government regulations such as the Health Insurance Portability and Accountability Act, related costs are being passed along to policyholders. This is necessary because investment in personnel, IT systems, and security are chipping away at profits.

Hospitals and doctors continue to rely on inefficient paper trails to manage patient records. As compliance with HIPAA takes hold, many find it necessary to move to electronic operations. HIPAA's guidelines regarding information sharing, patient privacy, and information security are presenting other changes, too."

[Excerpt from article by Lisa Smith, Managing Editor, Research, CMP]

Category 38.9 Medical information & HIPAA

2004-01-04 **eICU hospital monitoring remote medical monitoring treatment examination**

NewsScan; http://www.latimes.com/technology/ats-ap_technology12jan04

'ENHANCED INTENSIVE CARE': IF YOU NEED IT YOU'LL WANT IT

New technology known as eICU ("Enhanced Intensive Care") lets physicians miles away from their patents manage health care via cameras and banks of computer screens. Developed by Baltimore-based VISICU Inc., the technology is already in use at least 18 hospital systems nationwide. Whereas traditional health care systems rely on nurses to notice a problem with a patient and relay the information to a doctor, eICU informs the doctor directly. The doctor can check the patient's ventilator, intravenous medication and anything else in the patient's room, and one physician notes: "The camera is such that I can count eyelashes." (AP/Los Angeles Times 4 Jan 2004)

Category 38.9 Medical information & HIPAA

2004-01-27 **HIPAA medical information security privacy WebMD delay**

NIPC/DHS

AMA Complains WebMD Mishandling HIPAA Claims Jan. 27, 2004

Problems with WebMD's handling of claims leads to hundreds of thousands of dollars worth of delayed and denied payments, and caused some doctors to revert to paper.

The American Medical Association has sent a letter to WebMD Corp.,likely the medical industry's most powerful player in electronic insurance-claims processing, complaining that it has mishandled claims submitted by doctors resulting in "hundreds of thousands of dollars" in delayed and denied payments, InformationWeek has learned. WebMD acknowledges there have been problems, but attributes them to implementing a new process. According to the letter dated Jan. 8, sent to WebMD CEO Roger Holstein and signed by the AMA and seven other medical associations, the frequency of physicians' complaints about WebMD has risen since the Health Insurance Portability and Accountability Act standards went into effect Oct. 16.In addition to setting standards regarding the privacy of patient information, HIPPA is intended to simplify and encourage electronic claims processing. But WebMD's efforts at HIPAA compliance appear to be having the opposite effect, according to the letter, a copy of which was obtained by InformationWeek. WebMD attributes any problems to the early stages of a new process.

Category 38.9 *Medical information & HIPAA*

2004-01-29 **HIPAA medical information security privacy WebMD delay**

NIPC/DHS

Doctors Dependent on WebMD Despite Alleged Problems Jan. 29, 2004

Because of complexities with claims-processing and new requirements under HIPAA, doctors rely on WebMD and other clearinghouses to handle the work. The maturing field of Web-services technologies has the potential to let physicians' offices file medical claims directly to insurance companies using inexpensive Internet connections, eliminating the need for claims-processing clearinghouses. Yet some are convinced physicians will continue to depend on clearinghouses such as WebMD Corp., the biggest in the industry, because of the complex nature of electronic-claims processing. Doctors' offices "could use Web services" such as XML documents and the Simple Object Access Protocol to directly upload claims to insurance companies, says David Wroten, assistant executive VP of the Arkansas Medical Society. "But when a doctor's office tries, it immediately runs into little problems with different browsers," says Wroten, as Netscape Navigator and Microsoft Explorer each present the form differently. Rather than immerse themselves in technical details, offices rely on a clearinghouse to resolve problems and format the claim correctly. The majority of urban doctors' offices were using a clearinghouse before HIPAA was implemented Oct. 16. and have been reluctant to change since the new regulations went into effect, he says. But complaints about WebMD's inaccurate processing or lost claims were voiced in a Jan. 8 letter from the American Medical Association to WebMD CEO Roger Holstein. The letter said "thousands or hundreds of thousands of dollars" in delayed payments to some offices have resulted from mishandled claims.

Category 38.9 *Medical information & HIPAA*

2004-02-09 **HIPAA medical information security privacy compliance regulation insurance cost cut**

NIPC/DHS

New Claim Game Feb. 9, 2004

Insurance companies want doctors to bypass clearinghouses and submit claims directly. The move could cut costs and complexities from the system.

On March 1, Harvard Pilgrim Health Care Inc. will take a drastic step to realize the savings intended by the federally mandated Health Insurance Portability and Accountability Act, which went into effect four months ago. The insurance company will no longer pay "click charges" of about 35 cents per transaction to WebMD Corp., the industry's largest medical-claims-processing clearinghouse, which handles a third of the 10 million claims Harvard Pilgrim pays out every year.

In addition to establishing rules to ensure patient privacy, HIPAA set standards for the electronic exchange of information that in theory should ease connection problems between health-care providers and insurance companies, while reducing costs associated with manually processing paperwork.

Do clearinghouses provide a valuable service or merely add unnecessary costs? The industry has long depended on them to aggregate claims coming from physicians' offices and send them in batches to the correct payers, at a cost of about $414 million a year to insurance companies, according to Forrester Research. As the largest claims processor, WebMD is stumbling in its efforts to convince the industry that its clearinghouse adds value.

HIPAA undoubtedly is creating complexities in health care. For one, it specifies different formats for different functions, such as eligibility inquiries versus remittance responses. Claims also must be compliant in their content, which creates problems when a physician uses an old or rudimentary practice-management system for patient records and billing information. Fixing that can require intensive technical work between the physician's office and the clearinghouse and between the clearinghouse and the claim payer. But companies like Harvard Pilgrim don't see any savings being realized if WebMD becomes that dictator. Clearinghouses only add costs, Grose says. "It's a philosophical issue. WebMD just happens to be the one we disagree with most."

Category 38.9 *Medical information & HIPAA*

2004-02-20 **privacy medical records e-mail STDs partners notified**

NewsScan

YOU'VE GOT…

Public health officials in Los Angeles County in California are using e-mail to notify the partners of people who had been diagnosed with STDs. The director of programs at the AIDS Project Los Angeles says: "My reaction is, bravo. I think this is really appropriate, given the role the Internet seems to play in the transmission of the diseases. I think this is a good use of technology that the target population uses and understands. This program was just initiated in San Francisco a couple of months ago. It's real innovative." (Los Angeles Daily News 20 Feb 2004)

Category 38.9 *Medical information & HIPAA*

2004-12-07 **medical records Massachusetts eHealth pilot project doctors patients**

NewsScan; http://www.latimes.com/technology/ats-ap_technology14dec07

MEDICAL RECORDS-SHARING IN MASSACHUSETTS

If a new Massachusetts "eHealth" pilot project is successful, physicians in that state will be able to access patients' records from any hospital or clinic by computer. Gov. Mitt Romney says that switching from paper records to easily shared electronic records could save the state millions of dollars while improving patient safety and quality of care. He has given assurances that the system will have strict controls to allow patients to control who sees their records. (AP/Los Angeles times 7 Dec 2004)

Category 38.9 *Medical information & HIPAA*

2004-12-20 **medical automated medication errors quality assurance bugs flaws training people human factors**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A15178-2004Dec20.html

AUTOMATED MEDICATION WORSE THAN THE DISEASE?

A report from U.S. Pharmacopeia (USP), a nonprofit group that sets standards for the drug industry, says that as more hospitals have implemented automated systems for administering drugs the number of errors associated with them has risen. USP vice president Diane Cousins says, "It would seem logical that applying computer technology to the medication use process would have a significant positive impact in preventing medication errors. Yet, depending on the computer's design or user competence, new points of potential errors can emerge." Kenneth Kizer of the National Quality Forum agrees with Cousins: "Technology offers great opportunity to reduce errors, but it's not a panacea. You can't just throw a computerized system in and expect that everything's fixed. It has to be done right. The technology is only as good as the people who use it." (Washington Post 20 Dec 2004)

Category 38.9 *Medical information & HIPAA*

2005-01-19 **national health medical network recommendations policy financing standards interoperability**

NewsScan; http://www.nytimes.com/2005/01/19/technology/19health.html

ROAD MAP LAYS OUT THE ROUTE TO DIGITAL HEALTH RECORDS

A group of 13 health and information technology organizations have presented the Bush administration with recommendations for a "national road map" for development of a national health information network. The 54-page document borrows heavily from the technical and policy approach of the Internet, suggesting that the federal government limit its involvement to initial financing and endorsement of basic technical standards. A separate "standards and policy entity" would then take over management of the proposed system. The report concluded that a national health network should not include a central database of patient records, nor should it require people to carry "health ID cards." Patients would control their own records, and the optimal design of the network would use open, standard technology for maximum interoperability of disparate systems. Many medical groups have begun investing in creating local networks that connect electronic patient records and the study warns that failure to move swiftly to establish open communications standards between these networks may result in a large savings opportunity lost. "If we're not careful, we'll have little islands of excellence that don't talk to each other," says Jan Walker, lead author of a separate article on the subject recently published in Health Affairs. (New York Times 19 Jan 2005)

Category 38.9 *Medical information & HIPAA*

2005-01-26 **national health network medical companies nonproprietary standards software plans proposal project**

NewsScan; http://www.nytimes.com/2005/01/26/technology/26health.html

PREPARING FOR A DIGITAL HEALTH NETWORK

Eight leading high-tech companies -- IBM, Microsoft, Intel, Oracle, Accenture, Cisco, Hewlett-Packard and Computer Sciences -- have agreed to adopt open, nonproprietary technology standards as the software building blocks for a national health information network, which the Bush administration hopes will improve care and reduce costs by moving to a digital system for handling patient records, clinical research, claims and payments. IBM executive Neil de Crescenzo says, "The challenge is to turn a call for change in the nation's health care system into actual change. We got together to try to speak with one voice to the federal government and other stakeholders, and say this is an approach we will all stand behind." (New York Times 26 Jan 2005)

Category 38.9 *Medical information & HIPAA*

2005-02-04 **Canada privacy medical outsource USAPATRIOT Act data mining leakage confidentiality ChoicePoint immigration customers employees activists**

NewsScan; http://www.wired.com/news/privacy/0

CANADIANS UP IN ARMS OVER HEALTH INFO PRIVACY

Activists with the British Columbia Civil Liberties Association say that plans to outsource storage of Canadian citizens' health records to a U.S. company places that sensitive information in jeopardy. They fear that putting the data in the hands of Maximus Can, a subsidiary of U.S.-based Maximus, could lead to data-mining exercises, such as those that involved passenger records from JetBlue and other airlines. Or, as in the case with data on Latin American citizens purchased in 2003 by ChoicePoint that was then sold to U.S. immigration authorities, it could be used to prevent British Columbians with serious health issues, such as AIDS, from entering the U.S. Under the U.S.A.P.A.T.R.I.O.T. Act, U.S. companies can be forced to reveal information while prohibited from telling customers or employees that it has been shared. Activists fear that reach will extend to subsidiaries of U.S. companies operating outside its borders. "There really isn't a database of cross-referenced information that you could consider to be more personal… The potential for this information to be used and misused is great," says Michael Vonn, policy director for the British Columbia Civil Liberties Association. (Wired.com 4 Feb 2005)

Category 38.9 *Medical information & HIPAA*

2005-03-10 **medical hospital informatics security quality assurance QA errors iatrogenic illness drug dosage prescriptions flaws bugs user confusion medications patients doctors nurses computers**

RISKS; http://tinyurl.com/9dwev; http://tinyurl.com/d7qsp 23 78

DRUG-ERROR RISK AT HOSPITALS TIED TO COMPUTERS

Monty Solomon and Peter Neumann summarized a serious problem in hospitals:

Hospital computer systems widely touted as the best way to eliminate dangerous medication mix-ups can actually introduce many errors, according to the most comprehensive study of hazards of the new technology. The researchers, who shadowed doctors and nurses in the University of Pennsylvania hospital for four months, found that some patients were put at risk of getting double doses of their medicine while others get none at all. 22 types of mistakes were identified, such as failing to stop old medications when adding new ones or forgetting that the computer automatically suspended medications after surgery. The findings underscore the complexity of improving safety in US hospitals, where the Institute of Medicine estimates that errors of all kinds kill 44,000 to 98,000 patients a year.

A related story recounts similar findings from a different study.

HOSPITAL COMPUTERS MAKE THINGS WORSE

Reports over the past few years of increasing numbers of patient injuries and deaths due to medical errors sent hospital administrators scrambling for computerized solutions. But two new studies suggest that, in many cases, these high-tech systems have left doctors and nurses increasingly frustrated while providing little evidence of real benefit to patients. In fact, one widely used system actually helped foster medication errors, researchers found. See the 9 Mar 2005 issue of the Journal of the American Medical Association.

Sympatico News, Hospital Computers Fail to Deliver: study finds they facilitated errors

---

Category 38.9 *Medical information & HIPAA*

2005-03-11 **medical hospital informatics security quality assurance QA errors iatrogenic illness drug dosage prescriptions flaws bugs user confusion medications patients doctors nurses computers**

RISKS 23 79

COMPUTERIZED PHYSICIAN ORDER ENTRY SYSTEMS STILL TROUBLESOME

Charles J. Wertz provided abstracts for two interesting articles:

The 9 Mar 2005 issue of the *Journal of the American Medical Association* contains two articles and an editorial that should be of interest to Risks readers.

ROLE OF COMPUTERIZED ORDER ENTRY SYSTEMS IN FACILITATING MEDICATION ERRORS discusses a variety of issues including poor interface design requiring a physician to look at as many as 20 screens to see all the information about a patient, misleading and frequently misinterpreted dosage information, dosage change requires adding the new and deleting the old, poor integration of multiple systems, poor handling of discontinuation and resumption of medications, loss of orders and others. This article appears to be the result of a well done comprehensive study at one specific hospital.

The Editorial, COMPUTER TECHNOLOGY AND CLINICAL WORK: STILL WAITING FOR GODOT makes a number of good points such as, "The misleading theory about technology is that technical problems require technical solutions; ie, a narrowly technical view that leads to a focus on optimizing the technology. In contrast, a more useful approach views the clinical workplace as a complex system in which technologies, people, and organizational routines dynamically interact." Anyone interested in systems design will find this interesting.

The other Article, EFFECTS OF COMPUTERIZED CLINICAL DECISION SUPPORT SYSTEMS ON PRACTITIONER PERFORMANCE AND PATIENT OUTCOMES: A SYSTEMATIC REVIEW provides a comprehensive review of the topic.

Category 38.9 *Medical information & HIPAA*

2005-03-12 **medical hospital informatics security quality assurance QA errors iatrogenic illness drug dosage prescriptions flaws bugs user confusion medications patients doctors nurses computers blame game shifting responsibility administrators management**

RISKS 23 79

COMPUTERS IN HOSPITALS BLAMED FOR HUMAN ERROR

In response to several articles about how awful biomedical informatics systems are, Bob Morrell retorted that administrators readily blame computers for errors committed by their staff:

>Recent coverage of a JAMA article on the patient errors (cited by R. Akerman in RISKS-23.78) caused by computers will likely be cited by those who resist the movement towards an electronic medical record. This despite the fact that all acknowledge that the current mixed state of computerized and non-computerized medical systems is abysmal. My perspective on this is that we often miss the core truth of most medical mistakes: they are caused by humans, not computers. In the 1990's I developed several programs designed to find medical mistakes. As such, I spent a lot of time analyzing mistakes, and dealing with defensive reactions by physicians and nurses to the mistakes found. The most common mistake, at its core, was raw human misunderstanding: conceptual misunderstanding leading to misinterpretation of medical data (surgeons who thought the higher the bacterial MIC number, the better the antibiotic, when the reverse is true, and therefore put the patient on an antibiotic guaranteed to be ineffective). A close second was communication failures, where a key report was pocketed, lost or otherwise not communicated to others who would understand its importance.

However, in all these cases, the typical hospital political hierarchy sought to turn each of these medical errors into a computer error, lest a human (particularly a Doctor human) be found at fault. While I was grumpy about this at first, I soon realized that there was at least some truth in it, in that more easily understood medical reports, that highlighted and provided some interpretation to key information, and were more widely distributed were in fact improvements worth making to medical systems, and certainly would prevent far more errors than my mistake finding programs would ever find. The problem was however, that as the concept of the electronic medical record began taking shape, resistance to it often cited the end of incident analysis that blamed the computer, rather than the physician or nurse who was primarily at fault. The JAMA cases certainly sound like real problems with the human/computer interface, but they sound suspiciously like the final reports we used to end up on real mistakes made by real humans.

The medical environment is extremely complex, understaffed and wrought with automated and semi automated systems that all can fail or conflict whether they are computerized or not. I routinely saw problems with continuation of standing order dosing long before those standing orders were computerized. Blaming the computer misses the point, even if it does point out how the computer system could be made better.

The risk is one I often see in The Risks Digest: problems with computerized systems seem to get more attention than the usually much greater problems in the existing non-computerized systems.<

Category 38.9 *Medical information & HIPAA*

2005-11-20 **United Kingdom UK data sharing privacy concerns medical research**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4455306.stm

BRITISH ORGANIZATION URGES DATA SHARING

In the United Kingdom, a report from the Council for Science and Technology calls on the government to share information among its various agencies while keeping a close eye on privacy concerns. Due to the sheer amount of data that the government collects and stores, pooling that data can facilitate improved public services, as happens already with health-related data. Mark Walport, head of medical charity at the Wellcome Trust and author of the report, said such data sharing in medical research has uncovered links between health problems and social factors and can allow researchers to closely track the effectiveness of various treatments over time. Walport suggested that similar benefits could be derived from governmental sharing of other types of data, which is currently not being used effectively. Walport said he believes that with adequate creative thinking, the government could see significant benefits from sharing data while ensuring protection for personal privacy. BBC, 20 November 2005

Category 38.9 Medical information & HIPAA

2005-12-02 **medical blunders risks information systems certification CAP links**

RISKS; http://tinyurl.com/ayf5m 24 11

RISKS OF MEDICAL BLUNDERS

RISKS moderator Peter Neumann summarizes reports of some serious medical blunders involving bad data:

* In 1999, a 47-year-old woman was diagnosed with breast cancer in Magee-Womens Hospital (part of the U. Pittsburgh Medical Center), and underwent a mastectomy. It was later discovered that the hospital lab had switched biopsy specimens. Ten cases against the hospital are now pending in state courts, even though the hospital has passed federal inspections. Similar lawsuits and complaints name other medical centers.

* In Maryland, a hospital lab sent out hundreds of HIV and hepatitis test results despite data showing that the results might be invalid and mistakenly lead infected patients to believe they were disease-free. The same laboratory had just received a top rating from CAP inspectors.

* In Yakima, Wash., eight emergency room doctors walked off their jobs to protest hospital deficiencies they said included lab mistakes, such as mixed-up blood samples. CAP had declared the lab "in good standing" the year before.

* At the famed Mayo Clinic in Minnesota, an allegedly misdiagnosed gall bladder cancer case led to revelations of a close relationship between the clinic and CAP. A Mayo pathologist serving on a CAP advisory panel twice sought and obtained accreditation renewals despite unacceptable lab practices cited by CAP inspectors.

Category 38.9 Medical information & HIPAA

2005-12-13 **medical systems security disaster recovery backup plan business continuity paper**

RISKS; http://news.bbc.co.uk/1/hi/england/cambridgeshire/4521608.stm 24 13

CAMBRIDGE HOSPITAL BUSINESS CONTINUITY PLANS WORK

RISKS correspondent Paul Bennett reports the following story about medical systems security and disaster recovery:

A computer system at a Cambridge hospital used for patient information such as admissions and discharges experienced some problems because of a fire at the Buncefield oil depot in Hertfordshire. A company providing some IT services to Addenbrooke's Hospital was based at the industrial park near the depot and was destroyed in the fire. It was expected to take a week to get the computer system up again, although reportedly no medical services were affected.

[Abstract by Peter G. Neumann]

Another UK correspondent, Peter Mellor, follows up:

The explosion and fire at the fuel depot near Hemel Hempstead, Hertfordshire:
http://images.thetimes.co.uk/TGD/picture/0,,250768,00.jpg

Connection with computers? Well, several nearby installations were wrecked (amazingly, no-one was seriously injured), one of which contained the electronic patient records of Addenbrooke's Hospital, Cambridge. The hospital reported that it would have to rely on paper records for several
days until the computer files could be restored.

On the positive side, at least they had back-up. On the other hand, their disaster recovery planning seems to be a bit slack.

[Summary by Karthik Raman]

---

41 Cryptanalysis techniques & tools

Category 41 *Cryptanalysis techniques & tools*

1998-06-10 **cryptanalysis cracking RFI TEMPEST power fluctuations**

RISKS 19 80

Scientists at Cryptography Research published an analysis of three new approaches for cryptanalysis based on fluctuations in power usage or electromagnetic radiation from computer systems. For details on Simple Power Analysis, Differential Power Analysis and High-Order Differential Power Analysis see a variety of articles available from <http://www.cryptography.com/dpa/>.

Category 41 *Cryptanalysis techniques & tools*

2000-10-12 **decryption distributed computing international cryptanalysis**

NewsScan, New York Times
http://partners.nytimes.com/2000/10/12/technology/12R-CODE2.htm

A team of Swedish computer enthusiasts has succeeded in deciphering 10 increasingly difficult codes presented by author Simon Singh in his bestseller, "The Code Book." Singh, who has a doctorate in physics at Cambridge University in the U.K., took two years to develop the brain teasers with Dr. Paul Leyland, who works for Microsoft in Cambridge. The codes, which took the Swedes the equivalent of 70 years of computer time to decrypt, ranged from ciphers dating back to ancient Greece through the famed Nazi Enigma code machine used in World War II. The team was awarded a check for $15,000 for their efforts. Team leader Fredrik Almgren said the task was extremely daunting and that he and his fellow scientists were tempted to abandon the effort several times: "The first stages were very simple but at one point we thought we wouldn't get any further than stage eight. When you do come to the 10th stage it is a question of heavy mathematics and rather difficult algorithms that I don't even claim to understand myself." (Reuters/New York Times 12 Oct 2000)

Category 41 *Cryptanalysis techniques & tools*

2001-08-07 **decryption cracking law enforcement police investigation forensics swap file data remanence rubber-hose cryptanalysis**

RISKS 21 58

A report on the cryptography mailing list republished in RISKS included the following information about a police investigation that used cryptanalysis against a disk encryption program:

The German encryption program Safeguard Easy has been broken by the Danish police. Today the police from the city Holstebro in Jutland presented evidence in court, that was provided after breaking the encryption on five out of sixteen computers that where seized april 25 this year.

All 16 computers were protected with Safeguard Easy from the german encryption provider Utimaco. It is not known whether DES, 128-bit IDEA, Blowfish or Stealth was used as algorithm on the computers. All four algorithms are built in Safeguard Easy. Details are sparse. It is not known how the encryption was broken, whether it was brute forced or flaws in the program was exploited.

In followup correspondence, commentators suggested that since only some of the encrypted systems were cracked, perhaps the forensic analysis was able to locate passwords in the Windows swap file.

However, it turned out that actually the cryptanalysis was based on password guessing.

Category 41 *Cryptanalysis techniques & tools*

2002-05-14 **smart card inference cracking confidentiality cryptography key vulnerability**

NewsScan; http://www.newscientist.com/news/news.jsp?id=ns99992273

SMART CARDS REVEAL ALL DURING CAMERA FLASH
A flash of light can cause sensitive information stored on a smart card microprocessor to be revealed, say UK researchers at Cambridge University, who've found that firing light from an ordinary camera flash at parts of a smart card chip can assist a thief in determining the sensitive information stored on the card, including the cryptographic key used to secure financial transactions. The attack is described as "semi-invasive," as only part of a chip's protective covering must be removed in order to "flash" it. Meanwhile, another group at Cambridge has developed a microchip design that would resist this technique, using a more complex "asynchronous" microprocessor that would not respond in the same way to light interference. (New Scientist 13 May 2002)

Category 41 *Cryptanalysis techniques & tools*

2003-07-22 **crypanalysis password cracking Windows fast**

NewsScan, NIPC/DHS

NEW METHOD CRACKS PASSWORDS IN SECONDS

A senior research assistant at the Swiss Federal Institute of Technology's Cryptography and Security Laboratory has published a paper outlining a way to speed up the process of cracking alphanumeric Windows passwords to only 13.6 seconds on average. The previous average time was 1 minute, 41 seconds. The new method uses massive lookup tables to match encoded passwords to the original text entered by a person, thus reducing the time it takes to break the code. "Windows passwords are not very good," says researcher Phillippe Oechslin. "The problem with Windows passwords is that they do not include any random information." The only requirement for the cracker is a large amount of memory in order to accommodate the lookup tables. The larger the table, the shorter the time it takes to crack the password. Users can protect themselves by adding nonalphanumeric characters to a password, which adds another layer of complexity to the process. Any cracker would then need more time or more memory or both to accomplish the break-in. For more information on Oechslin's method, check out http://lasecwww.epfl.ch/php_code/publications/search.php?ref=Oech03
(Cnet News.com 22 Jul 2003)

[NIPC/DHS:]
July 22, CNET News.com — Cracking Windows passwords in seconds.

Swiss researchers from the Cryptography and Security Laboratory of the Swiss Federal Institute of Technology in Lausanne (EPFL) released a paper on Tuesday, July 22, outlining a way to speed the cracking of alphanumeric Microsoft Windows passwords, reducing the time to break such codes to an average of 13.6 seconds from 1 minute 41 seconds. The method involves using large lookup tables to match encoded passwords to the original text entered by a user, thus speeding the calculations required to break the codes. Called a time-memory trade-off, the situation means that an attacker with an abundance of computer memory can reduce the time it takes to break a secret code. Users can protect themselves against the attack by adding non-alphanumeric characters to a password. Philippe Oechslin, one of the researchers, said he hadn't notified Microsoft of the issue before publishing the paper.

Category 41 *Cryptanalysis techniques & tools*

2003-11-12 **cryptanalysis crack password Kansas auditor IT poor planning**

NIPC/DHS

November 07, Government Computer News — Kansas auditors crack 1,000 passwords.

The Kansas Health and Environment Department has serious IT security and disaster recovery problems, the state's legislative auditor has found. The auditors said they used password-cracking software to decipher more than 1,000 of the department's passwords-including several administrative passwords-or 60 percent of the total, in three minutes. The department began fixing the security weaknesses and other problems found in its systems as soon as it learned of them, department secretary Roderick L. Bremby said in response to the report. "The department's anti-virus system was badly flawed, allowing computers to become infected with a large number of different viruses, worms and Trojan horses," said the report. "The department's firewall was poorly configured, creating several large holes in and out," the report said. Auditors found that the department lacked or failed to enforce many basic security policies, such as procedures for incident response, physical security, configuration documentation and former-user account deletion. They also found several major problems with security planning.

Category 41 *Cryptanalysis techniques & tools*

2005-05-17 **hyperthreading multiprocessor architecture shared cache decryption cracking timing attacks encryption weakness cryptanalysis**

RISKS; http://www.daemonology.net/papers/htt.pdf 23 88

HYPERTHREADING AND SHARED CACHE ALLOW TIMING ATTACKS ON ENCRYPTION KEYS

Olin Sibert reported on public announcements about an unexpected consequence of hyperthreading multiple Intel Pentium 4 processors using shared cache:

Security researcher Colin Percival recently (13 May) announced a security vulnerability caused by the combination of the Hyperthreading and shared cache features of Intel Pentium 4 processors. By carefully measuring the time required for instructions to execute in one thread while the other thread is performing a cryptographic calculation, the secret key can be determined.

. . . .

Sibert concluded, "The RISK here is a classic example of relying on underlying abstractions (the hardware memory model) to behave in an ideal manner, rather than understanding their implementations. Many security flaws result from the adversary breaking the veil of abstraction to look at the soft, juicy parts inside. Even when the higher-level model is perfect (or formally verified), the mapping to implementation can hide a multitude of sins."

>This vulnerability was also announced by Adi Shamir during the Cryptographer's Panel at RSA in February 2005. I thought it was the most interesting item in all the keynotes (although the hash function announcements were a close second), but it got essentially no press coverage (unlike this time, where it is being widely reported). Adi subsequently told me that he had a working implementation and planned to present it at the Eurocrypt rump session next week. The two attack implementations (Colin's and Adi's) are apparently quite different, but yield the same result, underscoring the severity of the problem. It's also similar to Paul Kocher's classic timing attacks.

The problem is particularly bad for processors with simultaneous multithreading ("Hyperthreading"), since that allows context switches to take place at a granularity of individual instructions, and thus allows very fine-grained time measurements. However, the same basic problem is present in any computer with a cache that is physically shared by processes in different security domains.<

42 Crypto algorithms (weakness, brute-force attacks, implementation flaws)

Category 42 *Crypto algorithms (weakness, brute-force attacks, implementation flaws)*

1997-01-29 **cryptanalysis RSA challenge 40-bit key**

AP

RSA Data Security Inc. established a contest to crack ciphertexts created with keys of different lengths. A graduate student at U Cal Berkeley tackled the message encrypted with a 40-bit key — the longest key routinely granted export permits by the United States government. Ian Goldberg used 250 workstations in parallel and tested 100 billion keys an hour for 3.5 hours and read the cleartext: "This is why you should use a longer key." RSA Data Security Inc. spokesman Kurt Stammberger said, "It shows you that any kid with access to computers can crack this kind of cryptography. The cryptography software that you are allowed to export is so weak as to be useless."

Category 42 *Crypto algorithms (weakness, brute-force attacks, implementation flaws)*

1997-01-31 **Cryptanalysis**

RISKS 18 80

In late January, UC Berkeley graduate student Ian Goldberg took a mere 3.5 hours to decrypt a message encrypted using the RC5 algorithm with a 40-bit key — the most secure length of encryption key that the federal government allows U.S. companies to export.

Category 42 *Crypto algorithms (weakness, brute-force attacks, implementation flaws)*

1997-06-19 **cryptanalysis DES brute force parallel**

PR Newswire

The 56-bit DES encryption standard, long claimed adequate by the U.S. Government, was shattered in early June using 14,000 computers; the winning key was found by Michael K. Sanders, an employee of iNetZ, a Salt Lake City, Utah-based online commerce provider using an ordinary Pentium PC. Sanders was part of a loosely organized group of computer users responding to the "RSA $10,000 DES Challenge." The code-breaking group distributed computer software over the Internet for harnessing idle moments of computers around the world to perform a "brute force" attack on the encrypted data. The cracking effort required four months to decrypt a single message. The key happened to be about 25% of the way through the keyspace; on average, such a crack would be expected to run through half the keyspace. RSADSI's Jim Bidzos interpreted the exercise as a triumph: "We've been saying for a long time that DES is no longer secure and here is the proof." Other observers suggested that four months and 14,000 computers running in parallel to decipher a single message seems like evidence of pretty effective encryption — as long as the confidentiality of the message were to evaporate within a few months.

Category 42 *Crypto algorithms (weakness, brute-force attacks, implementation flaws)*

1998-02-27 **brute force cryptanalysis crypto DES cracking parallel**

RISKS 19 60

The 56-bit DES-II-1 challenge thrown down by RSA Data Security Inc. was completed by a massively-distributed array of computers coordinating their brute-force attacks via the distributed.net "organization." The cleartext was "Many hands make light work." The participants collectively examined 6.3 x 10^16 keys — fully 90% of the entire keyspace — in about 40 days. Conclusion: "56-bit DES is no longer sufficient for protecting valuable information" according to David McNett, a project leader. The estimated collective computer power in distributed.net was roughly equivalent to 41,712 Intel Pentium 166 MHz processors.

Category 42 *Crypto algorithms (weakness, brute-force attacks, implementation flaws)*

1998-03-31 **encryption flaw triple DES**

EDUPAGE

Eli Biham and Lars Knudson, cryptographers at the Technion in Israel and the University of Norway, respectively, found a serious flaw in the triple DES, causing the ANSI to delay its adoption as a standard for financial information transaction security.

Category 42 *Crypto algorithms (weakness, brute-force attacks, implementation flaws)*

1998-04-14 **encryption flaw cellular phone**

EDUPAGE

The new GSM digital cell phones turned out to be vulnerable to cryptographic attack if the attacker has access to the smart card ("SIM", for Subscriber Identification Module) required to operate the phones. In a spirited rebuttal, the North American GSM Alliance, LLC (the eight largest GSM network operators in the United States and Canada) provided the following assertions (with explanations that reassured this reader, at least):
1. GSM phones are not vulnerable to cloning (digital network software precludes multiple concurrent use of the same identifier).
2. There is no risk to subscribers.
3. There is no risk of over-the-air eavesdropping (the encryption algorithms are strong).
4. The ability to copy a SIM card is nothing new (and useless anyway because of the single-use algorithms).
5. The key code which protects a subscriber identity is not "fatally flawed." (Among other arguments, the authentication code broken by the cryptanalysts is not the algorithm used for encrypting conversations.)

Category 42 *Crypto algorithms (weakness, brute-force attacks, implementation flaws)*

1998-06-28 **cryptanalysis cracking SSL secure sockets layer**

EDUPAGE

Lucent Technologies, the business unit broken out of AT&T and including Bell Labs, announced that a staff scientist had cracked the Secure Sockets Layer. SSL is the protocol used for linking a Web browser securely to a Web server. The attack requires a physical connection to the targeted server and involves bombarding the server with about a million specific different messages and analyzing the responses. Patches appeared within days. In August, IBM announced that two researchers had invented a defensive mechanism, the Cramer-Shoup method, to defeat these "active" attacks.

Category 42 *Crypto algorithms (weakness, brute-force attacks, implementation flaws)*

1998-07-17 **cryptanalysis DES weakness keyspace 56-bit brute force**

RISKS 19 87

Matt Blaze offered a prize of "56 bits" ("2 bits" = $0.25 for you non-USAns) or $U7.00 for locating a DES key that would convert a ciphertext with a repeating pattern into a plaintext with a repeating pattern: "In particular, I wanted a DES key such that some ciphertext block of the form <XXXXXXXX> decrypts to a plaintext block of the form <YYYYYYYY>, where X and Y represent any fixed eight-bit byte value repeated across each of the eight bytes of the 64 bit DES codebook block." Blaze explained, "Finding a key of this form would require either computational effort approximately equal to searching the DES keyspace or discovering a new cryptanalytic technique against DES. Knowing such a key would therefore demonstrate that it is feasible to mount an exhaustive search against the DES keyspace or that there is some weakness in DES that allows keys to be found analytically." The prize was won by John Gilmore of the EFF, working with Deep Crack, the multiprocessor parallel computation array in a few days of search. The solution was, "With a (parity-padded) key of 0E 32 92 32 EA 6D 0D 73, the plaintext of 8787878787878787 becomes the ciphertext 0000000000000000".

Category 42 *Crypto algorithms (weakness, brute-force attacks, implementation flaws)*

1998-07-19 **cryptanalysis brute force parallel array supercomputer DES**

EDUPAGE

John Gilmore, Paul Kocher and a dozen other scientists created a massively parallel array of 1500 special-purpose DES-cracking processors for about $250K and set it to work cracking a message encrypted using the DES. It took them only 56 hours to scan about a quarter of the keyspace and locate the correct key to decrypt the ciphertext established by RSA Data Security Inc. as the object of the latest cryptanalysis contest. The EFF supported the effort financially and estimates that with the fruits of research in hand, the next parallel array would cost only about $50K.

Category 42 *Crypto algorithms (weakness, brute-force attacks, implementation flaws)*

1998-08-18 **cryptography algorithms review cryptanalysis FROG AES**

RISKS 19 92

Bruce Schneier and colleagues analyzed FROG, a candidate for the AES (Advanced Encryption Standard) and found it lacking. "Taken together, these observations suggest that FROG is not a very strong candidate for the AES." The complete document was available at <http://www.counterpane.com/publish.html>.

Category 42 *Crypto algorithms (weakness, brute-force attacks, implementation flaws)*

1998-12-22 **encryption decryption cryptanalysis brute force DES crack**

Wired http://www.wired.com/news/print_version/technology/story/16995.html

RSA Data Security Inc. established yet another demonstration project to show how weak 56-bit encryption has become in the face of massively parallel computing. The RSA DES Challenge III posted a ciphertext and offered a prize for its decryption.

Category 42 *Crypto algorithms (weakness, brute-force attacks, implementation flaws)*

1999-01-20 **cryptanalysis parallel processing crack DES challenge**

RISKS 20 17

The latest RSA challenge on cracking a message encrypted using the 56-bit DES algorithm was solved in about 22 hours by John Gilmore and the EFF's Deep Crack massively-parallel computing system and with the help of almost 100,000 volunteers around the world who attacked different parts of the keyspace. The EFF reported that the average search speed was 240 billion keys per second. Cryptographers agreed that the 56-bit DES is now inadequate as a method for securing data transmissions. The EFF won the grand prize of $10,000 for the feat.

Category 42 *Crypto algorithms (weakness, brute-force attacks, implementation flaws)*

1999-02-15 **PKI public key infrastructure dirty pair private criminal hackers**

INTERNETWEEK; Cylink http://www.cylink.com/library/white/sterilize.htm

According to scientists at Cylink, a network security vendor, it is possible for criminal hackers to develop "dirty" public/private key pairs to trick users of e-commerce. The scam would create keypairs that would allow different messages to have the same digital signature block; a criminal could thus spoof an authentic message by working backwards from the signature block, send the fraudulent message to the intended victim, and cause the public key cryptosystem to report a valid signature. The company recommended that proposed public keys be "sterilized" by a certification authority that would insert randomized data into the keys and provide mechanisms for legitimate users to modify their private keys accordingly.

Category 42 *Crypto algorithms (weakness, brute-force attacks, implementation flaws)*

1999-08-15 **encrypting file system cracked broken cryptanalysis algorithm bug defect debate disagreement analysis riposte rebuttal argument**

Crypto-gram 99 08

According to James J. Grace Senior and Thomas S. V. Bartlett III, Microsoft's Encrypting File System in Windows 2000 does not prevent discovery of disk decryption keys. A vigorous debate followed, in the "No it doesn't" — "Yes it does" style. See the story at < http://www.ntsecurity.net/forums/2cents/news.asp?IDF=118&TB=news >.

Category 42 *Crypto algorithms (weakness, brute-force attacks, implementation flaws)*

1999-08-16 **cryptography decryption TWINKLE engine brute force**

Wall Street Journal

Adi Shamir (the "S" in RSA) of the Weizmann Institute of Science in Rehovot, Israel announced a successful brute-force attack on a 512-bit RSA private key; the cryptanalysis took seven months and required 292 computers at 11 different sites. However, Shamir also described the design for a $2M cryptanalytic computer called "TWINKLE" that could apply brute-force attacks successfully to RSA keys of 512 bits or lower keylength in a less than a week.

Category 42 *Crypto algorithms (weakness, brute-force attacks, implementation flaws)*

1999-09-04 **decryption brute-force parallel computing challenge supercomputer**

InformationWeek

The RSA-155 challenge (decrypting a message encrypted using a 155-bit RSA asymmetrical encryption private key) took six weeks of processing by a Cray 900-16 supercomputer, 300 SGI and Sun Microsystems workstations and Pentium PCs working in parallel. As the project director from the National Research Institute for Mathematics and Computer Science in the Netherlands, Herman Riele, said, ". . . Internet transactions protected by RSA-155 are still generally safe."

Category 42 *Crypto algorithms (weakness, brute-force attacks, implementation flaws)*

1999-11-15 **elliptic curve public-key cryptography cracked cryptanalysis parallel processing brute-force**

Crypto-gram http://www.counterpane.com/crypto-gram-9911.html 99 11

A group of cryptographers cracked a message encrypted with a 97-bit elliptic curve private key. The project required parallel processing by 740 computers and used 16,000 MIPS-years. Although Certicom, the company sponsoring the challenge, claimed that this result showed that the elliptic-curve algorithms are stronger than the RSA PKC, Bruce Schneier demurred, writing that the case was not yet proven. See < http://www.counterpane.com/crypto-gram-9911.html >.

Category 42 *Crypto algorithms (weakness, brute-force attacks, implementation flaws)*

1999-12-04 **encryption crack algorithm weakness DVD unlock movie**

Newsbytes

IBM, Intel, Matsushita Electric, and Toshiba, the member of the 4Cs industry group (the 4C Group soon became the 5C Group with the addition of Hitachi), chose a digital watermark standard for DVD-audio in June. However, in early November, the DVD Content Scrambling System (CSS) was cracked. The CSS was supposed to protect digital video disks against unauthorized duplication through a set of interlocking encryption keys and algorithms on the disks and in the players. The free DeCSS program, widely circulated on the Net, completely bypasses the encryption system. According to Mike Musgrove, writing for Newsbytes, "XingDVD Player, a program from Xing Technologies, a subsidiary of RealNetworks Inc., reportedly left this CSS software unscrambled — somewhat like leaving an extra set of car keys on the passenger seat. A small team of computer programmers in Norway used this vulnerability to design the DeCSS software. A spokesman for RealNetworks did not have a comment at press time."

In December, Matsushita Electric Industrial Co. and JVC announced a six-month delay in releasing their DVD-audio players because of concerns over protection of intellectual property. This was described in the press as the first case in which a cracked encryption scheme delayed a significant consumer-electronic product release. However, some sceptics noted that the music industry had already expressed reservations about supporting the CSS2 (the Content Scrambling System version used in protecting audio tracks), which was felt to be insecure.

[MK comments: This case demonstrates the foolishness of not posting cryptographic algorithms in public for strong analysis and testing. As Dorothy Denning said years ago , the security of an encryption algorithnm must not depend on its obscurity.]

Category 42 *Crypto algorithms (weakness, brute-force attacks, implementation flaws)*

1999-12-06 **cellular phone encryption algorithm cryptanalysis flaw bug weakness vulnerability**

Wired http://wired.lycos.com/news/print/0,1294,32900,00.html

Alex Biryukov and Adi Shamir of the Weizmann Institute in Israel published a paper showing how a simple PC was able to break the A5/1 encryption algorithm used in the GSM cryptosystem for cell phones in less than a second. Estimates were that more than 230 million cellular phones made by Ericsson, Motorola, Nokia, Siemens and other popular brands were vulnerable to such decryption. However, manufacturers pointed out that no one has ever demonstrated an ability to intercept a GSM phone call in real time, so the ability to decrypt the calls remains of academic interest. This assertion was challenged immediately by experts who pointed to easily-available, inexpensive scanner devices that successfully intercept GSM communications. Other spokespersons for the industry said that they would move to using published algorithms rather than relying on proprietary, secret algorithms for future encryption standards in the industry.

Category 42 *Crypto algorithms (weakness, brute-force attacks, implementation flaws)*

2000-02-28 **encryption algorithm implementation broken cryptanalysis weakness DVD**

Crypto-gram 99 11

In late 1999, the DVD content-protection scheme called CSS (Content Scrambling System) was cracked and software to do so made available freely on the Internet. Cryptographer Bruce Schneier published a cogent summary of the situation in his Crypto-gram newsletter 99-11 < http://www.counterpane.com/crypto-gram-9911.html >. He explained that the problem lay in the fundamental model. Each DVD player has one of 400 different unlock keys. Every DVD has a decryption key that is required to read the data. The decryption key is encrypted 400 times — once with each of the unlock keys that could be present on any given DVD player. Unfortunately, this scheme fails because the computer must be able to put those keys into memory— and once in memory, a specially-crafted program can necessarily snaffle the decryption key. Schneier comments, "It might be a bitter pill for the entertainment industry to swallow, but software content protection does not work. It cannot work. You can distribute encrypted content, but in order for it to be read, viewed, or listened to, it must be turned into plaintext. If it must be turned into plaintext, the computer must have a copy of the key and the algorithm to turn it into plaintext. A clever enough hacker with good enough debugging tools will always be able to reverse-engineer the algorithm, get the key, or just capture the plaintext after decryption. And he can write a software program that allows others to do it automatically. This cannot be stopped." The only way protection can work in such a scheme is to put the algorithm into the hardware, he wrote — and it would have to extend to the monitor itself.

Category 42 *Crypto algorithms (weakness, brute-force attacks, implementation flaws)*

2003-04-14 **cryptography history award scientists future trends fundamentals**

ACM; NWF http://www.nwfusion.com/newsletters/sec/2004/0503sec1.html

The famous cryptographers Leonard Adleman, Ronald Rivest, and Adi Shamir - the developers of the RSA encryption code - received the Association for Computing Machinery's 2002 Turing Award "for their seminal contributions to the theory and practical application of public-key cryptography." Their Turing Award lectures, given last June, are available online.

Rivest, Shamir and Adleman implemented public-key cryptography in the 1970s following the landmark work of Whitfield Diffie, Martin Hellman and Ralph Merkle. They then founded RSA Security, which became one of the most respected security companies in the world.

The distinguished scientists' lectures are available online in a variety of formats at:
http://www.acm.org/awards/turing_citations/rivest-shamir-adleman.html

It was exhilarating to listen to these brilliant people speaking to us, and I hope some of you will have an hour to spare to enjoy their lectures.

42.1 Crypto algorithm weaknesses

Category 42.1 *Crypto algorithm weaknesses*

1997-03-20 **cryptanalysis eavesdropping cellular phone**

NYT

Cryptanalysts David Wagner (University of California at Berkeley), Bruce Schneier and John Kelsey (both of Counterpane Systems) announced that they had successfully cracked the proprietary encryption incorporated into the new generation of digital phones. The cryptographers strongly criticized industry for trying to secure systems without opening their algorithms to public scrutiny. Said famed author Schneier, ""Our work shows clearly why you don't do this behind closed doors. I'm angry at the cell phone industry because when they changed to the new technology, they had a chance to protect privacy and they failed." An additional criticism of the way the cell-phone industry incorporated encryption was that it deliberately adopted a weak standard to comply with U.S. government regulations forbidding the export of strong cryptography. John Markoff, writing in the New York Times, quoted James X. Dempsey, senior staff counsel for the Center for Democracy and Technology as saying, "This should serve as a wake-up call. . . . This shows that Government's effort to control encryption technology is now hindering the voice communications industry as well as the data and electronic communication realm."

Category 42.1 *Crypto algorithm weaknesses*

1997-03-20 **cellular-phone crypto**

RISKS 18 92

Bruce Schneier and colleagues at UC Berkeley announced in March that the most advanced digital cellular phones in use today have a flawed cryptographic algorithm, the Cellular Message Encryption Algorithm (CMEA), that can allow an eavesdropper with a PC to crack the conversations in minutes. The scientists blame the flaw on the closed-door, secret process in which the algorithm was implemented and make a plea for open analysis of cryptographic algorithms. They criticize pressure from the US government that they argue pushed the developers into the closed-door development.

Category 42.1 *Crypto algorithm weaknesses*

1997-11-26 **phone phreaking cellular research**

RISKS 19 48

Prof. Ross Anderson and his team at Cambridge University took up a challenge by MobilCom, a subsidiary of Deutsche Telekom, to phreak a specific cellular phone protected by a smartcard. After some effort, they developed a scheme that would appear to allow them to crack any GSM phone for which the digital identifier could be captured. Unfortunately, the challenge and offer of 100,000 DM had been withdrawn by the time the team finished its work.

Category 42.1 *Crypto algorithm weaknesses*

1997-12-22 **RFI eavesdropping theft authentication transponder**

RISKS 19 52

Philip Koopman reported on risks of the new Speedpass automatic payment scheme being promoted by Mobil Oil in the US. The main vulnerability appears to be weak encryption in the low-frequency, low-power radio transponders, resulting in easy capture and decryption of identification codes. Spoofing the devices should be easy with this captured information, leading to easy theft of fuel.

Category 42.1 *Crypto algorithm weaknesses*

2000-03-27 **encryption algorithm weakness decryption e-commerce**

RISKS 20

Stephen King's electronically-distributed book, _Riding the Bullet_, was released in encrypted form on the Web; decrypted formats quickly appeared. As Peter G. Neumann commented in RISKS, the incident provided " stark evidence of security weaknesses in PC-based eBook distribution systems" and "The episode has irked the companies developing such systems, who complain that export restrictions have kept them from using more powerful encryption techniques."

Category 42.1 *Crypto algorithm weaknesses*

2000-03-31 **e-book electronic book cryptography crack**

NewsScan, Wall Street Journal
http://interactive.wsj.com/articles/SB954465411569087773.htm/t000030180.html

Computer hackers cracked the software code that was designed to prevent multiple downloads of Stephen King's "Riding the Bullet" novella, confirming publishers' worries over the dangers inherent in electronic publishing. The e-book's publisher, Simon & Schuster, confirmed that at least two hackers downloaded the software necessary to read the book from Glassbook Inc., one of the Web companies given rights to distribute the book, and managed to break the encryption code that prevented more than one customer from having access to each electronic copy sold. Pirated copies of the book were then distributed to about six Web sites and chat groups. The publisher contacted many of the Internet service providers hosting the sites and had them shut down. "All the publishers are well aware there is no perfect technical solution to this problem," says Glassbook president Len Kawell. "We will do our best with technology; the rest is a matter of patrolling." (Wall Street Journal 31 Mar 2000)

Category 42.1 *Crypto algorithm weaknesses*

2000-07-21 **cryptanalysis cracking DVD scrambling hackers free speech litigation lawsuit**

Edupage, EE Times, NewsScan, New York Times, Los Angeles Times
http://www.latimes.com/business/20000818/t000077486.html

Over the course of 1999, several groups posted information about flaws in the Content Scrambling System (CSS) developed for DVD video players by the 4C group (IBM, Intel, Matsushita, Toshiba). The DeCSS software posted on the Net led to cancellation of the planned December 1999 launch of DVD-audio players (which use a related encoding scheme called CSS2) and postponed release of the new devices until mid-2000. Respected cryptographer Bruce Schneier pointed out that any decoding scheme suffers from a fatal weakness: the decoded data stream must be available somewhere to be able to display pictures or generate sound. Even the decryption keys, he argued, are available in cleartext in memory. ". . . [S]oftware content protection does not work. It cannot work," he said. Nonetheless, in January 2000, the Motion Picture Association of America (MPAA) sued the criminal-hacker support publication 2600.com and several Web site owners to get DeCSS program allegedly written by Norwegian teenager Jon Johansen off the Net. Free-speech advocates at the Electronic Frontier Foundation (EFF) argued that the copy-protection scheme should not be granted legal protection; 2600 called for street protests. The organization's Web site claimed that A missive on the 2600.com Website, meanwhile, claims that the issue was "whether you have the right to play DVDs on the computer of your choice and whether you should be able to see DVDs from other countries." The plaintiffs argued that the tool was promoting outright theft of their intellectual property.

[In July,] Eight movie studios . . . [went] to court charging that Eric Corley, who publishes the computer hacker magazine and Web site called "2600," has violated the law by distributing software that breaks the code used to encrypt DVDs. An attorney for the studios warned: "The threat of world copying is here and the process has begun. It will become an avalanche unless this court acts." A warning of a different kind came from the defendant's attorneys, who argued that a decision for the plaintiff would mean the end of "fair use," the concept that allows for limited and prescribed exceptions to general copyright rules. (New York Times 18 Jul 2000)

The Norwegian teenaged programmer Jon Johansen, who with two colleagues created the DeCSS software that breaks the encryption coding of DVD files, was called as a witness in the New York trial in which Hollywood studios are suing Long Island-based programmer Eric Corley for distributing the DeCSS software on the Internet, thereby encouraging illegal use of copyrighted movies. Corley's lawyer and the Electronic Frontier Foundation are defending his actions as an exercise of the Constitution's First Amendment right to freedom of speech. They argue that Corley never used DeCSS to pirate a movie, and that in fact to use the software to pirate movies would be impractical. (New York Times 21 Jul 2000)

[In August,] A federal judge ruled . . . against [the publisher of 2600, The Hacker Quarterly,] who posted software code that could be used to disable the electronic locks on DVDs, ordering defendant Eric Corley to remove the code from his 2600.com Web site as well as all links to other sites that post the DeCSS decryption code. The ruling came as a sweeping vindication of the entertainment industry's ongoing battle against piracy of copyrighted works. ". . . [The] landmark decision nailed down an indispensable constitutional and congressional truth: It's wrong to help others steal creative works," said Jack Valenti, chairman of the Motion Picture Association of America. The Electronic Frontier Foundation, which funded Corley's legal expenses, expressed surprise that the judge had also banned the links to other sites in his decision. "He is carving out a new exception for software under the 1st Amendment," said an EFF spokeswoman. (Los Angeles Times 18 Aug 2000)

Category 42.1 *Crypto algorithm weaknesses*

2000-08-09 **intellectual property IP DVD encryption algorithm crack**

NewsScan, Washington Post http://www.washingtonpost.com/wp-dyn/articles/A58594-2000Aug8.html

Fearful that increasing numbers of pirated movies will be swapped on the Internet, Hollywood studios and the DVD industry have taken legal action against a Norwegian teenager who wrote code to break the encryption of DVD files. The suit also names as defendant the hacker magazine that posted the code on its Web site, as well as dozens of other Web sites that reposted it. Jack Valenti of the Motion Picture Association of America says: "We're putting a stake in the ground and saying you can't do this. You can't break this code, you can't put the code on the Internet, you can't have file-sharing with movies the way you do with music. We're going to protect our copyright." Duke University law professor James Boyle sees the MPAA position as a novel use of copyright law, since it targets the medium rather than the message: ""People think of copyright as prohibiting certain actions. You can't copy too much of something, you can't perform something without permission. What the content companies are starting to do is use copyright to regulate devices and research and communication. So now you can't communicate about a computer code." (Washington Post 9 Aug 2000)

Category 42.1 *Crypto algorithm weaknesses*

2001-07-26 **cryptography weakness wireless protocol WEP 802.11 eavedropping cracking known-ciphertext attack**

RISKS 21 55

Famed cryptographer Adi Shamir (the "A" in "RSA") announced a new paper on weaknesses in WEP (Wired Equivalent Privacy):

"WEP is the security protocol used in the widely deployed IEEE 802.11 wireless LAN's. This protocol received a lot of attention this year, and several groups of researchers have described a number of ways to bypass its security.

Attached you will find a new paper which describes a truly practical direct attack on WEP's cryptography. It is an extremely powerful attack which can be applied even when WEP's RC4 stream cipher uses a 2048 bit secret key (its maximal size) and 128 bit IV modifiers (as proposed in WEP2). The attacker can be a completely passive eavesdropper (i.e., he does not have to inject packets, monitor responses, or use accomplices) and thus his existence is essentially undetectable. It is a pure known-ciphertext attack (i.e., the attacker need not know or choose their corresponding plaintexts). After scanning several hundred thousand packets, the attacker can completely recover the secret key and thus decrypt all the ciphertexts. The running time of the attack grows linearly instead of exponentially with the key size, and thus it is negligible even for 2048 bit keys."

Peter G. Neumann wrote, "Matt Blaze . . . put Adi's paper at < http://www.crypto.com/papers/others/rc4_ksaproc.ps >. . . ."

Rubin and colleagues published another relevant paper a week later; in RISKS, Rubin wrote the following:

Using the Fluhrer, Mantin, and Shamir Attack to Break WEP by Adam Stubblefield, John Ioannidis, and Aviel D. Rubin

We implemented an attack against WEP, the link-layer security protocol for 802.11 networks. The attack was described in a recent paper by Fluhrer, Mantin, and Shamir. With our implementation, and permission of the network administrator, we were able to recover the 128-bit secret key used in a production network, with a passive attack. The WEP standard uses RC4 IVs improperly, and the attack exploits this design failure. This paper describes the attack, how we implemented it, and some optimizations to make the attack more efficient. We conclude that 802.11 WEP is totally insecure, and we provide some recommendations.

http://www.cs.rice.edu/~astubble/wep/

Category 42.1 *Crypto algorithm weaknesses*

2001-08-06 **cryptographic algorithm weakness e-commerce Passport single signon**

RISKS 21 58

David P. Kormann and Aviel D. Rubin, Risks of the Passport Single Signon Protocol, IEEE Computer Networks, volume 33, pages 51-58, 2000.

. . .

Abstract:

Passport is a protocol that enables users to sign onto many different merchants' web pages by authenticating themselves only once to a common server. This is important because users tend to pick poor (guessable) user names and passwords and to repeat them at different sites. Passport is notable as it is being very widely deployed by Microsoft. At the time of this writing, Passport boasts 40 million consumers and more than 400 authentications per second on average. We examine the Passport single signon protocol, and identify several risks and attacks. We discuss a flaw that we discovered in the interaction of Passport and Netscape browsers that leaves a user logged in while informing him that he has successfully logged out. Finally, we suggest several areas of improvement.

http://avirubin.com/passport.html

Category 42.1 *Crypto algorithm weaknesses*

2001-08-15 **encryption algorithm cracked weakness decryption video chilling effect lawsuits DMCA HDCP**

RISKS 21 60

Monty Solomon wrote in RISKS that a video crypto standard was reported cracked:

"Noted cryptographer Niels Ferguson says he's broken Intel's vaunted High-bandwidth Digital Content Protection (HDCP) Digital Video Encryption System, but fear of U.S. law is keeping him silent on the details. HDCP connects digital cameras, high-definition televisions, cable boxes, and video disks players. [Source: Article by Ann Harrison, 13 Aug 2001, PGN-ed; http://www.securityfocus.com/news/236]"

Peter G. Neumann added: [Intel has not threatened him, but he can still be sued by the U.S. Govt under DMCA, or by the motion-picture industry. His comments are at < http://www.macfergus.com/niels/dmca/index.html >. Knowledge that it is (or might be) breakable is likely to result in other folks doing it, and perhaps posting it anonymously in some non-US Web site. The globalization of the Internet is clearly going to be an increasingly difficult problem for industries trying to defend information supposedly protected under flawed standards. . . .]

Niels Ferguson wrote an essay in RISKS 21.60 entitled, "Censorship in action: why I don't publish my HDCP results ." Some excerpts:

I have written a paper detailing security weaknesses in the HDCP content protection system. I have decided to censor myself and not publish this paper for fear of prosecution and/or liability under the US DMCA law.

Introduction

My name is Niels Ferguson. I'm a professional cryptographer. My job is to design, analyse, and attack cryptographic security systems, a bit like a digital locksmith. I work to make computer systems and the Internet more secure. You would think that people would be in favour of that, right?

Computer security and cryptography are hard. It is easy to make mistakes, and one mistake is all it takes to create a weakness. You learn from your mistakes, but there are too many mistakes to make them all yourself. That's why we publish. We share our knowledge with others, so that they don't have to repeat the same mistake. Take a look at < http://www.macfergus.com/niels/dmca/index.html../pubs/publist.html> my publications. You will see a mixture of new designs, analyses, and attacks. This is how we learn and how we improve the state of the art in computer security.

HDCP

Recently I found the documentation of the < http://www.digital-cp.com> High-bandwidth Digital Content Protection (HDCP) system on the Internet. HDCP is a cryptographic system developed by Intel that encrypts video on the DVI bus. The DVI bus is used to connect digital video cameras and DVD players with digital TVs, etc. The aim of HDCP is to prevent illegal copying of video contents by encrypting the signal.

HDCP is fatally flawed. My results show that an experienced IT person can recover the HDCP master key in about 2 weeks using four computers and 50 HDCP displays. Once you know the master key, you can decrypt any movie, impersonate any HDCP device, and even create new HDCP devices that will work with the 'official' ones. This is really, really bad news for a security system. If this master key is ever published, HDCP will provide no protection whatsoever. The flaws in HDCP are not hard to find. As I like to say: "I was just reading it and it broke."

[Later in the paper, Ferguson pens a cogent attack on the very premise of the DMCA (Digital Millennium Copyright Act):]

The DMCA imposes a serious restriction on the freedom of speech. The DMCA makes it illegal to talk about certain security systems. The equivalent law for non-digital protection systems would make it illegal to warn people about a cheap and very weak door lock being installed on their houses because criminals could also use that same information.

In western society we restrict the freedom of speech only for very serious reasons, and after careful consideration. For example, it is illegal to shout "fire" in a crowded theatre, or to ask someone to commit a murder. The DMCA restricts the freedom of speech because the movie industry is afraid of losing money. Below I will argue that the DMCA does not achieve that goal, but that aside: do we really want to sell our freedom of speech for money?

The DMCA is a scary development. Next time that commercial interests clash with the freedom of speech, the industry will point to the DMCA and claim they need equivalent protection. They might outlaw the publication of a report detailing bad safety features in a car, or of flaws found in a particular brand of tires. After all, those publications harm industry too. Where will it stop?

[I encourage everyone interested in the DCMA to read the entire text of this essay, which is available at < http://www.macfergus.com/niels/dmca/index.html >. -- MK]

Category 42.1 *Crypto algorithm weaknesses*

2002-02-15 **wireless networks Wi-Fi 802.1x WEP vulnerabilities implementation man-in-the-middle attacks interception session hijacking**

RISKS 21 92

From an article by Ephraim Schwartz in InfoWorld, Thursday, February 14, 2002 as reported in RISKS by Monty Solomon:

Researchers Claim to Crack Wi-Fi Security; Proponents deny wireless networking spec is vulnerable to hijack, authentication attacks.

A University of Maryland professor and his graduate student have apparently uncovered serious weaknesses in the next-generation Wireless Fidelity security protocol known as 802.1x. In a paper, "An Initial Security Analysis of the IEEE 802.1X Standard" funded by the National Institute of Standards, Professor William Arbaugh and his graduate assistant Arunesh Mishra outline two separate scenarios that nullify the benefits of the new standard and leave Wi-Fi networks wide open to attacks. The use of public access "hot spots" are particularly vulnerable to session hijacking because these locations do not even deploy the rudimentary Wired Equivalent Privacy protocol. "This problem exists whether you use WEP or not, but it is trivial to exploit if not using WEP," said Arbaugh.

Flaws Described

Dubbed "session hijacking" and "man-in-the-middle," both attacks basically exploit inherent problems in Wi-Fi as well as exploiting how the new 802.1x standard is designed. "Here's how session hijacking works. The hacker waits for someone to finish successfully the authentication process. Then you as the attacker send a disassociate message, forging it to make it look like it came from the AP [access point]. The client [user] thinks they have been kicked off, but the AP thinks the client is still out there. As long as WEP is not involved you can start using that connection up until the next time out, usually about 60 minutes," said Arbaugh. [...]

http://www.pcworld.com/news/article/0,aid,84424,00.asp

Category 42.1 *Crypto algorithm weaknesses*

2002-03-10 **weak encryption vulnerabilities ICAT CVE**

ICAT Metabase

The ICAT Metabase < http://icat.nist.gov/icat.cfm > for the Common Vulnerabilities and Exposures (CVE) database reported 10 vulnerabilities involving weak encryption out of a total of 1241 for the period from 1 Jan 2001 to 10 Mar 2002. This represents about 1% of all vulnerabilities logged for that period. Overall, for the entire period since the CVE began recording vulnerabilities in 1995, weak encrytion is named in 51 of the 3677 vulnerabilities or about 1% of the total. The vulnerabilities listed for 2001 and up to 10 Mar 2002 are as follows:

CAN-2001-1005: Starfish Truesync Desktop 2.0b as used on the REX 5000 PDA uses weak encryption to store the user password in a registry key, which allows attackers who have access to the registry key to decrypt the password and gain privileges. Published Before: 8/31/2001 Severity: Medium

CAN-2001-1003: Respondus 1.1.2 for WebCT uses weak encryption to remember usernames and passwords, which allows local users who can read the WEBCT.SVR file to decrypt the passwords and gain additional privileges. Published Before: 8/31/2001 Severity: Medium

CAN-2001-0983: UltraEdit uses weak encryption to record FTP passwords in the uedit32.ini file, which allows local users who can read the file to decrypt the passwords and gain privileges. Published Before: 8/31/2001 Severity: High

CAN-2001-0618: Orinoco RG-1000 wireless Residential Gateway uses the last 5 digits of the 'Network Name' or SSID as the default Wired Equivalent Privacy (WEP) encryption key. Since the SSID occurs in the clear during communications, a remote attacker could determine the WEP key and decrypt RG-1000 traffic. Published Before: 8/2/2001 Severity: High

CAN-2001-0352: SNMP agents in 3Com AirConnect AP-4111 and Symbol 41X1 Access Point allow remote attackers to obtain the WEP encryption key by reading it from a MIB when the value should be write-only, via (1) dot11WEPDefaultKeyValue in the dot11WEPDefaultKeysTable of the IEEE 802.11b MIB, or (2) ap128bWepKeyValue in the ap128bWEPKeyTable in the Symbol MIB. Published Before: 7/21/2001 Severity: Medium

CAN-2001-0382: Computer Associates CCC\Harvest 5.0 for Windows NT/2000 uses weak encryption for passwords, which allows a remote attacker to gain privileges on the application. Published Before: 6/18/2001 Severity: High

CAN-2001-0133: The web administration interface for Interscan VirusWall 3.6.x and earlier does not use encryption, which could allow remote attackers to obtain the administrator password to sniff the administrator password via the setpasswd.cgi program or other HTTP GET requests that contain base64 encoded usernames and passwords. Published Before: 3/12/2001 Severity: High

CAN-1999-0757: The ColdFusion CFCRYPT program for encrypting CFML templates has weak encryption, allowing attackers to decrypt the templates. Published Before: 3/12/2001 Severity: Medium

CAN-2001-0103: CoffeeCup Direct and Free FTP clients use a weak encryption to store passwords in the FTPServers.ini file, which could allow attackers to easily decrypt the passwords. Published Before: 2/12/2001 Severity: Medium

CAN-2000-1173: Microsys CyberPatrol uses weak encryption (trivial encoding) for credit card numbers and uses no encryption for the remainder of the information during registration, which could allow attackers to sniff network traffic and obtain this sensitive information. Published Before: 1/9/2001 Severity: Medium

Category 42.1 *Crypto algorithm weaknesses*

2005-02-16 **Chinese researchers break compromise SHA-1 secure hash algorithm SHA-256 SHA-512 NIST recommendations**

DHS IAIP Daily; http://www.eetimes.com/article/showArticle.jhtml?articleId=60401254

CHINESE RESEARCHERS CLAIM TO HAVE COMPROMISED SHA-1 HASHING ALGORITHM.

A team of three Chinese researchers claim to have compromised the SHA-1 hashing algorithm at the core of many of today's mainstream security products. Top cryptographers said users can still rely on today's SHA-1-based systems and applications, but next-generation products will need to move to new algorithms. In a panel discussion at the RSA Conference on Tuesday, February 15, Adi Shamir, a celebrated cryptographer and professor at Israel's Weizmann Institute of Science, said he received an e-mail that morning containing a draft technical paper from the research team of Xiaoyun Wang, Lisa Yiqun Yin, and Hongbo Yu who have links to Shandong University in China. The paper described how two separate documents could be manipulated to deliver the same SHA-1 hash with a computation of lower complexity level than previously believed possible. Shamir and others said they believe the work of the Chinese trio will probably be proven to be correct based on their academic reputations, although details of the paper are still under review. Perhaps anticipating the news, the National Institute of Standards and Technology issued a recommendation earlier this month that developers move to SHA-256 and SHA-512 algorithms by 2010.

42.2 Brute-force attacks

Category 42.2 *Brute-force attacks*

1997-08-22 **hacker challenge crypto**

Dow Jones, EDUPAGE

Crypto-Logic Corp. has offered to pay $1M to anyone who cracks its e-mail encryption system within a year. The encryption depends on a one-time pad and is, in theory, unbreakable.

Category 42.2 *Brute-force attacks*

2000-01-17 **encryption algorithm cracked cryptanalysis brute-force parallel processing distributed**

Wired http://www.wired.com/news/print/0,1294,33695,00.html

The French systems integrator CS Communications & Systems developed a secret-key encryption algorithm and challenged cryptographers to crack a message encrypted with a 56-bit key. After 62 days of processing on 38,000 computers, the Distributed.net group cracked the message and won the $10K prize. The parallel processing effort had to check 98% of the keyspace to find the key.

Category 42.2 *Brute-force attacks*

2000-02-17 **legal restrictions password decryption cracking tool burglary jurisprudence**

Channel4000.com http://www.channel4000.com/news/stories/news-20000217-164727.html

In Minneapolis, David Thomas Bell (33) was charged with 15 felony charges of unauthorized computer access, theft of trade secrets, attempted theft of trade secrets, computer theft, and possession of burglary tools. Nicole Lin Brelje (28) was charged with four felony counts. The defendants were accused of stealing a client list from Bell's former employer so they could take their business to Bell's and Brelje's new employer; the victim estimated the value of that list at $2.5M. Investigation also suggested that Brelje had helped Bell run L0phtCrack, a password-guessing program, on their new employer's system. Bruce Schneier commented in his Crypto-Gram for 2000-03-15 < http://www.counterpane.com/crypto-gram-0003.html > that the interesting aspect of the case was the charge that using L0phtCrack constituted possession of burglary tools.

Category 42.2 *Brute-force attacks*

2002-11-14 **supercomputer cryptanalysis brute-force speed power keylength keyspace**

NewsScan

CRAY LAUNCHES NEW LINE OF SUPERCOMPUTERS
Cray released more details about its long-awaited Cray XI machine and says it plans to begin shipping, on schedule, by the end of this year. An entry-level Cray XI will start at $2.5 million, but CEO Jim Rottsolk says he expects the majority of systems sold to range from $5 million to $40 million. A top-of-the-line machine with 50 cabinets would cost $200 million to $300 million and would likely topple NEC's position as the maker of the world's fastest system. (Wall Street Journal 14 Nov 2002)

Category 42.2 *Brute-force attacks*

2002-11-15 **supercomputers contest cryptanalysis brute-force factoring**

NewsScan

SUPERFAST SUPERCOMPUTERS
And they're off and running and it's neck and neck at the turn... Or, anyway, NEC. In the current ranking of world's fastest-computers, compiled semi-annually by computer scientists at the University of Tennessee and the University of Mannheim, the fastest computer right now is the Earth Simulator, made by NEC Corporation of Japan. Of the remaining computers in the top ten, seven are from the U.S., one is from France, and one is from the United Kingdom. One of the top-ranked supercomputers, the NetworkX/Quadrics machine at Lawrence Livermore National Laboratories in California, uses the Linux operating system and Intel microprocessors. In the new ranking, the U.S. has 46% of all supercomputer systems installed, and is the producer of 91% of all systems manufactured. (New York Times 15 Nov 2002)

Category 42.2 *Brute-force attacks*

2002-11-19 **supercomputers cryptanalysis brute-force factoring**

NewsScan

SUN SUPERCLUSTERS
Sun Microsystems has developed new superclustering technology (code-named Wildcat) capable of achieving throughput rates of 4.8 gigabytes to one teraflop per second; now called Sun Fire Link connect, the technology will be used in data center operations in education, research, government, and other facilities. Calling it a "much more scalable cluster interconnect to address commercial and high-performance computing environments," Sun says that Fire Link will have the capability to support up to 800 CPUs. (Internet.com 18 Nov 2002)

Category 42.2 *Brute-force attacks*

2002-11-20 **supercomputers cryptanalysis brute-force factoring**

NewsScan

IBM COMPUTERS TO RIVAL HUMAN BRAIN
IBM has signed a $290 million contract with the federal government for new supercomputers; one, called ASCI Purple, is eight times faster than the computer currently used for nuclear testing; the second, called Blue Gene/L, will be used in weather modeling. Blue Gene/L will be powered by 130,000 of IBM's new Power5 microprocessors and will be 400,000 times faster than the typical home computer. ASCI Purple will be 2 1/2 times faster than the current speed champion, NEC's Earth Simulator. (Reuters/Forbes Newswire 20 Nov 2002)

Category 42.2 *Brute-force attacks*

2003-01-09 **supercomputers cryptanalysis brute force factoring**

NewsScan

IBM RENTS OUT SUPERCOMPUTING POWER
IBM has launched a new program to rent out processing power on its supercomputers, and has signed up Petroleum Geo-Services, a petrochemical company, as its first customer. PGS has about 1,000 of its own dual-processor Linux computers clustered into a single computing resource, but it's renting another 400 from Big Blue, says a company spokesman. The new service reflects IBM's push toward "utility computing," which enables companies with fluctuating needs for computing power to pay for it as they use it. An e-commerce operation, for instance, may need to beef up its processing power during the busy holiday shopping season, but that demand drops off in January. IBM also expects to find many of its customers in the petrochemical and life sciences industries. (CNet News.com 8 Jan 2003)
http://news.com.com/2100-1001-979780.html

Category 42.2 *Brute-force attacks*

2003-01-28 **parallel processing supercomputer grid computing Unix brute-force decryption encryption cryptography factoring PKC PKI**

NewsScan

GM TO LINK IBM UNIX MACHINES INTO SUPERCOMPUTER
General Motors is buying 10 high-performance Unix computers from IBM and plans to link them together to form one of the world's most powerful supercomputers. GM plans to use the supercomputer to run a range of simulations, from crash tests to noise measurements, and said the new system will quadruple its supercomputing capacity. GM's new system is "a fairly dramatic deployment of technology," says a senior marketing analyst, who notes that using supercomputers to simulate automobile performance is much quicker and cheaper than building prototypes. It will also make it easier for GM to "engage in limited production-run products" for specialty cars. (Wall Street Journal 29 Aug 2002)

TIME MACHINES FOR A NEW CENTURY
Wolfgang Grentzsch of Sun Microsystems thinks that grid computing (which links large numbers of computers into a giant grid-like single system) should be thought of as "time machines," because they will speed up our perception of the world — just as the steam engine and the internal combustion engine speeded up travel and our sense of time. "On the grid, you can do things much, much faster, and you can do things you never were able to do before." Things like virtual tests of new drugs, which could change all the current equations in the nation's health care delivery system. IBM's Dan Powers says that the longer-term vision of grid computing is basically about "the virtualization of information technology." (Reuters/USA Today 29 Aug 2002

GRIDS ARE THE 'JET-AGE' MODEL OF COMPUTING
Grid computing, which links individual computers into a network that harnesses the power of surplus processing cycles and applies them to new tasks, is gaining wider acceptance. Computer scientist Larry Smarr of the University of California at San Diego explains: "Today's Internet could be thought of as a Polynesian model, where you have all these islands, and people use canoes to get from one to another. We're changing that to a jet-age model, where you can get from one city to another traveling at speeds far greater than what you travel at once you get into the city itself." Smarr and colleagues in Illinois are building an "OptIPuter" — a computing grid to connect the University of San Diego with Illinois universities. The OptIPuter project is buying an optical-switching router made by a Texas company called Chiaro Networks. Smarr says: "University researchers can generate some market demand for these products and help get companies like Chiaro through the desert until the commercial economy picks up again." (KRT/San Jose Mercury News 18 Dec 2002)

IBM GRIDS UP FOR BATTLE
Looking at developing new markets that will generate big computer-services business, IBM is launching ten new grid computing initiatives targeted at niche markets where grid technology is being welcomed by early adopters. (Grid computing salvages the unused processing cycles of large numbers of networked computers to allow massing sharing of data storage and computer power.) As part of the initiatives IBM has formed alliances with Toronto-based Platform Computing and New York-based DataSynapse, as well as with Avaki, Entropia, and United Devices. (The Register 28 Jan 2003)
http://www.theregister.co.uk/content/61/29060.html

Category 42.2 *Brute-force attacks*

2003-02-26 **nanotechnology parallel processing cryptanalysis brute-force**

NewsScan

DNA COMPUTING UPDATE
Two years ago Israeli researchers developed an incredibly tiny computer that used DNA and enzymes as its software and hardware (a computer so small that a trillion of the machines could be placed in a single drop of water). Now, the same researchers say they've found a way for molecular machines to do without an external energy source and to perform 50 times faster than the previous version, which is listed in the Guinness Book of Records as the world's smallest biological computing device. (Scientific American 25 Feb 2003)

Category 42.2 *Brute-force attacks*

2005-02-01 **RFID radio frequency identification device cryptographic weakness crack parallel processing fraud theft gasoline purchase automobile lock**

RISKS; http://www.theregister.com/2005/01/31/rfid_crypto_alert/ 23 69

KERCHOFF RULES

Chris Leeson summarized the predictable failure of a proprietary encryption algorithm:

According to an article in *The Register*, the security on RFID devices used in car keys and petrol pump payment systems has been broken (the article actually says "Researchers have discovered cryptographic vulnerabilities in the RFID technology…"

The encryption uses "an unpublished, proprietary cipher that uses a 40-bit key".

The researchers managed to reverse-engineer the system and program a microchip to do the decoding in 10 hours. Using 16 of the chips in parallel reduced the search time to 15 minutes. At about $200 per chip that's not an expensive brute force attack.

The article notes that although potential criminals could make fraudulent petrol charges and deactivate vehicle immobilisation systems, they would still have top get past physical locks in the car.

Provided that the car has them, of course.

I can't resist quoting from the last two paragraphs:

> "The team recommends a program of distributing free metallic sheaths to cover its RFID devices when they are not being used in order to make attacks more difficult.
>
> The company that markets ExxonMobil's SpeedPass system has said it has no knowledge that any fraudulent purchases have ever been made with a cloned version of its device."

The Risks? Well, apart from the fairly obvious security/fraud issues, it does seem to me that this is using technology for technology's sake. When I want to disarm the alarm on my car, I point the remote at it and press the button. I don't need an "always on" control…

Category 42.2 *Brute-force attacks*

2005-03-30 **cryptanalysis evidence encryption massively parallel processing network computing government project criminal investigations**

RISKS; http://www.washingtonpost.com/wp-dyn/articles/A6098-2005Mar28.html 23 83

SECRET SERVICE BUILDS DISTRIBUTED NETWORKING ATTACK TOOL FOR CRYPTANALYSIS

Faced with the increasing prevalence of encrypted evidence on computers seized in criminal investigations, the Secret Service has created a massively parallel computing array using 4,000 "of its employees' computers into the 'Distributed Networking Attack' program." Brian Krebs, writing in the Washington Post and abstracted by Peter G. Neumann of RISKS, reported that "The wide availability of powerful encryption software has made evidence gathering a significant challenge for investigators. Criminals can use the software to scramble evidence of their activities so thoroughly that even the most powerful supercomputers in the world would never be able to break into their codes. But the U.S. Secret Service believes that combining computing power with gumshoe detective skills can help crack criminals' encrypted data caches. Taking a cue from scientists searching for signs of extraterrestrial life and mathematicians trying to identify very large prime numbers, the agency best known for protecting presidents and other high officials is tying together its employees' desktop computers in a network designed to crack passwords that alleged criminals have used to scramble evidence of their crimes -- everything from lists of stolen credit card numbers and Social Security numbers to records of bank transfers and e-mail communications with victims and accomplices."

Category 42.2 *Brute-force attacks*

2005-11-10 **password cracking service hackers online brute force rainbow tables**

EDUPAGE; http://www.theregister.co.uk/2005/11/10/password_hashes/

NEW SERVICE CRACKS PASSWORDS

Three computer hackers have set up a Web site that offers access--for a fee--to so-called rainbow tables, which are said to allow cracking of most passwords. Computers use codes, or hashes, to conceal user passwords. The creators of the RainbowCrack Online Web site spent two years generating hashes for virtually all possible passwords and storing them in vast tables. With the tables, breaking a password becomes as simple as looking up the hashes and working backwards to the password. Developers of RainbowCrack said the service is not intended for malicious uses but as a tool for network administrators to improve the security of their systems. Security expert Bruce Schneier disagreed, saying he doesn't see any "legitimate business demand" for the service. Philippe Oechslin of Swiss firm Objectif Securite said that system designers can easily incorporate elements into password schemes that add sufficient complexity as to make rainbow tables ineffective in cracking passwords. Schneier said that although such changes are not difficult, very few systems are designed to use them. "A lot of systems are weak," he said. The Register, 10 November 2005

42.3 Crypto product implementation flaws

Category 42.3 *Crypto product implementation flaws*

1997-05-07 **crypto algorithm RC2 S/MIME e-mail**

Wired

Phil Zimmermann of PGP Inc is battling Netscape and Microsoft because they incorporate the crippled 40-bit encryption of S/MIME from RSADSI. Another political problem in the e-mail encryption arena is the attempt by RSADSI and supporters to have S/MIME, a proprietary product, declared as an industry standard.

Category 42.3 *Crypto product implementation flaws*

2001-03-20 **cryptanalysis public key cryptosystem weakness private key cracking**

RISKS 21 28

David Kennedy, CISSP summarized a report about a major problem with OpenPGP: with access to a PGP user's private keyring, it is possible to obtain the private key and then use it to forge PGP signatures. Kennedy pointed to research by Czech cryptologists published at < http://www.i.cz/en/onas/tisk4.html >. The quoted material included this description of the cryptanalysis: "A slight modification of the private key file followed by capturing a signed message is enough to break the private key. These tasks can be performed without knowledge of the user's passphrase. After that, a special program can be run on any office PC. Based on the captured message,the program is able to calculate the user's private key in half a second. The attacker can then sign any messages instead of the attacked user. Despite of very quick calculation, the program is based on a special cryptographic know-how."

In a later posting to RISKS, Kennedy wrote, "Hal Finney has a succinct analysis posted to the Open-PGP list archived at:
http://www.imc.org/ietf-openpgp/mail-archive/msg04767.html
My [DK's] summary of Hal's analysis:
1. Attackers have to diddle the secret key.
2. Does *not* work with commercial PGP 7.0.3 w/RSA keys (unknown about earlier).
3. Does work with all DSA keys and RSA keys in GPG."

Category 42.3 *Crypto product implementation flaws*

2001-11-09 **cryptography hardware software weakness vulnerability cracking penetration decryption abuse insider crime confidentiality passwords bank automated teller machines**

RISKS 21 74

Andrew Brydon, writing in RISKS, summarized the findings of research on automated banking machine security in Britain: "A serious weakness has been discovered in the methods used by banks to protect the number that lets you get money from a cash machine. Researchers from the University of Cambridge have found that the computer systems which check that these numbers are valid are easy to defeat. They warn that unscrupulous insiders could exploit these weaknesses to raid customer accounts. The researchers have called on banks to revise their security arrangements and use more open procedures to protect customers' cash. . . . The physical construction of the cryptoprocessors is certified to a high standard to ensure that the boxes cannot be forced to give up the keys they use to scramble data. Any physical tampering with the box makes them destroy the keys they use. [However,] security researchers Michael Bond and Richard Clayton have found serious weaknesses in the software cryptoprocessors use to handle the encryption keys as they talk to different programs. ... using the clues provided by the leaky software, the cracking time can be reduced to just 24 hours."

http://news.bbc.co.uk/hi/english/sci/tech/newsid_1645000/1645552.stm

---

Category 42.3 *Crypto product implementation flaws*

2002-07-12 **PGP plugin encryption flaw bug**

NewsScan

PRETTY POOR PRIVACY FROM NETWORK ASSOCIATES
A computer security company has uncovered a flaw in PGP (Pretty Good Privacy) -- a freely distributed, public key encryption system that's used to scramble e-mail messages -- that could allow malicious users to unscramble sensitive messages. The flaw is found only in PGP plug-ins for Microsoft Outlook users distributed by Network Associates. "The PGP vulnerability enables an attacker to send a specially crafted e-mail to any Outlook address enabled with the PGP plug-in, which will in turn give them access to that system," says eEye Digital Security, which discovered the problem. EEye chief hacking officer Marc Maiffret says the flaw allows an attacker to do "anything a user of that machine could do -- copy files, delete files, install a backdoor." Gartner research director for Internet security John Pescatore says, "This vulnerability means people using [the affected] version of PGP actually are less secure than if they weren't using security at all. It's always a really, really bad thing when a security product has a bug." (NewsFactor Network 11 Jul 2002)
http://www.ecommercetimes.com/perl/story/18560.html

Category 42.3 *Crypto product implementation flaws*

2003-02-24 **e-mail code crack Secure Sockets Layer SSL Swiss Federal Institute Technology**

NIPC/DHS

February 20, Reuters — Swiss crack e-mail code, but minimal impact seen.

Professor Serge Vaudenay of the Swiss Federal Institute of Technology in Lausanne, Switzerland, found a way to unlock a message encrypted using Secure Socket Layer (SSL) protocol technology, according to a posting on the research institute's Web site. However, U.S. cryptography experts said it was not the version of security that most consumers use to shop online. Rather, it is a version that only affects e-mail, is limited in scope, and not widely used, said Professor Avi Rubin, who is technical director of the Information Security Institute at Maryland's Johns Hopkins University. In addition, an attacker would have to be in control of a network computer located in the middle of the two people communicating over which the messages were flowing, he said. ``It's possible, but it has limited applicability," he said. He said patches are already available to fix the hole, which affects one particular mode of OpenSSL. Like all co-called ``open source" software, OpenSSL is free software created by developers who can modify it at any time. Bruce Schneier, chief technical officer at network monitoring firm Counterpane Internet Security, agreed. Besides the mitigating circumstances which lessen the likelihood that attackers would be successful, Schneier said SSL is irrelevant to security because attackers can more easily get at secret information while it is stored on computers and servers at the sending and receiving ends. ``SSL protects the communications link between you and the Web" server, he said. ``Nobody bothers eavesdropping on the communications while it is in transit."

Category 42.3 *Crypto product implementation flaws*

2003-07-25 **Windows passwords cryptography salt implementation flaw**

http://www4.gartner.com/DisplayDocument?doc_cd=116510

Gartner analyst Ray Wagner wrote,
"According to news reports published on 23 July 2003, Swiss technology researchers have issued a report that describes how Windows computers protected by alphanumeric passwords can be quickly and easily cracked — in less than 14 seconds — by using precalculated data stored in look-up tables. Such ease of cracking, suggest the researchers, is due to Microsoft not using "salt" (a standard security mechanism applied to encrypted passwords) in its Windows operating system. Other computer operating systems, such as Linux, Mac OS X and Unix, do use salt in their password encoding technologies, which can deter or delay password breaches."

Category 42.3 *Crypto product implementation flaws*

2005-01-31 **car keys Texas Instruments TI crack immobilizer radio-frequency microchips encryption decryption transponder**

NewsScan; http://australianit.news.com.au/articles/0

WHERE DID I PUT MY CAR KEYS?

A research team at Johns Hopkins University has found a way to crack the code used in millions of car keys -- a development that could allow thieves to bypass the security systems on newer car models. The researchers found that the "immobilizer" security system developed by Texas Instruments could be cracked using a relatively inexpensive electronic device that acquires information hidden in the microchips that make the system work. The radio-frequency security system being used in more than 150 million new Fords, Toyotas and Nissans involves a transponder chip embedded in the key and a reader inside the car. If the reader does not recognize the transponder, the car will not start, even if the key inserted in the ignition is the correct one. (The Australian, 31 Jan 2005)

Category 42.3 *Crypto product implementation flaws*

2005-02-09 **SafeNet SoftRemote Virtual Private Network client VPN key process memory disclosure update issued**

DHS IAIP Daily; http://securitytracker.com/alerts/2005/Feb/1013134.html

VULNERABILITY IN SAFENET SOFTREMOTE VPN CLIENT MAY ALLOW LOCAL USERS TO OBTAIN VPN KEY

The SafeNet SoftRemote client 'IreIKE.exe' process stores the VPN password (i.e., preshare key) in process memory. A local user with access to memory can obtain the key. The client also stores the key in encoded form in the Windows Registry and in policy files ('.spd' files). A local user with access to the registry or the policy files can decode the key. Vendor has prepared a fix to be available shortly: http://www.safenet-inc.com/products/vpn/softRemote.asp

---

Category 42.3 *Crypto product implementation flaws*

2006-03-08 **Linux kernel dm-crypt key storage failure vulnerability solution update**

DHS IAIP Daily; http://securitytracker.com/alerts/2006/Mar/1015740.html 23

LINUX KERNEL DM-CRYPT FAILS TO CLEAR KEY STORAGE.

A vulnerability was reported in dm-crypt in the Linux kernel. A local user can obtain information about cryptographic keys. Analysis: The dm-crypt component does not properly clear the crypt_config structure before freeing the structure, which may allow a local user to obtain cryptographic keys. Versions affected: 2.6.15 and prior versions. Solution: The vendor has issued a fixed version (2.6.16-rc1).

Category 42.3 *Crypto product implementation flaws*

2006-04-13 **bank automatic teller machines ATM encryption network vulnerabilities upgrade flaw protocols architecture design**

RISKS; Redspin http://tinyurl.com/er74m 24 26

TRIPLE DES UPGRADES EXPOSE BANK ATM NETWORKS TO COMPROMISE

Redspin, Inc., an audit firm, published a white paper analyzing the unexpected effects of a combination of security upgrades to bank automated teller machine (ATM) networks. In brief, although the original intention of the industry plan was to upgrade DES encryption to Triple DES, additional changes included switching to TCP/IP networks instead of dedicated communications lines. The auditors discovered that the data being sent through the wider bank internal networks includes unencrypted data (except for the PIN): "The card number, the expiration date, the account balances and withdrawal amounts, they all go across the networks in cleartext…." The company's press release stated, "Our biggest concern is that not many bank managers know this," says John Abraham, the company's president. "They assume that everything is encrypted. It's not a terrible assumption, so it's no wonder that most bank managers we've talked to are unhappy to discover this after spending $60,000 to upgrade an ATM."

"Fortunately," continues Abraham, "prevention isn't that complicated, as long as bankers are aware that there is a potential problem. ATM machines need to be kept separate from the rest of the bank's computer network, to try to recreate that direct line to the processor. Also, Redspin is developing a tool to help bankers determine their level of vulnerability. This white paper is all about raising awareness."

Category 42.3 *Crypto product implementation flaws*

2006-05-11 **Linux random number generator vulnerabilities holes paper**

DHS IAIP Daily; http://www.securiteam.com/unixfocus/5RP0E0AIKK.html 23

HOLES IN THE LINUX RANDOM NUMBER GENERATOR

A new paper was recently released which describes holes in Linux's random number generator, as well as a clear description of the Linux /dev/random. The Linux random number generator is part of the kernel of all Linux distributions and is based on generating randomness from entropy of operating system events. The output of this generator is used for almost every security protocol, including TLS/SSL key generation, choosing TCP sequence numbers, and file system and e-mail encryption. Although the generator is part of an open source project, its source code is poorly documented, and patched with hundreds of code patches. This paper presents a description of the underlying algorithms and exposes several security vulnerabilities. Analysis of the Linux Random Number Generator paper: http://www.gutterman.net/publications/GuttermanPinkasReinman 2006.pdf

---

43 I&A products (tokens, biometrics, passwords, Kerberos)

Category 43 *I&A products (tokens, biometrics, passwords, Kerberos)*

2004-06-01 **password-plus identification authentication I&A two-factor theft**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A5693-2004Jun1.html

ARE PASSWORDS PASSÉ?

Scandinavian countries are at the forefront of a movement to ditch conventional asswords in favor of so-called two-factor authentication. These "password-plus" systems use things like disposable cards with scratch-off codes in conjunction with the usual four-digit PIN for online banking and other secure transactions. Each code is used once, and the bank replenishes the supply by sending a new card when the customer is running low. "A password is a construct of the past that has run out of steam," says Identix CEO Joseph Atick. "The human mind-set is not used to dealing with so many different passwords and so many different PINs." Other "password-plus" options include Vasco Data Security International's pocket-sized device that issues a random second code each time you type your regular password in. Or MasterCard International's system, which requires swiping your "smart" credit card through a special reader and entering your PIN to obtain a single-use password good at Office Max, British Airways and a dozen other merchants. And while U.S. banks are well aware of the perils of password theft, they're "all afraid of making the first step," says a Gartner analyst. "They don't want consumers going to other banks because it's too hard." (AP/Washington Post 1 Jun 2004)

Category 43 *I&A products (tokens, biometrics, passwords, Kerberos)*

2005-10-19 **Internet banking identification authentication I&A two-factor regulators government**

RISKS; http://tinyurl.com/cfvjm; http://tinyurl.com/dngl4 24 08

FEDS DEMAND TWO-FACTOR AUTHENTICATION FOR INTERNET BANKING

Federal regulators will require banks to strengthen security for Internet customers through authentication that goes beyond mere user names and passwords, which have become too easy for criminals to exploit. Bank Web sites are expected to adopt some form of "two-factor" authentication by the end of 2006, regulators with the Federal Financial Institutions Examination Council said in a letter to banks last week.

[Abstract by Peter G. Neumann]

43.1 Tokens

Category 43.1 Tokens

2000-10-10 **token smart card identification authentication I&A military government employee**

NewsScan; New York Times http://www.nytimes.com/reuters/technology/tech-smartcard-pentag.html

PENTAGON ROLLS OUT SMART CARD ID
The Defense Department has taken the wraps off its new high-tech security badge, designed to control access to DoD buildings and computer networks. The new ID badge, dubbed a "common access card," features a magnetic strip and two bar codes, and will function as the standard ID for about 4 million people, including active duty military, selected reserve forces, civilian Pentagon employees and eligible contractors. The badge will also include a stored "certificate" that will enable the cardholder to sign digitally such things as e-mail and deployment orders. Although the badges are being hailed by DoD for their ability to enhance privacy through encryption, privacy advocates have voiced fears that the Pentagon could be laying the groundwork for the introduction of a national ID card in the U.S. "The military is frequently used as guinea pigs for proposals that would be too controversial to try among civilians," says David Banisar, senior fellow at the Electronic Privacy Information Center. "Ultimately, the danger is that people could be routinely tracked. Their records could be routinely used for purposes other than those originally intended." (Reuters/New York Times 10 Oct 2000)

Category 43.1 Tokens

2001-10-29 **token-based identification authentication I&A military smart cards**

NewsScan; http://www.washingtonpost.com/wp-srv/aponline/20011029/aponline173744_000.htm

NEW "SMART CARDS" FOR THE TROOPS
Four million U.S. troops and civilian Defense Department employees will be receiving new credit-size "smart cards" that will enable them to unlock doors, get cash, make purchases, check out weapons, and obtain computer and network access. There will be no medical data on the cards. A Pentagon spokesman says that "there's a very limited amount of intrusion into anyone's privacy." (AP/Washington Post 29 Oct 2001)

Category 43.1 Tokens

2002-01-08 **token identification authentication I&A drivers' license registration national identity card**

NewsScan; http://apnews.excite.com/article/20020108/D7GTF1H01.html

'SMART' DRIVERS' LICENSES UP AHEAD
The U.S. Transportation Department is working with the states to develop a new generation of drivers' licenses that contain electronically stored information such as fingerprints or retinal scans. Privacy advocates say the move toward "smart" licenses is really a backdoor way to establish federal ID cards -- an idea that has gained popularity among government officials following the Sept. 11 terrorist attacks. "The debate after Sept. 11 showed that Americans are instinctively suspicious of a single federally issued card, but they might be more sympathetic to identifications issued by businesses or perhaps states," says Jeffrey Rosen, a law professor at George Washington University. "What you're seeing here is a sort of a hardening of the driver's license that could lead to development of a national ID system without creating a national ID card," says Marc Rotenberg, who heads up the Electronic Privacy Information Center. (AP 8 Jan 2002)

Category 43.1 Tokens

2002-02-06 **smart card token consumer profiling data storage identification authentication I&A e-commerce**

NewsScan;
http://www.usatoday.com/life/cyber/tech/review/2002/2/06/smartcard.htm

NEW SMART CARD COULD KNOW EVERYTHING
A San Francisco company called PrivaSys has developed a battery-powered smart card that could be used to replace all the individual credit and debit cards a consumer might carry. The internal chip on the card will be able to store "loyalty" accounts (such as Frequent Flyer data) for a number of different vendors. The company has struck a deal with First Data, but will have to form additional alliances with other credit-processing companies to achieve its plan to make its card the only one you'll need in your purse or wallet. (USAToday 6 Feb 2002)

Category 43.1 *Tokens*

2002-02-27 **personal identification implanted token microchip skin transponder privacy anonymity**

NewsScan; http://www.latimes.com/technology/la-000100545dec19.story?coll=la%2Dheadlines%2Dtechnology

CHIP ID IS ONLY SKIN-DEEP [19 Dec 2001]
Applied Digital Solutions, based in Palm Beach, Florida, is making headlines with plans to become the first company to sell microchips designed to be implanted into humans. One initial target market is likely to be people with artificial limbs and organs -- a user could have up to 60 words of relevant medical information embedded in the chips, which could then be read by medical personnel if the patient were brought unconscious into an emergency room. With rollout in South America scheduled in about 90 days, another potential market is potential kidnap targets who could use the chips in combination with GPS devices to alert security personnel to their whereabouts. Future plans call for ordinary people to use the chips as the ultimate ID, supplanting the functions now performed by passwords and keys. "I'd be shocked if within 10 years you couldn't get a chip implanted that would unlock your house, start your car and give you money," says Chris Hables Gray, author of "The Cyborg Citizen." And lest you think it unlikely that you'd want to try something like this out, futurist Paul Saffo reminds us, "As some people wring their hands about the invasion of privacy and civil liberty, a whole other generation is going to go, 'Cool! I've always wanted to embed technology in my body.' It's going to be fashion. One sure sign that teenagers will love it is if it terrifies their parents." (Los Angeles Times 19 Dec 2001)

CHIP IMPLANT COMPANY SEEKS FDA APPROVAL [27 Feb 2002]
A Florida company that has developed a computer ID chip suitable for implanting in the human body has applied to the Food and Drug Administration for approval of its product. The VeriChip, as it's called, can be used to store information, such as medical records, which could be accessed by emergency medical personnel in the event of an accident. Applied Digital Solutions says it plans to limit its marketing of the VeriChip to companies that ensure its human use voluntary. A person or intermediary company would buy the chip for about $200 and have it encoded with the desired information. The person seeking the implant would then take the chip -- about the size of a grain of rice -- to a doctor, who would insert it under the skin with a large needle device. Meanwhile, privacy advocates have expressed doubts about the VeriChip: "The problem is that you always have to think about what the device will be used for tomorrow. It's what we call function creep. At first a device is used for applications we all agree are good but then it slowly is used for more than it was intended," says Lee Tien, an attorney for the Electronic Frontier Foundation. (AP Feb 27 2002)
http://apnews.excite.com/article/20020227/D7HUDV3O0.html

Category 43.1 *Tokens*

2002-03-21 **identification and authentication I&A terrorism national security**

Technology Review http://www.technologyreview.com/articles/garfinkel0402.asp

Simson Garfinkel wrote a penetrating analysis of the tenuous link between I&A (identification and authentication) and national security. The driver's license has become a _de facto_ form of I&A, used by banks, airlines, bars and innumerable other organizations. Various state governments and non-governmental groups have proposed adding biometric authentication to the usual picture. But Garfinkel concludes his analysis with the following sensible comments: "Like the FBI, which tucked a laundry list of new powers into the [U.S.A.P.A.T.R.I.O.T.] Act of 2001, the American Association of Motor Vehicle Administrators and the Department of Transportation are using the terrorist attacks as a convenient excuse for deploying a national identification system that would have been politically untenable this time last year. Remember, even if the September 11 terrorists had been carrying smart-card-enabled driver's licenses with biometric authenticators, they still would have been allowed to board their flights. American Airlines knew Richard Reid's identity-it just didn't know that he had plastic explosives concealed in his shoes. Forcing every American to carry a new state-issued identification card may cut down on illicit drinking and make things easier for police at traffic stops, but it is simply not a rational way to deal with the specter of terrorism. Better identification systems won't do much to stop people who have evil in their hearts but not in their history."

Category 43.1 *Tokens*

2002-03-29 **homeland security identification authentication I&A biometrics smart cards airports**

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/2955860.htm

'SMART CARD' FOR FREQUENT FLIERS
EDS, Maximus, and other high-tech companies are racing to capture the emerging market for "smart cards" that will allow frequent fliers to speed through air security checkpoints after they submit to retina or hand scans. Promoters of the systems believe that "trusted traveler" programs like these not only add to customer convenience but also enhance security, by providing (in the words of an EDS executive) "better knowledge of the people getting on the airplane." Civil libertarians are skeptical, and Barry Steinhardt of the American Civil Liberties Union worries that the use of such systems would "encourage security personnel to put their guard down" and that terrorists would just obtain phony documents. But Rachel Rowland of Maximus says, "It's far easier for someone to get a fake driver's license. With these cards, nobody else is going to have the same digital map of your fingerprint." (AP/San Jose Mercury News 28 Mar 2002)

Category 43.1 *Tokens*

2002-04-09 **homeland security terrorism I&A identification authentication identity cards travelers airports**

NewsScan; http://www.nytimes.com/2002/04/09/technology/09PASS.html

CAN YOU TRUST A "TRUSTED TRAVELER"?
One proposal for improving airport security has been the creation of hard-to-counterfeit "trusted traveler" ID cards for frequent travelers, but software developer Richard P. Eastman asks the obvious question: "What makes a trusted traveler? The guy who travels all the time; who travels on business; who has a reason to travel. Does that mean the terrorist can't penetrate that group? Of course he can." Beyond objections of that sort, civil libertarians have been arguing that ID cards for travelers will set a dangerous precedent. Barry S. Steinhardt of the American Civil Liberties Union predicts, "Quickly enough, policy makers are going to say, 'If this works, let's require everyone to go through background checks before they get on a plane.'" (New York Times 9 Apr 2002)

Category 43.1 *Tokens*

2002-08-09 **I&A identification authentication wireless card surveillance monitoring**

NewsScan; http://www.nytimes.com/2002/08/08/technology/08SECU.htm

WIRELESS SECURITY SYSTEM FOR AIRPORT RAMP AREAS
The new federal Transportation Security Agency is giving $1 million in R&D funds to the Hackensack, NJ company ID Systems, to determine whether a wireless surveillance-and-control system designed for tracking vehicles in car factories can be adapted for airports. "You can't have an airline employee walk around with 200 keys, for all the 200 vehicles," says the head of ID Systems -- so the company has developed a vehicle control system called Wireless Asset Net. To use an airport vehicle on the tarmac, an employee would have to enter an ID card into a reader to obtain authorization from a central computer. (New York Times 8 Aug 2002)

Category 43.1 *Tokens*

2002-10-17 **I&A identification authentication e-commerce token**

NewsScan;http://news.bbc.co.uk/1/hi/technology/2334491.stm

QUIZID TARGETS DIGITAL AUTHENTICATION
U.K. firm Quizid Technologies has launched a credit-card-sized device that is being heralded as a major breakthrough in the search for greater security for Internet-based transactions. Users are issued a card and a personal code, based on a set of color keys on the card. Each time the user wants to complete a transaction, he or she punches in the color code and a random number is generated. The card works in conjunction with the Quizid vault — a bank of computers that can process 600 authentications per second. Security experts welcomed the new device: "Without an architecture of trust more sophisticated than a PIN or password, the U.K. is definitely not in danger of becoming a first-world knowledge-based economy," says security analyst Simon Moores. (BBC News 17 Oct 2002)

Category 43.1 *Tokens*

2002-10-23 **implantable radio wireless transponder chip identification authentication I&A**

NewsScan

FDA APPROVES IMPLANTABLE ID CHIP
In a surprise move, the Food and Drug Administration okayed the use of implantable ID chips in humans, providing they are used for "security, financial and personal identification or safety applications." The FDA has still not ruled on whether the VeriChip, made by Applied Digital Solutions, can be used for medical purposes, however. The company has promoted the device in the U.S. for its ability to provide detailed medical history data in cases where the patient is unable to communicate with emergency room personnel. Applied Digital president Scott Silverman says he's happy with the FDA's decision: "We'll now go into high gear with our sales, marketing and distribution plans in the U.S.," adding that the company will focus on the security and ID aspects of the chip, at least for the time being. Meanwhile, Leslie Jacobs, whose family volunteered to "get chipped" last May, says she's still hoping the FDA will approve the VeriChip for medical use. Both her husband and son have ongoing health problems. (Wired.com 23 Oct 2002)
http://www.wired.com/news/politics/0,1283,55952,00.html

Category 43.1 *Tokens*

2005-02-15 **key car house RFID radio freqency identifier hack future prediction**

NewsScan; http://www.usatoday.com/tech/news/2005-02-15-nokey-usat_x.htm

A KEYLESS FUTURE

Some luxury vehicles don't have an ignition key slot anymore and residential-door hardware companies are marketing push-button entry systems for homes. Kevin Kraus of the door hardware company Schlage says, "In 10 to 20 years, the key will be nothing but a backup device." Cars offering keyless systems include the Lexus GS sport sedan, Cadillac XLR and STS, Mercedes-Benz S-Class and Chevrolet Corvette. Although Johns Hopkins University researchers recently reported they were able to hack their way through radio-frequency security codes on cars, Texas Instruments (one of the makers of radio-frequency equipment) says it has never had a security breach. Gale Johnson, editor of the trade publication Locksmith Ledger comments, "The mechanical key is disappearing. Locksmiths today are a little like a buggy maker in 1900." (USA Today 15 Feb 2005)

Category 43.1 *Tokens*

2005-02-17 **identification authentication I&A RFID radio frequency identification device passport counter-terrorism border security data leakage confidentiality**

RISKS; http://www.economist.com/science/displayStory.cfm?story_id=3666171 23 73

HIGH-TECH PASSPORTS ARE NOT WORKING

Yves Bellefeuille reports on an article in _The Economist_:

The usual arguments are made -- the technology isn't reliable, there will be too many false positives, and so on -- but there's also a new argument I hadn't seem before:

"The data on these chips will be readable remotely, without the bearer knowing. And -- gain at America's insistence -- those data will not be encrypted, so anybody with a suitable reader, be they official, commercial, criminal or terrorist, will be able to check a passport holder's details...

"Passport chips are deliberately designed for clandestine remote reading. The ICAO [International Civil Aviation Organisation, a UN agency] specification refers quite openly to the idea of a "walk-through" inspection with the person concerned "possibly being unaware of the operation"."

Apparently, the only country that's ready for the US requirements is Belgium. It's really the *only* country: the US itself won't be able to deal with the passport requirements it's imposing on others by the November 2005 deadline!

Category 43.1 *Tokens*

2005-10-15 **identification authentication token I&A**

RISKS; http://cingular.com/voicemail_west 24 08

HAVING YOUR PHONE IS A CINGULAR TOKEN OF IDENTITY

Effective 26 Oct 2005, Cingular is switching to a new voicemail system for all its customers. One of the "features" is "Skip Password"--apparently, one will no longer need to enter a password if one has physical access to a handset. The option to continue to use a password will still be available, but "skip password" appears to be the default.

[Abstract by Steve Fenwick]

Category 43.1 *Tokens*

2006-05-02 **two-factor authentication chip-and-PIN credit card transactions fraud**

RISKS 24 28

TWO-FACTOR "CHIP-AND-PIN" CREDIT CARDS MAY BE SUBJECT TO FRAUD

Nick Rothwell reported on a developing story from Britain, where SHELL UK withdrew the new "chip-and-PIN credit card payment facilities from 160 of their garages, following incidents of fraud." Rothwell wrote, "In this particular case, it appears that the card terminal devices designed by Trintech, although tamper-resistant (i.e. will fail to operate if tampered with), were tampered with to commit the fraud. Trintech are claiming that their equipment is not at fault, and the issue is one of the "environment" in which they were installed." He added, "According to [BBC Radio 4's news program] You and Yours, there have been previous incidents of chip-and-PIN fraud where unscrupulous retailers were able to add items to a customer's bill after the payment transaction."

43.2 Biometrics

Category 43.2 *Biometrics*

1997-04-15 **biometric speech identification authentication**

PR Newswire

The Speech Recognition API Committee announced release of the Speaker Verification API Specification (SVAPI), version 1.0. This specification helps developers working on speech recognition and authentication. See <http://www.srapi.com/svapi> for details.

Category 43.2 *Biometrics*

1998-01-05 **biometric authentication face**

Business Wire

Facial recognition systems from Miros, Inc. passed the one-millionth face in January. More than one million faces have been identified worldwide using the system.

Category 43.2 *Biometrics*

1998-05-01 **biometric authentication iris scan ATM bank identification**

RISKS 19 71

British banks began installing iris-scanning devices at ATMs for positive identification and authentication of customers.

Category 43.2 *Biometrics*

1998-07-09 **biometric identification authentication fingerprint camera**

EDUPAGE

Compaq's new Fingerprint Identification Technology unit, about the size of a deck of cards, was the least expensive unit produced so far. At $99, it could significantly improve identification and authentication even for PCs. It would certainly be an improvement over passwords, which are notoriously poorly chosen and managed by practically everyone.

Category 43.2 *Biometrics*

1998-08-18 **biometrics identification authentication typing rhythm**

EDUPAGE

IT'S THE "TOUCH" IN TYPING THAT'S IMPORTANT
Canadian Web filter maker Net Nanny will begin testing "biopassword" technology on its Web site, with future plans calling for including it in their smut filters, incorporating it into office software, and licensing it to the security and automobile industries. The company bought the rights to the technology, which was developed at the Stanford Research Institute, in 1989. Biopassword technology records not only how you type your password, but also exactly how you do it, blocking would-be intruders who steal passwords but don't have the same keyboard touch as the legitimate password-holder. "I once drank three pints of beer in an hour," says Net Nanny CEO Gordon Ross. "My rhythm didn't match, and I was denied entry to my computer, because I was impaired." So then what? "When it ships, it will have a manual override," says Ross. (St. Petersburg Times 17 Aug 98)

Category 43.2 *Biometrics*

1998-11-17 **biometric authentication laptop access control**

Computer Reseller News
http://www.techweb.com/printableArticle?doc_id=TWB19981117S0009

Hewlett Packard announced that its laptop computers would include options for fingerprint scanning in 1999. In addition, HP was examining other biometric authentication systems such as voice recognition and iris scanners.

Category 43.2 *Biometrics*

1999-01-01 **forensic database ear prints criminals suspects evidence**

PA News

Scientists in Britain established the uniqueness of ear-cartilage patterns and successfully prosecuted a burglar who put his ear to a window to detect sounds in the home he burgled. The thief murdered a 94-year-old woman and was consequently sent to prison for life. The police authorities had gathered 1200 ear prints from volunteers by the end of 1998 and were hoping to begin collecting ear prints from suspects. The officer in charge of the project was John Kennerley, Chief Fingerprint Officer with Lancashire police; his work was based on pioneering research by Cor Van Der Lugt of the Netherlands.

Category 43.2 *Biometrics*

1999-07-01 **biometric identification authentication I&A fingerprint scan banking financial transactions**

EDUPAGE; Future Banker

FINGERPRINTS AS PASSWORDS: TWITCHING TO TAKE HOLD IN INDUSTRY

Fingerprint scanning technology should be gradually implemented by the banking industry as a means of verifying identity, says Identix CEO Randall Fowler. Identix, a leader in image scanning technology, produces biometrics products capable of distinguishing between an actual fingerprint and a photo of one. Fowler stresses the need for fingerprint scanning technology, noting that financial transactions no longer occur face to face, but "between two strangers with a piece of silicon in between them." He says, "Somebody has to give the silicon the ability to recognize who it's dealing with, particularly in the banking industry." In line with providing this technology, Identix and Motorola recently formed a partnership to develop biometrics devices that will eliminate the need to use PIN numbers in accessing a banking network. Motorola's Digital DNA unit has reduced the size of its CMOS-chips that store fingerprint optics, so the chips can be attached to the side of phones, cash registers, ATMs, and other devices. Fowler says financial institutions are likely to adopt biometrics technology slowly, as they replace computer systems. (Future Banker 07/99)

Category 43.2 *Biometrics*

1999-11-15 **biometric identification authentication I&A fingerprint bank Internet Web**

PRNewswire

SecuGen Corporation, SAFLINK Corporation, and ING Direct Canada announced plans for a fingerprint biometric security system for ING Direct's Internet banking products. Customers will use a finger-print recognizing computer mouse for identification and authentication.

Category 43.2 *Biometrics*

1999-11-17 **biometric authentication signature face fingerprint**

Computer Reseller News

At the 1999 Fall Comdex, several companies introduced new or refined versions of their biometric authentication products. Bionetrix <http://www.bionetrix.com/> announced a new infrastructure for integrating a wide range of I&A products. Visionics <http://www.faceit.com/> continued to improve its facial recognition systems. CompuLink Research <http://www.clrusa.com/contactus.htm> announced its new U-Match fingerprint-reading mouse.

Category 43.2 *Biometrics*

2000-05-03 **biometric identification and authentication I&A fingerprint scanner personal computers**

NewsScan, Los Angeles Times
http://www.latimes.com/business/20000503/t000041568.html

Microsoft says it plans to incorporate biometric technology in its Windows software that will enable users to sign on by brushing their fingertips across a scanner rather than typing in a password. Biometric technology scans the details of a person's fingerprints, iris patterns, facial structure or other physical characteristics and compares them against a database of stored user information. The company will use authentication technology from I/O Software Inc. (Reuters/Los Angeles Times 3 May 2000)

Category 43.2 *Biometrics*

2000-06-13 **intellectual property distribution encryption biometric I&A identification & authentication**

NewsScan, New York Times http://news.cnet.com/news/0-1005-200-2066437.html

Musicrypt.com and Net Nanny Software are teaming up to market an advanced "biometric" identification technology that would block would-be cyberpirates from distributing music free over the Net. In a new twist, the software identifies individual music listeners by the way they tap out letters on computer keyboards. This information is then used to protect songs against unauthorized distribution and use. The companies are hoping that music labels or online retailers will insert the technology into downloaded music, so that only a person who buys a given song would be able to play it on a computer. Identifying the buyer by these keystroke patterns is far more secure than using passwords, which can be passed on to thousands of people, the companies say. "What we're doing with (this software) is making the user the key," says John Heaven, Musicrypt's chief executive. One biometrics industry analyst notes that the keystroke technology is less accurate than other technologies such as fingerprinting or retinal scans, but it makes up for that weakness in its relative ease of use: "I would say that biometrics in general are ready for the consumer level. I wouldn't have said that two years ago. It would have been a disaster then." (News.com 13 Jun 2000)

Category 43.2 *Biometrics*

2001-07-31 **voice synthesis recognition biometric authentication I&A vulnerability**

NewsScan

VOICE CLONING
AT&T Labs has created new text-to-voice software that makes it possible for a company to use recordings of a person's voice (for example, John F. Kennedy's) to utter life-like statements that they never made. Priced in the thousands of dollars and called "Natural Voices," the software could be used by telephone call centers and other such activities. An AT&T executive said: "If ABC wanted to use Regis Philbin's voice for all of its automated customer-service calls, it could." Issues sure to arise include disputes over voice-licensing rights and measures to prevent fraudulent uses. One potential client for the software noted: "Just like you can't trust a photography anymore, you won't be able to trust a voice either." (New York Times 31 Jul 2001)
http://www.nytimes.com/2001/07/31/technology/31VOIC.html

Category 43.2 *Biometrics*

2001-10-01 **biometric identification authentication I&A e-commerce fingerprint recognition**

NewsScan

PUTTING A FINGER ON E-PAYMENTS

Indivos, an Oakland, Calif. firm, has developed software that uses fingerprint scanners to process electronic payments of all kinds. "We're putting this in front of the mainstream consumer," says a company spokesman. "You won't need cash or cards to pay for anything. All you need is your finger and you never leave home without it." Indivos has partnered with fingerprint sensor manufacturer Digital Persona to test the service at a "major fast food chain" in California and supermarkets throughout the country. Fingerscans, which are the leading biometric application, will represent 33% or $300 million of the market by 2006, according to Frost & Sullivan. (Wired.com 1 Oct 2001)
http://www.wired.com/news/business/0,1367,47127,00.html

Category 43.2 *Biometrics*

2001-10-26 **biometric face recognition surveillance terrorism airport security privacy**

NewsScan

BOSTON'S LOGAN AIRPORT TO USE FACE-RECOGNITION SYSTEM
Boston's Logan Airport, where the September 11th terrorists boarded planes they hijacked for their attacks on New York and Washington, has decided to install face-recognition technology to scan the faces of travelers and compare them against a computerized database of suspected terrorists. The American Civil Liberties Union has opposed the technology, calling it intrusive and ineffective. (AP/USA Today 26 Oct 2001)

Category 43.2 *Biometrics*

2001-11-01 **face recognition biometric identification authentication**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A20852-2001Oct31.html

THE FACE-RECOGNITION SOFTWARE MARKET
Since the September 11th terrorist attacks, face-recognition technology has been given a much friendlier reception than it did when it was introduced at the last Super Bowl game or at Tampa early this year. Now, Visionics and Viisage, the two major companies in that industry, are engaged in fierce competition for dominance in a market expected to grow from $200 million in revenue this year to $2 billion in 2004. Face-recognition systems compare digital translations of a person's facial characteristics to images in a database of suspected terrorists and criminals. Critics of the technology insist that its use is likely to be expanded into uses beyond the apprehension of evil-doers, and argue that it is not always accurate. In response, advocates for the technology admit that it is "not as precise as fingerprints" but insist that occasional "false positives" can easily be resolved by local authorities. (Washington Post 1 Nov 2001)

Category 43.2 *Biometrics*

2001-11-08 **fingerprint recognition biometric identification authentication I&A**

NewsScan; http://interactive.wsj.com/articles/SB1005172330856003280.htm

REPLACING PASSWORDS WITH FINGERPRINTS

A new fingerprint-recognition device called U.are.U could soon eliminate the need to remember passwords for accessing restricted Web sites, making it as easy as the touch of a finger. The $69 system, from Silicon Valley-based DigitalPersona, is aimed at consumers and small businesses, and designed to work with systems running Windows XP. Once the device has been "trained" to recognize a fingerprint, all the user has to do is type his or her user ID and password for each secure Web page into the software that controls the fingerprint module. From then on, access will be granted just by tapping the device. U.are.U can also encrypt certain files or folders on the PC so that they can be read only by designated people. (Wall Street Journal 8 Nov 2001)

Category 43.2 *Biometrics*

2002-01-03 **biometric face recognition identification authentication surveillance screening**

NewsScan; http://www.siliconvalley.com/docs/news/svfront/026914.htm

DIGITAL PHOTO DATABASE TO CONFIRM IDENTITY OF FOREIGN TRAVELERS
The U.S. State Department will soon begin comparing foreign travelers' faces with digitized photographs to confirm that individuals shown in their travel papers are the same persons who actually applied and were approved for admission to this country. And new legislation being considered in Congress would require biometric identifiers on passports issued by a number of countries, including Japan and most of Western Europe, that are in the visa-waiver program. (San Jose Mercury News 3 Jan 2002)

Category 43.2 *Biometrics*

2002-01-19 **biometrics database linkage privacy**

RISKS 21 87

Ben Rosengart noted the following:
>*Time Magazine* is reporting that the federal Department of Transportation, by instruction of the Congress, is working to link together the states' driver databases, and also to introduce biometric security on drivers' licenses.

http://www.time.com/time/nation/article/0,8599,191857,00.html

RISKS include false arrest due to database screwups, abuse for personal reasons by government personnel, abuse by the government itself, all the RISKS known to be associated with biometrics, disclosure of the databases to the public, and probably much, much more.<

Category 43.2 *Biometrics*

2002-01-20 **I&A identification authentication biometrics face recognition anti-terrorist homeland security airport**

Security Wire Digest 4 5

PALM BEACH AIRPORT PILOTS NEW BIOMETRICS PROGRAM
Palm Beach International Airport is scheduled this week to begin a 90-day pilot program that scans passengers' faces and then compares the images to a database of the country's most wanted criminals. Using technology by Miami-based ACT Systems Integrators, the program uses facial recognition technology to flag suspected terrorists, and has the capacity to compare images with up to 30,000 photographs of known criminals. If a match isn't found, the passenger's image is discarded. The American Civil Liberties Union is against the measure, believing it too intrusive and saying it violates individuals' right to privacy. The airport already uses biometrics for new employees, who must undergo fingerprint scans that are compared to a FBI database of known offenders. Current employees also will undergo the facial scanning.

Category 43.2 *Biometrics*

2002-01-25 **biometric face recognition I&A identification authentication airport security**

RISKS 21 89

Iceland's main airport will have face recognition systems installed. Chris Leeson notes in RISKS that this can work only for known faces and he hopes that the security staff will not come to rely mainly on the system.

Category 43.2 *Biometrics*

2002-02-18 **token smart card identification authentication I&A immigration government identity thumbprint fingerprint recognition biometrics**

NewsScan; http://www.nytimes.com/2002/02/18/technology/18KONG.html

HONG KONG TO USE DIGITAL ID CARDS

Hong Kong is planning to introduce an identity card with an embedded digital chip containing a replica of the cardholder's thumbprint, for matching against an optical reader at border crossings into China. "You don't have to have an immigration officer there to look at the card," says an immigration official in Hong Kong. "It's just a self-service kiosk." Besides verification of identity, the chip could be made to include medical, financial, and other data on an individual, but at least for now the card will contain only basic information. Sin Chung-kai, a pro-democracy member of the Hong Kong legislature, says: "We're not opposed to people having to carry ID cards. The crux of the controversy is how much information should be stored on the card... If I were a film star and I had some kind of disease, I wouldn't want it to be on my ID card. I also wouldn't want the ID to be my cash card. I don't want my spending traced." (New York Times 18 Feb 2002)

Category 43.2 *Biometrics*

2002-05-17 **biometric authentication I&A identification fraud simulation fingerprint**

NewsScan;
http://news.bbc.co.uk/hi/english/sci/tech/newsid_1991000/1991517.stm

'GUMMY' FINGERS FOOL FINGERPRINT SECURITY SYSTEMS

A Japanese engineering professor has managed to trick biometric security systems using artificial fingers made with gelatin. In addition to creating a fingerprint by pushing a finger into a malleable plastic mixed with gelatin, the researchers were able to create credible fingers using fingerprints lifted from a glass. First, the latent print was hardened, using glue that sticks to the ridges of the fingerprint. The hardened print was then photographed, using a digital camera, and enhanced using Adobe Photoshop software to create heightened contrast between the ridges and gaps. The image was then transferred to a photosensitive sheet, etched into copper and used to create another mold. Both methods resulted in a fake finger that was able to fool a variety of biometric readers 80% of the time. Security experts say the experiments cast serious doubt on any claims that this type of biometric system can be made fully secure. (BBC News 17 May 2002)

Category 43.2 *Biometrics*

2002-05-20 **biometric I&A identification authentication fake fraud simulation**

Security Wire Digest, Crypto-Gram 4 39

BIOMETRICS FAIL STICKY TEST
Biometrics companies found themselves in a sticky situation recently when a Japanese researcher demonstrated how a fake finger formed with gelatin fooled fingerprint readers an average 80 percent of the time. Tsumtomu Matsumoto, a graduate student at Yokohama National University, presented a study at an IT conference last week showing scanners' vulnerability. Using the same ingredients found in Gummi Bear candies, Matsumoto created a fake fingerprint modeled after an authorized user's in less than an hour. Though that method requires the user's permission, the researcher demonstrated another by lifting a legitimate user's print off a surface, digitally enhancing it on a computer and printing it on a transparent sheet. The imprint is then etched to create a fingerprint impression later filled with gelatin, which when cooled creates the same impression as the earlier gummy finger. Both types fooled 11 different detectors 70 to 90 percent of the time.

Category 43.2 *Biometrics*

2002-05-24 **homeland security facial recognition biometrics surveillance I&A identification authentication privacy surveillance**

PoliTech

A press release from Visionics Corp in May 2002 included the following description of a trial of their facial recognition equipment:

>Visionics Corporation (Nasdaq: VSNX), the worldwide leader in identification technologies and systems, announced today that its latest FaceIt® ARGUS surveillance system will be used to augment security measures at the Battery Park Screening Facility in the ferry embarkation area to Ellis Island and the Statue of Liberty in the New York harbor during this Memorial Day holiday weekend.

The state of the art system is on loan from Visionics to the United States Park Police for the holiday weekend and is part of a series of stepped up security measures that will be visible at New York City landmarks.

Major Thomas H. Wilkins of the United States Park Police commented, "Since the tragic events of September 11, our agency has been focused on preventing future attacks while ensuring everyday life remains as uninterrupted as possible. Ellis Island and the Statue of Liberty are potent symbols of our country's freedoms and it is our mission to make these landmarks safe for visitors and tourists."

The installation of FaceIt® ARGUS at Battery Park Screening Facility will encompass the security portal area that precedes the ferry boarding planks. The system will automatically scan all faces passing through the entryway and compare them against a database of known terrorists compiled by federal authorities. The installation will be in compliance with Visionics' privacy principles---signage informing the public that the system is in use is posted in corresponding areas and all non-matches are automatically deleted from the system.<

Category 43.2 *Biometrics*

2002-05-27 **I&A identification authentication biometrics facial recognition airport homeland security**

RISKS 22 10

Peter G. Neumann summarized an experimental failure:

The face recognition system in experimental use at Palm Beach International Airport on 15 volunteers and a database of 250 snapshots. The success rate is less than 50%. Extrapolations also suggest a false-positive rate of about 50 passengers a day for a single checkpoint handling 5,000 passengers. "Eyeglasses gave the system a great deal of difficulty, in spite of copious Visionics marketing hype denying this particular glitch. Small rotations of the head, fifteen to thirty degrees off the camera's focal point, also bamboozled it repeatedly, and the lighting had to be just right."
http://www.theregister.co.uk/content/55/25444.html

Category 43.2 *Biometrics*

2002-05-30 **facial recognition biometrics I&A identification authentication civil liberties surveillance privacy**

NewsScan; http://www.aclu.org/news/2002/n052402a.html

ACLU BLASTS USE OF FACE RECOGNITION SYSTEMS
The American Civil Liberties Union (ACLU) has issued a stinging criticism of the use of computer-based face recognition systems to aid in the war against terrorism. ACLU official Barry Steindardt says: "To have such a system in place near the Statue of Liberty -- our nation's beacon of liberty -- is both ironic and disheartening. It may be a good sales stunt for the manufacturer, but it is an insult to the American people and to those in law enforcement who truly know how to keep us safe." The ACLU's position is that the system has a high rate of "false positives" that wrongly match people with photos of others, thereby subjecting people to "being pulled aside for intrusive searches and security checks." (ACLU 24 May 2002)

Category 43.2 *Biometrics*

2002-07-25 **biometric identification authentication I&A shopping**

NewsScan

ONE-FINGER CHECKOUT AT GROCERY STORES
At various locations around the country grocery store chains are testing new technology that allows shoppers to pay for purchases simply by putting a finger on a screen that records not a full fingerprint but a digital image, or template, of certain key elements of that fingerprint, such as where lines intersect or end. The encrypted information is then matched to the customer's credit card, debit card or checking account information, as well as to any frequent-shopper "loyalty" card. Shoppers so far seem to be accepting the new technology (and feel that it provides an additional level of security), but Carlene Thissen of Retail Systems Consulting fears a possible consumer backlash over privacy concerns: "Like iris scans, retinal scans or even voice recognition, when it's attached to your body like that, there might be more of a reaction." If the new finger payment technology proves itself in grocery stores, you can expect to see it eventually used by fast food chains, video rental companies, pharmacies, and airline and hotel check-in desks. (New York Times 25 Jul 2002)

Category 43.2 *Biometrics*

2002-07-29 **biometric identification authentication I&A fingerprint hand geometry iris voice cards**

NewsScan; http://apnews.excite.com/article/20020728/D7L26PGO0.htm

MILITARY ID GOES HIGH-TECH

The U.S. Defense Department is developing high-tech identification cards that will encode information about the bearer's fingerprints and other unique physical characteristics, such as hand shape, iris pattern, or voice print. The next-generation cards would add another level of security by requiring computer users to log in using their ID card and password and then undergo an additional biometric scan to verify their identity. Current ID cards that are used to log on to military computer systems contain a computer chip that holds the owner's name, rank and serial number. (AP 28 Jul 2002)

Category 43.2 *Biometrics*

2002-10-21 **I&A identification authentication voice recognition biometrics**

NewsScan

VOICE-AUTHENTICATION
A voice-authentication system developed the Mountain View, CA. company Vocent will be used to help Visa International verify the unique identity of employees making password changes and customers making online purchases. Vocent says that the system, which stores a person's digital voiceprint that can be accessed over the Internet, will help Visa set new standards for online or mobile voice-verification for use by thousands of Visa's member banks. A number of other companies are also developing voice recognition or authentication technology for this and other purposes. (San Jose Mercury News 21 Oct 2002)

Category 43.2 *Biometrics*

2002-11-06 **I&A identification authentication biometrics iris scan**

NewsScan

THE EYES HAVE IT IN NEW IDENTIFICATION SYSTEMS
Iris-recognition systems developed by Iridian Technologies of Moorestown, NJ, are being used now in Pakistan to detect Afghani refugees who have been returning multiple times for United Nations aid, straining the UN's resources. It is one of the largest real-world tests of the Iridian technology; another major test this year has been in Saudi Arabia, where the technology was used to monitor about 25,000 pilgrims making the haji, or journey to Mecca. (KRT/San Jose Mercury News 6 Nov 2002)

Category 43.2 *Biometrics*

2003-01-09 **biometric iris scanner I&A identification authentication authorization**

NewsScan

RETINAL SCANNING AT U.K. SCHOOL
The Venerable Bede school in London will use advanced eye-recognition software to determine which students are to be billed for their lunches and which may eat for free because they are poor. The school decided to use the technology to protect poor children from being ridiculed by the more well-off children. [As an historical aside, it might be noted that the concern for poor would probably please the school's namesake. Venerable Bede, the 8th century monk best known for his history of ecclesiastical history, said on his deathbed: "I have a few treasures in my box, some pepper and napkins and incense. Run quickly and fetch the priests of our monastery, and I will share among them such little presents as God has given me."] The school's headmaster said that the software will also be used in the library for book check-out and return but added: "This is not a James Bond school for spies... This is not science fiction. This is technology that exists." (USA Today 9 Jan 2003)

Category 43.2 *Biometrics*

2003-03-10 **biometric I&A identification authentication facial scanning recognition**

NewsScan

FACE SCANNING TECHNOLOGY GOES 3D
A pair of identical whiz-kid twins in Israel have developed a face-scanning system that can even tell them apart. Unlike the two-dimensional scanning technologies now in use in some cities and airports, the 3D system maps the surface of a person's face by scanning it with a series of light patterns and stores the data as a three-dimensional image in a computer. The system uses a mathematical algorithm to measure the distances between a number of sample points on the facial surface, and the distances are then reconfigured as straight lines in a 3D space, creating a new and abstracted image based on precise mathematical calculations. "One of my students calls it sculpting in numbers," says Ron Kimmel, a professor at the Technion Institute in Haifa. "This kind of mapping makes it all invariant, or it is not influenced by our expressions. If we smile a little bit or we change our face a little, it will still be mapped into the same signature, the same kind of surface." Analysts say facial signatures could be embedded in credit cards, building entry permits, or even ATM cards. The facial recognition project began as an assignment in Kimmel's class, where he promised the twins that if they developed a system that could distinguish them, he'd give them a grade of 100. (Reuters 9 Mar 2003)

Category 43.2 *Biometrics*

2003-07-22 **biometric unready new techonology**

NewsScan

BIOMETRICS TECHNOLOGY: NOT YET READY FOR PRIMETIME
Gartner Research director Anthony Allen told guests at the launch of European Biometrics Forum that while widespread use of biometrics was likely by 2008, the technologies still had some kinks to be ironed out. Biometrics, which includes technologies used for voice, face, iris and fingerprint identification systems, is virtually useless without adequate back security measures and databases, said Allen, and current systems have several fallibilities that must be corrected. For instance, evidence shows that wearing eyeglasses can fool an eyescanner, prosthetic makeup can confuse face scanners, a sore throat can change a voice print and breathing heavily on a fingerprint scanner can make prints unrecognizable. However, newer generations of technology are beginning to rectify some of these shortcomings; the latest fingerprint scanners now incorporate methods of detecting body heat and blood flow and can scan below the surface later, making it more difficult to deceive. (The Register 22 Jul 2003)

Category 43.2 *Biometrics*

2003-08-24 **biometrics foreign visitors travel visa airplace citizen alien**

NewsScan

BIOMETRIC SCANS FOR U.S. VISITORS
Biometric face and fingerprint scans for travelers will become routine security measures for foreign visitors next year. By October 2004 the 27 countries whose citizens can travel to the U.S. without visas must begin issuing passports with embedded computer chips with the traveler's facial identification. Civil libertarian Marc Rotenberg of the Electronic Privacy Information Center opposes the mandate: "Our government has forced on European governments the obligation to adopt biometric identifiers though most in the U.S. still oppose such systems." But Kelly Shannon of the State Department argues that is not only "more secure for other countries, it's more secure for us. The idea is that it is contingent on reciprocal treatment for United States citizens." And Denis Shagnon of the International Civil Aviation Organization adds: "What was required was a globally interoperable biometric — one biometric that could be used worldwide and can be read worldwide." He regards the biometric techniques as "very user-friendly" and "unobtrusive." (New York Times 24 Aug 2003)

Category 43.2 *Biometrics*

2003-12-29 **fingerprint terrorist indentify people employment ID biometrics**

NewsScan

'NOT YOUR FATHER'S FINGERPRINT'

The biometrics industry — spurred on by heightened terrorist concerns — has rolled out a variety of new ways to identify people, ranging from retina and iris scans to mapping voice patterns or walking styles, but there's a clear winner among the competing technologies — the old-fashioned fingerprint. "They are looking for proven technology that's stable and familiar," says Joseph J. Atick, CEO of biometric firm Identix. "It's not about technology. It's about lowering your deployment risk." But these aren't your father's fingerprints — today's equipment does away with messy ink in favor of digital records, created by software when fingers are pressed against an electronic pad or sensitive photoplate. And often as not, the fingerprints are then combined with some other form of biometric ID, such as facial recognition. Meanwhile, growing use of passports, drivers' licenses and employment ID cards embedded with ID-data microchips is spawning a new business for data processing giants such as IBM, Unisys and Siemens. "The technology (to integrate ID data with public records) is advancing rapidly. The big growth will be in 2005 and 2006," says a Unisys official. (New York Times 29 Dec 2003)

Category 43.2 *Biometrics*

2004-02-17 **biometric authentication passports air travel Europe**

NewsScan

FINNISH GROUP GETS FIRST ORDER FOR BIOMETRIC PASSPORTS

Finland's Setec has received its first order for 3 million passports containing the new biometric technology required by the International Civil Aviation Organization and the U.S. government. U.S. law requires 27 countries, mostly in Europe, to issue biometric passports after Oct. 26, 2004, or require their citizens to apply for visas to visit the U.S. Setec's first order comes from Denmark, which is implementing the new passports this year, although current passport holders won't be required to upgrade until their current documents expire. (AP 17 Feb 2004)

Category 43.2 *Biometrics*

2004-04-27 **fingerprinting Ohio schools PIN biometrics meal plan**

NewsScan

FINGERPRINT TECHNOLOGY IN OHIO SCHOOLS

The Akron, Ohio school district has begun using a $700,000 "iMeal" program that identifies students in school lunch lines using their fingerprints. Students whose parents don't want them fingerprinted can instead be issued a PIN number to participate in the school lunch program. The coordinator of Akron's Child Nutrition Services says, "It's a parental and student choice what to do. We don't encourage or discourage either option." Whether students use fingerprints or PIN numbers, they'll be able to pay as they go through the lunch line or draw from a prepaid account. (AP/San Jose Mercury 27 Apr 2004) News

---

Category 43.2 *Biometrics*

2004-05-19 **biometric transportation aviation**

DHS IAIP Daily; http://www.gao.gov/cgi−bin/getrpt?GAO−04−785T

May 19, General Accounting Office — GAO-04-785T: Aviation Security: Challenges in Using Biometric Technologies (Testimony).

The term biometrics covers a wide range of technologies that can be used to verify identity by measuring and analyzing human characteristics—relying on attributes of the individual instead of things the individual may have or know. Since the September 11, 2001, terrorist attacks, laws have been passed that require a more extensive use of biometric technologies in the federal government. In 2002, the General Accounting Office (GAO) conducted a technology assessment on the use of biometrics for border security. GAO was asked to testify about the issues that it raised in the report, the current state of the technology, and the application of biometrics to aviation security. The GAO found that three key considerations need to be addressed before a decision is made to design, develop, and implement biometrics into a security system: 1. Decisions must be made on how the technology will be used. 2. A detailed cost-benefit analysis must be conducted to determine that the benefits gained from a system outweigh the costs. 3. A trade-off analysis must be conducted between the increased security, which the use of biometrics would provide, and the effect on areas such as privacy and convenience. Highlights: http://www.gao.gov/highlights/d04785thigh.pdf Source: http://www.gao.gov/cgi-bin/getrpt?GAO-04-785T

Category 43.2 *Biometrics*

2004-05-20 **biometric authentication credit card smart card**

http://www.beepcard.com/products.asp;
http://query.nytimes.com/gst/abstract.html?res=F60C17F8385B0C738EDDAC08
94DC404482

HI THERE! I'M YOUR OWNER!

Beepcard, a Santa Monica CA company, has introduced a smart card that could be used as a credit card with voice identification built-in. The authorized user would have to speak a registered password to activate the card.

[MK notes: Some known problems with voice pattern biometrics could be annoying. For example, depending on the sophistication of the algorithms, card might not recognize the authorized user if he or she were to have a cold.]

Category 43.2 *Biometrics*

2004-09-01 **biometric identification authentication I&A fingerprint ID checkout supermarket Blockbuster Kroger PigglyWiggly ten-digit code**

NewsScan

RETAILERS TEST BIOMETRIC CHECKOUT

Retailers, including Blockbuster, Kroger and PigglyWiggly supermarkets, are testing a finger-identification system that enables customers to pay for their goods just by placing their finger on a scanner and typing in a seven- to 10-digit code. "It's doing surprisingly well," says a PigglyWiggly spokeswoman. "The [customers] were a bit hesitant at first, but more and more of them have been able to grasp the concept each week." The supermarket chain plans to make the technology available in all 120 stores in the next few years. As finger-identification technology becomes increasingly common, companies are hastening to assure customers that they don't plan to share the information with others. Also, they point out that the system differs from government fingerprinting systems because finger ID records only unique data points -- instead of an entire print. (Wall Street Journal 1 Sep 2004)

Category 43.2 *Biometrics*

2004-09-09 **Microsoft password solution list Windows XP Fingerprint Reader biometric authentication I&A**

NewsScan

MICROSOFT POINTS TO PASSWORD SOLUTION

Microsoft has a solution for those who have difficulty keeping track of all the passwords and usernames required by many Web sites today. Its Fingerprint Reader hooks up to PCs running the XP operating system and scans the unique skin patterns of the user's finger. The software then stores the image and uses it as a reference to restrict access to secure Web sites. Microsoft warns that the Fingerprint Reader is not intended to protect sensitive data, such as financial information, but informal testing showed it did a pretty good job of keeping non-authorized users out, and also withstood attempts to fool it using Silly Putty and Scotch tape. However, the company emphasizes that its Fingerprint Reader is all about convenience, rather than security. The device will hit the stores in mid-November, priced at $54.95, and Microsoft is also incorporating the Fingerprint Reader in a new keyboard and wireless mouse. (AP 9 Sep 2004)

Category 43.2 *Biometrics*

2004-10-11 **biometrics fingerprints retina handprint facial recognition comparison benefits cost future sales passwords users**

NewsScan; http://online.wsj.com/article/0,,SB109744462285841431,00.html (sub req'd)

LET YOUR FINGERS DO THE TALKING

Fingerprint technology appears to be the biometric identification method of choice, surpassing competing systems such as retina scanning, handprint geometry and facial recognition. "Fingerprints will be dominant for the foreseeable future," says Don McKeon, product manager for biometric security at IBM. One reason for its popularity is falling prices for fingerprint readers: Microsoft recently introduced a stand-alone model for $54 and earlier this year American Power Conversion rolled out a model for PCs priced at $45. Meanwhile, IBM said last week it would begin selling laptops with built-in fingerprint readers and Microsoft is marketing a fingerprint reader-keyboard and -mouse. International Biometric Group predicts sales of fingerprint readers will rise 86% to $368 million this year, up from $198 million last year, spurred by user rebellion against the myriad passwords computer users must now memorize. "Our parents didn't deal with the problem of remembering 20 passwords, and our grandkids won't even know what they are," predicts McKeon.

Category 43.2 *Biometrics*

2005-02-01 **biometric identification authentication credit card payment supermarket retail store**

RISKS; http://news.com.com/2100-1029-5559074.html 23 70

BIOMETRIC PAYMENT SYSTEMS IN SUPERMARKETS

Monty Solomon extracted an interesting item on biometric I&A from an article by Jo Best:

A supermarket has given its customers the choice of paying by fingerprint at a store in the state of Washington--and has found them surprisingly willing to use the biometric system. U.S. chain Thriftway introduced the system, which uses technology from Pay By Touch, in its store in the Seattle area in 2002. It said it now sees thousands of transactions a month using the payment method. Once people have enrolled in the Pay By Touch system, they have their fingerprint scanned as verification of identity at the checkout. They then choose which credit card they want to pay the bill with, having already registered the credit cards with the store.

Thriftway President Paul Kapioski said rather than shying away from the technology because of concerns about protecting their privacy, customer demand ensured that the biometric payment system made it past the pilot stage. …

Category 43.2 *Biometrics*

2005-02-17 **password type authentication keystroke dynamics biometrics**

NewsScan; http://www.usatoday.com/tech/news/computersecurity/2005-02-17-typing-biometric_x.htm

YOU ARE WHAT YOU TYPE

Researchers at Louisana Tech and the University of Pennsylvania have come up with a way of incorporating a user's style of typing into his or her system password. One of the researchers explains, "We look at the time between keystrokes, and the time it takes to press a key." It appears that style of typing is as unique as your eye color or speech patterns. Who would have thought it. (AP/USA Today 17 Feb 2005)

Category 43.2 *Biometrics*

2005-04-04 **biometric identification authentication I&A theft fraud amputation automobile security**

RISKS; http://www.theregister.co.uk/2005/04/04/fingerprint_merc_chop/ 23 83

CARJACKERS SWIPE BIOMETRIC MERCEDES, PLUS OWNER'S FINGER

A Malaysian businessman has lost a finger to car thieves impatient to get around his Mercedes' fingerprint security system. Accountant K Kumaran, the BBC reports, had at first been forced to start the S-class Merc, but when the carjackers wanted to start it again without having him along, they chopped off the end of his index finger with a machete.

The fingerprint readers themselves will, like similar devices aimed at the computer or electronic device markets, have a fairly broad tolerance, on the basis that products that stop people using their own cars, computers or whatever because their fingers are a bit sweaty won't turn out to be very popular.

They slow thieves up a tad, many people will find them more convenient than passwords or pin numbers, and as they're apparently `cutting edge' and biometric technology is allegedly `foolproof', they allow their owners to swank around in a false aura of high tech.

And that is exactly where the risks lie, high-tech does not necessarily mean high-security!

At least in sci-fi, fingerprint systems check for a heartbeat or pulse!!!

[`Cutting edge', eh? Wow! Incidentally, for many years I've been citing the concept of an amputated finger as a hypothetical way of defeating a poorly designed fingerprint analyzer. It's no longer hypothetical. PGN]

--contributed by Alpha Lau via RISKS

Category 43.2 *Biometrics*

2005-06-15 **US extension biometric passport requirement UK DHS terrorism anti-terrorism civil liberties privacy concerns**

EDUPAGE; http://news.com.com/2100-7348_3-5748629.html

U.S. GRANTS ANOTHER EXTENSION TO BIOMETRIC PASSPORTS

In a concession to nearly half of the countries in the Visa Waiver Program, officials from the United States have again extended the deadline for the addition of biometric data to passports. The program allows citizens of 27 countries to visit the Unites States using a passport only--without applying for a visa--for up to 90 days. In an effort to increase security, U.S. authorities said they would require that biometric information be added to passports in participating countries by October 26, 2005. After 13 of the countries in the program said they would miss the deadline, which had already been delayed once, U.S. security officials said countries would have another year to comply with the new regulation. The United States will, however, require participating countries to add digital photographs by the October deadline. The United States stood to lose potentially billions of dollars spent by tourists and business travelers from those countries if the deadline had not been extended. CNET, 15 June 2005

Category 43.2 *Biometrics*

2005-12-02 **DHS federal identification fingerprint images biometrics templates**

DHS IAIP Daily; http://www.fcw.com/article91576−12−02−05−Web

FEDERAL IDENTIFICATION CARDS MAY GET FASTER, SAFER

By the end of December, the federal government is expected to pick a new storage standard for fingerprint data on its new Personal Identity Verification cards, a Department of Homeland Security (DHS) official said Friday, December 2. The cards are expected to use a mathematical template of fingerprint images of cardholders' two index fingers, instead of compressed images of the prints themselves, said Kevin Crouch, portfolio manager for Homeland Security Presidential Directive 12 implementation at DHS' Joint Office of Interoperable Communications. The switch breaks the nearly year-long deadlock over whether the PIV cards should use images or templates, said Walter Hamilton, chairman of the International Biometric Industry Association and vice president and general manager of biometric solutions at Saflink. The decision marks a victory for the biometrics industry, which supports using templates. Templates require less data and processing time and protect the privacy of data better than images do, Hamilton said. The National Institute of Standards and Technology supported using compressed images because the template technology is less tested than image technology.

Category 43.2 *Biometrics*

2005-12-12 **biometric security researchers crack Play-Doh fake fingerprints**

DHS IAIP Daily; http://www.pcpro.co.uk/news/81257/researchers−crack−
biometri c−security−with−playdoh.html

RESEARCHERS CRACK BIOMETRIC SECURITY WITH PLAY-DOH

Using fake fingerprints, researchers in New York have managed to break nearly all the biometric identification systems they tested. Headed by Clarkson University associate professor of Electrical and Computer Engineering Stephanie C. Schuckers, they used fake fingers made by taking casts of live fingers and using the molds to create copies in Play-Doh. The 60 fake fingers were then tested and were successfully authenticated by the combination of the fingerprint readers and their accompanying software in nine out of every ten attempts. "Digits from cadavers and fake fingers molded from plastic, or even something as simple as Play-Doh or gelatin, can potentially be misread as authentic," Schuckers explained. The team subsequently developed a technique for distinguishing live digits by detecting changing moisture patterns and reduced the false detection rate to less than 10 percent. "Since liveness detection is based on the recognition of physiological activities as signs of life, we hypothesized that fingerprint images from live fingers would show a specific changing moisture pattern due to perspiration but cadaver and spoof fingerprint images would not," Schuckers explained.

Category 43.2 *Biometrics*

2005-12-16 **NIST standard biometric minutia HSPC-12 DHS PD 12**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/37790−1.html

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY CHOOSES MINUTIA FOR HSPD-12 BIOMETRIC STANDARD

After nearly a year in the making, the National Institute of Standards and Technology (NIST) has been convinced that minutia is an acceptable way to store fingerprint biometric data on smart cards. Amid pressure from industry, agencies and the administration, NIST Thursday, December 15, released the biometric specification for Federal Information Processing Standard 201, Personal Identity Verification under Homeland Security Presidential Directive 12, calling for agencies to store two index fingerprints on the smart card using the International Committee for Information Technology Standard 358 for minutia. Each fingerprint template shall be wrapped in the Common Biometric Exchange Formats Framework structure, NIST said in Special Publication 800-76. NIST originally wanted to store fingerprints using a digital image because it is more entrenched, while minutia is still new and the standard hasn't been tested enough. During the past 11 months, the indecision caused the White House to get involved in the final decision. Agencies, vendors and other interested parties have until January 13, 2006, to comment on this latest draft. NIST then will issue a final version about a month later. Federal Information Processing Standards Publication on Personal Identity Verification of Federal Employees and Contractors:
http://www.csrc.nist.gov/publications/fips/fips201/FIPS-201- 022505.pdf NIST Special Publication 800-76:
http://csrc.nist.gov/publications/drafts/800-76Draft/sp-800- 76_draft.pdf

---

Category 43.2 *Biometrics*

2005-12-16 **biometrics face facial recognition NIST fingerprints ID cards specifications federa government draft**

EDUPAGE; http://www.fcw.com/article91747-12-16-05-Web

NIST SETS DATA SPECS FOR BIOMETRIC ID CARDS

The National Institute of Standards and Technology (NIST) has established and published biometric data specifications, required for federal ID cards slated for implementation in October 2006. The new specs cover fingerprints and facial image recognition. Comments on the draft specs will be accepted until January 13, 2006.

Category 43.2 *Biometrics*

2006-01-05 **US-VISIT US government DHS fingerprint biometric identification authentication I&A**

EDUPAGE; http://www.fcw.com/article91877-01-05-06-Web 23

US-VISIT WANTS ALL 10 FINGERS PRINTED

Officials at the Department of Homeland Security (DHS) have announced a plan to begin requiring visitors to the United States to have all 10 of their fingers to be printed to be admitted to the country. Currently, the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program requires prints of two fingers; the change to 10 will reportedly increase both security and privacy and will decrease the number of visitors who must undergo a second inspection to enter or leave the country. DHS said biometric technology such as fingerprinting is already reliable, but the agency is working with technology vendors to develop products that are more accurate, faster, and more mobile.

Category 43.2 *Biometrics*

2006-02-23 **wireless security research fingerprints biometrics University of Buffalo**

DHS IAIP Daily; http://www.networkworld.com/news/2006/022706−fingerprint −security.html 23

RESEARCHERS CLAIM ADVANCES IN USING FINGERPRINTS TO SECURE NETWORKS.

University of Buffalo, NY, researchers say they have found a way to improve security of wireless handheld devices and Websites. The research specifies how big a keypad sensor needs to be and how big a fingerprint image should be, as a key shortcoming of biometric systems now is that sensors often only can take partial fingerprints, says Venu Govindaraju, a University of Buffalo professor of computer science and engineering, and director of the school's Center for Unified Biometrics and Sensors (CUBS). The researchers' work has been published in the journal Pattern Recognition.

Category 43.2 *Biometrics*

2006-03-06 **Microsoft Fingerprint Reader hack Finnish military Black Hat Europe presentation unencrypted transmission sniffer**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/holes/s tory/0,10801,109276,00.html 23

RESEARCHER HACKS MICROSOFT FINGERPRINT READER.

A security researcher with the Finnish military has shown how they could steal your fingerprint, by taking advantage of an omission in Microsoft Corp.'s Fingerprint Reader, a PC authentication device that Microsoft has been shipping since September 2004. Although the Fingerprint Reader can prevent unauthorized people from logging on to your PC, Microsoft has not promoted it as a security device. Hoping to understand why Microsoft had included the caveat about sensitive data, a researcher with the Finnish military, Mikko Kiviharju, took a close look at the product. In a paper presented at the Black Hat Europe conference last week, he reported that because the fingerprint image taken by the scanner is not encrypted, it could be stolen by hackers and used to inappropriately log in to a computer. Because the fingerprint image is transferred unencrypted from the Fingerprint Reader to the PC, it could be stolen using a variety of hardware and software technologies, called "sniffers," that monitor such traffic, said Kiviharju. Kiviharju's report: http://www.blackhat.com/presentations/bh-europe-06/bh-eu-06-Kiviharju/bh-eu-06-kiviarju.pdf.

43.3 Passwords

Category 43.3 *Passwords*

1997-02-03 **PIN mnemonic**

PA News

CPP Card Protection Plan announced a simple grid for helping people retrieve up to six personal identification numbers using a two-digit code.

Category 43.3 *Passwords*

1997-02-23 **electronic commerce passwords**

EDUPAGE

PASSWORD-SHARING THWARTS WEB REVENUES
Web entrepreneurs who charge subscription fees for accessing their Web sites are finding their customers are passing along their passwords to friends, relatives, etc., thus diminishing Web operators' potential for making their venture pay off. "Everybody on the Internet who sell subscriptions has this problem to one degree or another," says a producer for SportsZone. A technical fix is possible, but Web site operators are reluctant to make things more difficult for legitimate subscribers to log on. Meanwhile, Internet Billing offers software that allows Web sites to limit how many times the same password may be used each day — a solution that would probably keep some of the piracy down, but runs the risk of alienating paying customers who just want to log on a lot. (Wall Street Journal 21 Feb 97)

Category 43.3 *Passwords*

1997-06-22 **hack challenge electronic commerce**

SOUTH CHINA MORNING POST; Canada Newswire

VirTech, a Canadian company running a virtual mall, challenged hackers and anyone else to break into its server for a prize worth about $7,000 (C$10,000). The Vanhacking Challenge Web Site asked attackers to seize a password, enter a restricted page, and alter a phrase in the closed page. It was designed to demonstrate how hard it is to capture credit-card data from a properly-secured Web site. By the close of the contest in mid-July, there were no winners.

Category 43.3 *Passwords*

2000-01-15 **weak cryptography design error password crack vulnerability**

Crypto-Gram http://www.counterpane.com/crypto-gram-0001.html; ZDNet http://www.zdnet.com/zdnn/stories/news/0,4586,2409537,00.html 00 01

Bruce Schneier criticized Netscape's decision to store e-mail passwords with weak encryption; he lambased the executives who defended the decision on the basis of allowing "security experts" to recover those passwords if users forgot them.

Category 43.3 *Passwords*

2000-07-14 **I&A identification & authentication credit history privacy**

NewsScan, San Jose Mercury News
http://www.sjmercury.com/svtech/news/breaking/merc/docs/054775.htm

To identify online customers of the Checkfree bill-paying service, Checkfree will ask them questions based on their credit histories - such as what bank financed their car loans and what their mortgage payments are - and check their answers against information provided by the Equifax credit-reporting company.. An Equifax executive says: "Our strategy is to provide safety, security and privacy for Internet commerce transactions... It makes the application process for Checkfree easier for the consumer." (AP/San Jose Mercury News 14 Jul 2000)

Category 43.3 *Passwords*

2001-03-02 **palm computer password back door failure bug weakness vulnerability confidentiality encryption decryption**

RISKS 21 26

According to Robert Lemos, writing for CNET News, the security company @Stake reported that any devices using the Palm operating system (PalmOS) have no effective security despite the password function. Apparently developer tools supplied by Palm allow a back door conduit into the supposedly locked data. The firm warned that "If someone finds or steals a Palm, the owner's data is basically an open book. And the theft of mobile devices for their data is becoming more common." In addition, wrote Lemos, "Last September, @Stake discovered that the encrypted password used by Palm OS to protect so-called private records from prying eyes could easily be broken. With the discovery of the latest back door, it would seem that no data is safe."

Category 43.3 *Passwords*

2001-05-11 **canonical passwords voicemail confidentiality**

RISKS 21 40

Vodafone Australia's mobile phone voicemail uses a canonical password if a user has not set one. As RISKS contributor Andrew Goodman-Jones noted, "Need to check on your friends', your ex's, your boss', your children's voicemail?"

Category 43.3 *Passwords*

2001-07-23 **password cracker MS Microsoft IE Internet Explorer freeware**

RISKS 21 56

A freeware application to crack the S Internet Explorer file that stores passwords was released on the Web with the following notice in the Earthlink Weekly Email Newsletter on 07/23/2001: "If you tell your browser to save Web site passwords so that you don't have to reenter them, you might forget those passwords over time. This program can reveal the passwords hidden behind those asterisks in Web site login screens."

Category 43.3 *Passwords*

2001-08-03 **password policy reset e-mail canonical password stupidity awareness**

RISKS 21 57

[No point in abstracting this one: here's Jim Horning's contribution to the demonstration of the state of security awareness (or even just of common sense) in corporate America:]

Subject: Password changes -- SIGH!

> From: <HR Department>
> Sent: Friday, August 03, 2001 10:12 AM
> To: <US Employees>
> Subject: IMPORTANT <HR Database> INFORMATION - PLEASE READ
>
> We want to make you aware that <HR Database> will be unavailable from 6pm
> (PT) on Friday, August 3 to 11:59pm (PT) on Sunday, August 5 due to server
> upgrades. During this time, you will not be able to access the website.
> In <Outsourced supplier>'s ongoing effort to improve site performance,
> these upgrades are occurring to load balance and increase site stability.
> Part of this site upgrade includes a password change. ALL USERS WILL HAVE
> A PASSWORD OF "change123" as of 12:01am PT Monday, August 6th, 2001. Once
> you enter the system for the first time on or after August 6th, you will
> be required to change your password and answer a secret question. In the
> future, you will be able to use the answer to the question to reset your
> own password.
> If you experience problems, please contact the whereiwork help desk at
> support@<Outsourced supplier>.

Category 43.3 *Passwords*

2001-09-05 **password management modification data corruption user interface design flaw stupidity error bug**

RISKS 21 65

Bill Bumgarner discovered that entering a password with an exclamation mark in the new-password fields for Consumer Reports' Web site results in _silent_ exclusion of the character. Thus when the user tries to enter the accepted password with the "!", the system naturally rejects the password. However, one can always get a plaintext copy of the "corrected" password via unsecured e-mail. . . .

[MORAL: designers must not edit a password without notifying the user of the change.]

Category 43.3 *Passwords*

2001-12-03 **credit card identification authentication I&A password fraud**

NewsScan

CREDIT CARD COMPANIES DEVELOP NEW PASSWORD SYSTEMS
To give customers an added feeling of security when they provide their credit card numbers to make purchases over the Internet, Visa and Mastercard will offer new password systems. The Visa system is being launched today as a optional feature, and will invite cardholders to link their cards to an additional password, beyond the information on the card itself; the Mastercard system, still in development, will require the user to download a small program. Amazon is one of the merchants that has declined to participate in the system, because "it would turn one-click ordering into four-point, three-click ordering." Dell, on the other hand, has already signed up for the system, not so much because of its own concerns about fraudulent purchases but because "we want to give customers more confidence in buying online," even though cardholders are not actually liable for fraudulent purchases made on their accounts. Credit card fraud is not a major problem for most companies, and Visa says that just 7 cents out of every $100 is lost to fraud. (New York Times 3 Dec 2001)
http://partners.nytimes.com/2001/12/03/technology/ebusiness/03CARD.html

---

Category 43.3 *Passwords*

2002-03-05 **quality assurance QA login identification authentication I&A procedures policies**

RISKS 21 93

Arthur Byrnes reminded us again in RISKS of the dangers of incompetent people regardless of security efforts. Twice in a single week, he saw major companies send unencrypted e-mail containing both login IDs and associated passwords along with usage instructions.

Duuuuhhhh.

Don't let your employees send that kind of e-mail!

Category 43.3 *Passwords*

2002-06-10 **password userID e-mail notification design plan confidentiality vulnerability exposure**

RISKS 22 12

The New York Times sent out new userIDs and passwords in a single cleartext e-mail message. Worse, the user ID was firstname_lastname and the password was an existing userID from an older system where no particular effort had been made to keep the userIDs secret.

Category 43.3 *Passwords*

2002-06-27 **password recovery management I&A identification authentication database management loss**

RISKS 22 13

Peter G. Neumann summarized an interesting case of bad-password recovery:

After the password for accessing a Norwegian history museum's database catalog for 11,000 books and manuscripts had been lost when the database's steward died, the museum established a competition to recover it. Joachim Eriksson, a Swedish game company programmer, won the race to discover the password (ladepujd, the reverse of the name of the researcher who had created the database). How he arrived at it was not disclosed. [Source: Long-lost password discovered: Norwegian history database cracked with help from the Web, By Robert Lemos, MSNBC, 11 Jun 2002]

Category 43.3 *Passwords*

2004-02-12 **SSN Social Security number unencrypted user ID e-mail**

RISKS 23 19

USERID+PW = NONO

Carl Fink noted in RISKS that his corporate Web site sent him his userID (his SSN) and his password in the same e-mail message (unencrypted, of course).

DON'T DO THAT.

Category 43.3 *Passwords*

2004-04-19 **password management policy awareness survey study**

http://www.securitypipeline.com/news/18902074

Mitch Wagner of securitypipeline.com wrote a summary of an informal man-in-the-street survey in London concerning attitudes and behavior with respect to passwords. Sample size was small: 172 people replied to the questions. Results were not good.

Quoting from Wagner's report:

>• 53 percent of users said they would not give their password to a telephone caller claiming to be calling from their IT department.

• Four out of 10 knew their colleagues' passwords.

• 55 percent said they'd give their password to their boss.

• Two thirds of workers use the same password for work and for personal access such as online banking and web site access.

• Workers used an average of four passwords, although one systems administrator used 40 passwords, which he stored using a program he wrote himself to keep them secure.

• 51 percent of passwords were changed on a monthly basis, 3 percent changed passwords weekly, 2 percent daily, 10 percent quarterly, 13 percent rarely and 20 percent never.

• Many workers who regularly had to change their passwords kept them on piece of paper in their drawers, or stored on Word documents.<

Other findings:

* ~¾ of the respondents said they would reveal their password in return for a chocolate bar [MK asks: but how would you know if they were telling the truth? They could get a chocolate bar in return for any old word.]

* Many respondents explained in that there passwords were based on partners, children, football teams, and pets.

* The most common password was "admin."

* Most people said they would steal confidential information when changing jobs.

* Most of the respondents admitted that they would not protect the confidentiality of salary information if the data were accidentally revealed to them.

Category 43.3 *Passwords*

2004-08-11 **password authentication weak I&A easy-to-guess**

NewsScan

MOST PASSWORDS ARE EASY TO GUESS

Most Internet users choose easy-to-guess passwords such as their pet's name, according to a survey by Visa Europe. More than three-fourths of those polled said they choose passwords relating to friends, family and memorable dates. The favorites are nicknames (21%), birthdays and anniversaries (15%), pet names (15%), family members' names (14%) and memorable dates such as the Battle of Hastings and England's World Cup victory (7%). Two percent even reported using "password" as their password. "It is not surprising that loved ones and pet names top the most popular list as often people struggle to remember random characters or designated log-in codes and opt to choose their own. Of course, it is important that our passwords are personal and meaningful to us, but also that they are difficult to decipher and not easily guessed," says Visa Europe VP Hugo Bottelier. When choosing a password, Visa suggests avoiding words that appear in the dictionary, as well as words relating to personal information that could be inferred or guessed. The most preferable type of password would have random letters, numbers and punctuation. And for heaven's sake, don't write it down and leave it by your credit card or PC! (Silicon.com 11 Aug 2004)

Category 43.3 *Passwords*

2004-08-11 **easy to use passwords Internet users**

DHS IAIP Daily; http://www.silicon.com/0,39024729,39123066,00.htm

August 11, silicon.com — Internet users still choosing easy to guess passwords.

Despite increased awareness about the need for secure passwords, internet users are still leaving themselves vulnerable to hackers by choosing easy to guess subjects such as their cat or partner's name. Over three-quarters choose passwords relating to friends, family and memorable dates, according to research into 1,000 internet users by Visa Europe. The favourites are nicknames, birthdays and anniversaries, pet names, family members' names, and memorable dates. All of those are details that basic social engineering techniques would uncover relatively quickly. To make matters worse a third of respondents said they use the same password for all their log-ins, while a quarter using it nearly all or most of the time. But the message about choosing hard to guess passwords does seem to be getting through to some people with 22 per cent opting for random letters.

Category 43.3 *Passwords*

2004-08-18 **password authentication graphical user picture drawing USENIX security Draw-A-Secret scheme**

DHS IAIP Daily; http://searchsecurity.techtarget.com/originalContent/0,28914
2,sid14_gci1000783,00.html

August 18, SearchSecurity.com — Graphical passwords still far from picture perfect.

Given the explosion of data now held in devices, and the fact many employees still use easily guessed words to access them, more companies are eyeing graphical password schemes. New research suggests a major weakness in current graphics-based password programs, whether self-drawn or computer-generated, remains people picking obvious choices. This raises the success of brute-force attacks launched by illegal dictionary tools. In a study of the password scheme Draw-A-Secret, in which users make a picture in a grid that's then replicated for access, users typically draw symmetrical, identifiable objects in the middle of the grid. 9 According to research by Julie Thorpe, a Canadian scholar who presented during last week's Usenix Security Symposium in San Diego, CA, and her partner Paul van Oorschot, it takes only six days for a computer to run through all of the most common choices. Add 999 more machines and the time narrows to 8.7 minutes. One way to up the odds would be for organizations using this program to require a minimum number of strokes (five or greater) and more unique drawings, such as disjointed or off-centered objects, Thorpe said.

Category 43.3 *Passwords*

2005-08-10 **unauthorized use administrator passwords students policy felony charges monitoring**

RISKS; http://www.wired.com/news/technology/0,1282,68480,00.html 24 02

ADMIN PASSWORDS TAPED TO BACKS OF LAPTOPS; STUDENTS FACE FELONY CHARGES

Thirteen high-school students in the Kutztown Area School District (Pennsylvania) face felony charges of tampering with computers after defeating security measures on laptops issued to them by the school district. They used administrator passwords (taped to the backs of the computers) to override Internet filters and download software such as iChat that the district policy forbids. The laptops included an application that allowed district administrators to see what students did with the computers. However, the students modified the monitoring program so that they could see what the administrators did with their computers. The students and their parents argued that the felony charges are unwarranted, but, according to the district, students and parents signed acceptable use policies that clearly state what activities are not allowed and that warn of legal consequences if the policy is violated. The students continued to violate district policies for use of the computers even after detentions, suspensions, and other punishments, according to the district. Only then did school officials contact the police.

[Abstract by Peter G. Neumann]

Category 43.3 *Passwords*

2005-09-16 **password sniffing audio recognition tuning spell-check high accuracy**

DHS IAIP Daily;
http://news.yahoo.com/s/sv/_www12662937;_ylt=AiX.GcAU5Lpn34b
ns3op.pus0NUE;_ylu=X3oDMTA3cjE0b2MwBHNlYwM3Mzg−,
http://siliconvalley.com

TUNING INTO PASSWORDS

Many people have heard of keyboard sniffing, in which someone sneaks software into your computer and monitors e-mail or documents. There is a new security threat that researchers are warning: keyboard listening. A graduate student in computer science at the University of California-Berkeley, developed a way of making audio recordings of keyboard strokes to see if words and phrases could be deciphered accurately. Using a microphone plugged into a laptop running generic speech recognition and spell-check software, the team was able to associate the sound of individual keys on a keyboard with specific letters and thus figure out what was being written with 96 percent accuracy.

Category 43.3 *Passwords*

2005-10-21 **canonical passwords Joe accounts primitive security elementary errors identification authentication I&A preemption denial of service DoS**

RISKS 24 08

CANONICAL PASSWORDS (STILL!)

San Francisco administrators of OARS, Online Assessment Reporting System, issued a generic password (same for all teachers) that left the system wide open to anyone who knew a teacher's user name, because many teachers had not gotten around to changing the password. [Source: Nanette Asimov, *San Francisco Chronicle*, 21 Oct 2005, B2]

Cingular moved its voicemail system over to an AT&T wireless service over the past two weeks. Anyone initializing the account before the legitimate owner can then gain total access to the account. Approximately 26 million Cingular subscribers of the old system are potentially affected. [Source: Ryan Kim, *San Francisco Chronicle*, 21 Oct 2005, C1]

[Abstracts by Peter G. Neumann]

Category 43.3 *Passwords*

2005-11-18 **passwords authentication plaintext plain text risks sniffing**

RISKS; http://www.infoworld.com/article/05/11/04/45OPsecadvise_1.html 24 11

RISKS OF PLAINTEXT PASSWORDS

RISKS contributor Steve Summit points us to a report about the risks of using plaintext passwords. He writes, "[T]he article also makes the point that although the passwords so sniffed are often "unimportant" ones, for services such as mere e-mail access or gambling site logins, people are often known to use their same passwords for these and for their "secure" systems such as Windows network logins."

Mr. Summit additionally recommends security expert Bruce Schneier's newsletter "Crypto-Gram", available at < http://www.schneier.com/crypto-gram.html>

Category 43.3 *Passwords*

2006-03-08 **password vault null user interface error design flaw stupid technical support idiots fools bafflegab nonsense frustrating**

RISKS http://catless.ncl.ac.uk/Risks/24.19.html#subj12 24 19

INSECURE APC BIOPOD ILLUSTRATES PROBLEMS WITH UNTRAINED STAFF

Gabe Goldberg provided a depressingly believable tale of wooden-headed stupidity in the face of his analysis of a design flaw in the APC "BioPod" password vault. The device provides biometric access control with or without a password. The password is derived automatically from the Windows password -- and Mr Goldberg correctly pointed out to the company that it accepts a null Windows password without warning the user that there is therefore no master password loaded on the device. Nothing he could say to the technical support person he spoke to could overcome the stock repetition of the very flaw he was trying to report. In the infuriating display of stubborn denial that characterizes very stupid people, the agent simply kept repeating the presumably written description of exactly what was wrong as if it were an explanation. Perhaps the best line in the entire dialog was "Officially the BioPod is not advertised as a security device, but a password manager, so it is not designed to increase the security of your computer, but provide a safe way to manage and store your passwords."

[MK adds: this design flaw also raises questions about the security experience of the people who designed the software.]

Category 43.3 *Passwords*

2006-03-08 **access control passwords keyspace keylength banking online policy**

RISKS 24 19

AUSTRALIAN NATIONAL CREDIT UNION LIMITS INTERNET PASSWORD KEYSPACE

A RISKS correspondent noted, "A step backwards for customers of Australian National Credit Union (www.friendlybanking.com.au) where from 21 Mar 2006 all users of the credit union's Internet banking will be limited to choosing passwords of six characters, consisting only of the numbers 0-9. They have previously had the ability to choose alpha-numeric passwords of varying length.

The credit union's website claims that the changes are for enhanced security. . . ." The correspondent added, "After I enquired about this apparent backward step, the credit union's response claimed this was required for the implementation of two-factor authentication, amongst other security enhancements. Two-factor authentication might be great for those who use it, but those that don't will be left with the limited password options."

Category 43.3 *Passwords*

2006-03-19 **vulnerability Microsoft Commerce Server 2002 authentication bypass solution update**

DHS IAIP Daily; http://www.securiteam.com/windowsntfocus/5AP0C2KI0E.html 23

MICROSOFT COMMERCE SERVER 2002 AUTHENTICATION BYPASS.

Improper authentication validation allows attackers to authenticate as an existing user in Microsoft Commerce Server 2002. Analysis: The problem is in the sample files of "authfiles." If the user makes his/her own solution site in Commerce Server and the "authfiles" are installed on the server, the user is vulnerable for positive user logon's using false passwords. If someone knows a user (some sites uses an e-mail address) and goes to http://site/authfiles/login.asp (some sites have it in another directory) and enters the Username and a false password, the user will get an error. After the error, if the user goes with the same browser to the root directory of the site, http://site/, another error occurs. Then, if the user navigates again to the site he/she will be logged on as the entered user. Vulnerable Systems: Microsoft Commerce Server 2002. Immune Systems: Microsoft Commerce Server 2002 SP2. Vendor Status: The vendor has issued a warning: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/csvr2002/htm/cs_se_securityconcepts_cbgw.asp The vendor has issued the following fix: http://www.microsoft.com/downloads/details.aspx?familyid=58e 6d658-cc3e-4846-8ef7-264e6eeb4c1e&displaylang=en

---

Category 43.3 *Passwords*

2006-05-02 **Cisco Unity Express expired password privilege escalation vulnerability**

DHS IAIP Daily; http://www.securityfocus.com/bid/17775/discuss 23

CISCO UNITY EXPRESS EXPIRED PASSWORD PRIVILEGE ESCALATION VULNERABILITY.

Cisco Unity Express (CUE) is prone to a privilege escalation vulnerability. Analysis: CUE contains a vulnerability that might allow an authenticated user to change the password for another user by using the HTTP management interface, if the password for the user being modified is marked as expired. This can result in a privilege escalation attack and complete administrative control of a CUE module, if the password being changed belongs to an administrator. An attacker could reset the password of a privileged account that has an expired password. Vulnerable: Cisco Unity Express 2.2(2); Cisco Unity Express 2.1(1); Cisco Unity Express 1.1(1); Cisco Unity Express. Solution: Fixes are available. Please see the referenced Cisco advisory for details: http://www.cisco.com/warp/public/707/cisco-sa-20060501-cue.s html

---

Category 43.3 *Passwords*

2006-05-08 **Cisco Secure ACS insecure password storage vulnerability**

DHS IAIP Daily; http://www.securityfocus.com/bid/16743/discuss 23

CISCO SECURE ACS INSECURE PASSWORD STORAGE VULNERABILITY.

Cisco Secure ACS is susceptible to an insecure password storage vulnerability. Analysis: With the master key, the user can decrypt and obtain the clear text passwords for all ACS administrators. With administrative credentials to Cisco Secure ACS, it is possible to change the password for any locally defined users. This may be used to gain access to network devices configured to use Cisco Secure ACS for authentication. If remote registry access is enabled on a system running Cisco Secure ACS, it is possible for a user with administrative privileges typically domain administrators to exploit this vulnerability. For a complete list of vulnerable products: http://www.securityfocus.com/bid/16743/info ACS 3.x for UNIX, and ACS 4.0.1 for Windows are not affected this issue. For more information: http://www.securityfocus.com/bid/16743/references

---

43.4 Kerberos

Category 43.4 *Kerberos*

2000-03-15 **Kerberos identification authentication I&A standards proprietary interoperability**

Cryto-Gram 2000 03-15

Microsoft integrated Kerberos into its authentication scheme for Windows 2000; however, the company altered the protocol by using the "data authorization" field in a non-standard way. Microsoft ignored the rules for making changes to an IETF protocol and rendered their version non-interoperable with standard implementations of Kerberos. Bruce Schneier wrote, "On the surface, this is just nasty business practices. If you're a company that has invested in a UNIX-based Kerberos authentication system and you want to support Windows 2000 desktops, your only real option is to buy a Windows 2000 Kerberos server and pay for the integration. I'm sure this is what Microsoft wants.

My worry is more about the security. Protocols are very fragile; we've learned that time and time again. You can't just make changes to a security protocol and assume the changed protocol will be secure. Microsoft has taken the Kerberos protocol — a published protocol that has gone through over a decade of peer review — and has made changes in it that affect security. Even worse, they have made those changes in secret and have not released the details to the world. Don't be fooled. The Kerberos in Windows 2000 is not Kerberos. It does not conform to the Kerberos standard. It is Kerberos-like, but we don't know how secure it is."

Category 43.4 *Kerberos*

2003-03-20 **Kerberos authentication protocol vulnerability leak**

NIPC/DHS

March 17, eWEEK — Details of Kerberos vulnerability leaked.

There is a serious weakness in MIT's Kerberos v4 authentication protocol that allows an attacker to impersonate any principal in a given realm. The Kerberos development team at MIT said the contents of an unpublished paper with details of this vulnerability have been leaked on the Internet. Using these details, an attacker familiar with Kerberos could easily exploit the vulnerability. Kerberos v4 tickets-or credentials-do not have a cryptographic hash of the encrypted data, random padding or a random initial vector. As a result, using a chosen plaintext attack, an attacker could fabricate a ticket. An attacker who controls a Kerberos cross-realm key would be able to impersonate any principal in the remote realm to any service in that realm. This attack could lead to a root-level compromise of the Kerberos key distribution center as well as any other hosts that rely on the KDC for authentication. Kerberos, developed at the Massachusetts Institute of Technology, is among the most widely deployed authentication protocols on the Internet. It is implemented in dozens of software applications, as well, including Windows 2000. However, Windows 2000 uses Kerberos v5 and Microsoft officials said that, while they're still researching the issue, they don't believe that operating system is vulnerable. Additional information may be found on the MIT Web site: http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2003-0 04-krb4.txt

---

Category 43.4 *Kerberos*

2004-09-01 **Kerberos authentication protocol open source vulnerabilities code execution attack**

DHS IAIP Daily; http://secunia.com/advisories/12408/

September 01, Secunia — Kerberos V5 multiple vulnerabilities.

Multiple vulnerabilities have been reported in Kerberos V5, where the most serious can potentially be exploited by malicious people to gain access to protected corporate networks and execute arbitrary code. Patches are available (see patch matrix in the original advisories). Update to version 1.3.5, when it becomes available: http://web.mit.edu/kerberos/dist/index.html Original Advisories: http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2004-0 02-dblfree.txt and http://web.mit.edu/kerberos/www/advisories/MITKRB5-SA-2004-0 03-asn1.txt

---

43.5 Single sign-on

Category 43.5 *Single sign-on*

1999-07-21 **single sign-on identification authentication I&A passwords**

Computer Reseller News Online
http://www.crn.com/search/display.asp?ArticleID=7653

NOVELL TO ADD SINGLE SIGN-ON
Novell this week will release Single Sign-on 1.0, new software that allows users to log on to multiple networks with a single password. The software will relieve end-users of having to manage multiple passwords, and will free IT managers of the task of redundant password administration. With Single Sign-on, the password is stored in NDS, which sends the password to the application, and the end user never sees a password dialog box. It will also support Lotus Notes, PeopleSoft, Entrust, and some host emulator products. IT organizations will enjoy the ability to spread network and service security over multiple databases, experts say. (Computer Reseller News Online 07/21/99)

Category 43.5 *Single sign-on*

1999-10-12 **medical informatics confidentiality HIPAA identification authentication I&A**

EDUPAGE; Wall Street Journal

INTEL AND AMA FORM SERVICE TO IMPROVE SECURITY OF ONLINE MEDICAL INFORMATION
Intel and the American Medical Association (AMA) are teaming to offer a service that will boost the online security of medical data. The service, which becomes available in the first quarter of 2000, will use "digital credentials" to prove the identities of doctors who are sending and accessing medical information over the Internet. The service launches Intel's "Internet Authentication Services" initiative, which permits the identification of parties at both ends of online transactions. The digital credential service, which is portable, is a big improvement over digital certificate security measures, according to Intel and the AMA. The use of the Internet for medical transactions will not reach mainstream levels unless security is improved. "This is important if the use of the Internet for health care is to go to the next level," says Jim Klein of the Gartner Group. (Wall Street Journal 10/12/99)

Category 43.5 *Single sign-on*

2002-04-04 **SSO single signon I&A identification authentication market analysis**

Yankee Group, Security Wire Digest 4 26

Yankee Grouop issued a market report on single-signon (SSO) systems and found significant progress throughout enterprise security and e-commerce applications. In a summary for Security Wire Digest, reporter Anne Saita wrote, "Microsoft's Passport, which got a huge boost in use once incorporated into the .Net initiative, is leading the field in the consumer SSO market with more than 3.5 billion monthly authentications worldwide. But Microsoft can expect stiff competition down the road from AOL, which simultaneously is developing its own SSO applications within an identity management system code-named 'Magic Carpet' and funding the Liberty Alliance, a business consortium spearheaded by Sun Microsystems that will compete head to head with Passport.

Computer Associates, IBM Tivoli and Novell also have made inroads in the legacy and client-server SSO space, as have SSO vendors that intersect the Web and legacy client-server applications markets, such as RSA Security, Entrust and Protocom, according to the report. The current lock these software giants and security companies have will make it difficult for newcomers in both the consumer and enterprise markets."

Category 43.5 *Single sign-on*

2004-03-01 **identification authentication I&A ISP Internet service provider wireless access piggybacking theft services IP address**

RISKS 23 22

E-MAIL ROBBERY, THE EASY WAY

Ralf Ertzinger analyzed the unfortunate decision by T-Online on user identification and authentication:

"T-Online is Germany's largest Internet provider, and while this in itself is not a risk, T-Online has always used a unique approach towards POP3 mail delivery. When being connected via T-Online, one does not have to provide a username or password to connect to the T-Online POP3 server in order to fetch mail, since the user is identified by his IP address.

Combine this with the growing number of (unsecured) WLAN access points and DSL routers and you get to read other people's mail just by driving along the streets. T-Online is aware of the problem, and provides information to secure WLAN access points on their web site, but changing the POP3 identification system (which was introduced long before anyone thought of broadband Internet, connection sharing and wireless LAN) seems to be almost impossible, having millions of customers."

Category 43.5 *Single sign-on*

2005-08-05 **General Services Administration GSA identity management plan single sign-on framework**

EDUPAGE; http://www.fcw.com/article89823-08-05-05-Web

GSA CALLS FOR COMMENTS ON IDENTITY MANAGEMENT PLAN

The General Services Administration (GSA) has called for comments on its plan for decentralized identity management. The system would permit secure single sign-on for users of online government services. A common network would link government or commercial entities that provide identity management services with the agency applications using those services. The program, called the E-Authentication Service Component, would employ this federated approach to avoid having government agencies develop their own e-authentication frameworks. Agencies could purchase and integrate a product from a government-approved provider list. The plan also calls for an E-Authentication Portal. Comments may be submitted through September 6, 2005. Federal Computer Week, 5 August 2005

43.6 E-mail authentication (e.g., SPF & SenderID)

Category 43.6 *E-mail authentication (e.g., SPF & SenderID)*

2004-10-26 **AOL Microsoft sender ID e-mail SPF Sender Policy Framework spoofing antispam forgery authentication SMTP headers IP address**

NewsScan;

AOL ACQUIESCES TO MICROSOFT SENDER ID AUTHENTICATION SCHEME

America Online reversed itself and now says it will adopt Microsoft's Sender ID e-mail authentication technology. Sender ID is a hybrid of earlier Microsoft technology and the technology that AOL initially championed, Sender Policy Framework (SPF). Sender ID works by checking records in the central domain-name system to check whether the sender's computer is authorized to use the domain name on the message, eliminating the annoying tactic of "spoofing," or forging, return e-mail addresses. AOL says it will begin testing Sender ID on inbound e-mail by year's end, while at the same time continuing to test other e-mail authentication technologies, including Domain Keys from Yahoo, plus to Cisco Systems technologies. (Wall Street Journal 26 Oct 2004)

Category 43.6 *E-mail authentication (e.g., SPF & SenderID)*

2004-11-11 **address antispam AOL authentication EarthLink e-mail forgery Framework FTC headers ID IP Microsoft Policy Sender SMTP spam SPF spoofing Yahoo zombie**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A41460-2004Nov10.html

AUTHENTICATION WON'T END SPAM, SAY EXPERTS

Panelists at a forum sponsored by the Federal Trade Commission warned that criminals are already one step ahead of major e-mail authentication initiatives planned by major ISPs, including AOL, Microsoft, Yahoo and EarthLink. The ISPs are still testing and backing several different plans, but the basic idea is that the e-mail system would check that the block of Internet addresses assigned to an e-mail provider includes the specific numeric address of a message sender. If the numeric address of the sender doesn't correspond with addresses assigned to the purported mail service, a red flag would be raised. The problem with that scheme, said the panelists, is that a majority of spam is now launched by "zombie" machines controlled by remote spammers. E-mail from a zombie PC looks as if it is coming from a legitimate source -- because it is. In the first half of this year, it's estimated that an average of 30,000 computers a day were turned into zombies, according to Symantec. But despite these discouraging statistics, the experts still insisted that authentication is a vital first step, to be followed by a system that evaluates the "reputation" of senders, perhaps using a process that marks good e-mail with an electronic seal of approval. (Washington Post 11 Nov 2004)

Category 43.6 *E-mail authentication (e.g., SPF & SenderID)*

2005-04-18 **e-mail secure transfer delivery receipt confirmation smart card reader electronic digital signature certificate authority**

RISKS; http://www.ynetnews.com/articles/0,7340,L-3073923,00.html 23 84

ISRAELIS TO RECEIVE SECURE E-MAIL ADDRESS TO BE USED FOR CONTACTS WITH AUTHORITIES

Shoshanah Forbes expressed skepticism about the proposed "secure e-mail" initiative in Israel:

"The Social-Economic Cabinet approved Sunday a plan put forth by Finance Minister Benjamin Netanyahu to expand Israel's *approachable Government* program. The government also approved the *safe deposit box* program, a system of secure e-mail boxes that would allow government offices to send official permits, signed forms, receipts and messages to businesses and individuals. [...] At first, the system will support forms in text format (TXT, PDF, RTF, HTML, XML), the last two without Active Script. The `safe' will require the recipient to send a `proof of receipt' to the sender. Each sent message will be coded to identify the sender, to allow the recipient to forward the message to a third party, and an expiry date. [...] In order to use the system, individuals and businesses will be required to obtain a smart card, a card reader (estimated cost: NIS 55 or about USD 12), and to register an electronic signature (approximately NIS 20 or about USD 4.5)."

In addition to all the usual RISKS such a scheme brings up, I should note that to this date, the bill paying website (http://www.mybill.co.il) works only with Win/IE, so I won't be surprised if the above setup will also be Win/IE only.

Category 43.6 *E-mail authentication (e.g., SPF & SenderID)*

2006-04-19 **e-mail authentication danger system break warning cryptography**

DHS IAIP Daily; http://news.com.com/Danger+Authenticating+e−mail+can+break+i t/2100−7349_3−6062953.html?tag=nefd.lede 23

DANGER: AUTHENTICATING E-MAIL CAN BREAK IT.

The promise of e-mail authentication is too good to ignore, but if it is implemented incorrectly it will break a company's mail system instead of fixing it, experts have cautioned. "Deploy smart. Don't just do it," Erik Johnson, a secure messaging executive at Bank of America, said in a presentation at the Authentication Summit Wednesday, April 19. "If you just do it, you may just break it." For the past two years, the technology industry has been advocating the use of systems to guarantee the identity of e-mail senders. It sees such authentication as key to the fight against spam and phishing, as it should help improve mail filters and make it harder for senders to forge their addresses. The industry also likes to advertise that these systems have practically no cost. The key problem for large companies is figuring out all the systems that send e-mail on their behalf, said Paul Judge, chief technology officer at e-mail security company CipherTrust. "If you are a large multinational organization, you may have e-mail gateways in 10 countries, you may have marketing companies that send e-mail on your behalf," he said.

44.1 Crypto algorithms

Category 44.1 *Crypto algorithms*

1997-06-27 **crypto algorithm RC2 S/MIME e-mail**

RSADSI press release

RSA Data Security Inc. released the full specifications of its proprietary RC2 encryption algorithm to the IETF for consideration as part of the new S/MIME standard for secure electronic messaging.
See <http://www.rsa.com/rsa/S-MIME/html/interop_center.html> for details of the interoperability testing.

Category 44.1 *Crypto algorithms*

1997-07-08 **crypto algorithm**

EDUPAGE

SCIENTISTS PROPOSE NEW ENCRYPTION SCHEME

Two scientists at the IBM Almaden Research Center in San Jose, Calif. Have developed a new approach to public key cryptography based on mathematical constructs called lattices. The system would be based on a particular set of hidden hyperplanes that constitute the private key and a method of generating points near one of those hyperplanes for the public key. The security of the system rests on the computational difficulty of finding the "unique" shortest line segment (or vector) that connects any two points in a given lattice — a task that's fairly easy in two or three dimensions, but much more difficult in a 100-dimensional lattice. The researchers are working to turn their theory into a marketable product, and see applications in creating digital signatures and other security and authentication schemes. (Science News 5 Jul 97)

[MK adds: This approach appears to have the advantage not only of generating key pairs that are incredibly difficult to find using brute-force cracking but also of ensuring continued employment for professors of cryptography who will have to explain the inconceivable to the next generations of computer science students.]

Category 44.1 *Crypto algorithms*

1997-09-02 **crypto standards Internet**

Inter@ctive Week

In September, the IETF told RSADSI that unless it surrendered its patents on its RSA cryptographic algorithms, there was no question of allowing S/MIME to become an Internet standard. No such standard has ever required royalty payments for use of its algorithms, as RSA expects. A competing Open PGP standard would require no royalties because it uses the Diffie-Hellman algorithms for a public key cryptosystem and those patents expired at the start of September 1997.

Category 44.1 *Crypto algorithms*

1997-10-26 **cryptography spoofing crackers**

EDUPAGE

NEC DEVELOPS 128-BIT ENCRYPTION TECHNOLOGY
Japan's NEC has developed 128-bit key encryption technology that makes use of an algorithm to create fake keys, which are then substituted for the real encryption keys when a potential hacker tries to crack the code. Under Japanese law, the product cannot be exported from Japan. (InfoWorld Electric 22 Oct 97)

Category 44.1 *Crypto algorithms*

1998-04-07 **encryption chaff restrictions**

EDUPAGE; RISKS 19 64

ENCRYPTION ALTERNATIVE SEPARATES THE WHEAT FROM THE CHAFF
An alternative approach to electronic privacy has been proposed by MIT cryptographer Ronald Rivest that could render the current debate over third-party encryption keys moot. Unlike conventional encryption programs, Rivest's new technique doesn't rely on altering message bits; rather, each bit is tagged with a "message authentication code" (MAC) and then mixed in with random bits tagged with incorrect MACs, called "chaff." The intended recipient can then use a secret code shared with the sender to "winnow" out the fake bits. (Science 3 Apr 98) A description of the process can be found at < http://theory.lcs.mit.edu/~rivest/chaffing.txt >.

Category 44.1 *Crypto algorithms*

1998-04-27 **encryption algorithm AES Advanced Encryption Algorithm**

PC Week 15 17

RSA announced its intention of proposing a candidate for the AES to NIST. Their algorithm would be a variation of RSA's well-known RC5 and would use at least a 128-bit block cipher.

Category 44.1 *Crypto algorithms*

1998-06-25 **encryption Skipjack Fortezza DoD DMS declassify**

EDUPAGE

NSA DECLASSIFIES ENCRYPTION CODE
The National Security Agency for the first time has declassified its 80-bit-length Skipjack encryption algorithm and its 1,024-bit-length key exchange algorithm, and made them publicly available. "This declassification is an essential part of the Department of Defense's efforts to work with commercial industry in developing reasonably priced computer-protection products," says the Pentagon. "This declassification decision will enable industry to develop software- and smart card-based security products, which are interoperable with Fortezza." The Skipjack algorithm is used in the Fortezza PC smart card, which controls access to computers in the Defense Message System and other DoD applications. (EE Times 24 Jun 98)

[MK notes: Declassification conforms to Kerchoff's Maxim, which states that the strength of an encryption algorithm must not depend on its secrecy.]

Category 44.1 *Crypto algorithms*

1998-07-30 **AES cryptography algorithm**

Newsbytes 151

NTT proposed their new E2 algorithm to the NIST as a candidate for the AES (Advanced Encryption Standard) that will eventually replace the DES. E2 is a new symmetric-key encryption algorithm using a 128-bit block-cipher technique.

Category 44.1 *Crypto algorithms*

1998-09-08 **encryption Vernam cipher one-time pad pseudorandom numbers**

EDUPAGE

TriStrata Security Inc. announced a Vernam cipher (one-time pad) using a pseudorandom number generator that it claimed provided a big enough keyspace to preclude successful attacks using the usual cryptanalytic approaches. Cryptographers expressed reservations about whether the relatively simple encryption would withstand rigorous testing. For the meantime, analysts were interested by the high speed of encryption, which allowed real-time encryption of high-volume multimedia streams such as audio and video carried over the Net.

Category 44.1 *Crypto algorithms*

1999-04-14 **encryption algorithm patent elliptic curve smart cards**

AMERICAN BANKER

RSA Data Security Inc. was awarded a US patent on "storage-efficient basis conversion," a technique that would enhance interoperability between different implementations of elliptic-curve cryptography. According to Jeffrey Kutler, writing in _American Banker_, "RSA said the existence of two common but conflicting numbering systems for ECC limits its usability and acceptance. Basis conversion is said to resolve the incompatibility between the polynomial and normal bases of calculation- and in a manner efficient enough to be handled within small or constrained computing appliances such as pagers, cell phones, or smart cards."

Category 44.1 *Crypto algorithms*

1999-08-16 **Advanced Encryption Standard**

EDUPAGE; American Banker, Crypto-Gram 99 08

U.S. UPGRADE OF ENCRYPTION PUTS BANKS IN PIVOTAL ROLE [EDUPAGE]
The National Institute of Standards and Technology (NIST) last week named five finalist algorithms as candidates to replace the federal Data Encryption Standard (DES). NIST has been working since 1997 to develop a standard to replace DES, and a final algorithm may not be chosen for another year. The new Advanced Encryption Standard (AES) will have a key length of at least 128 bits, compared with DES' 56-bit key length. Experts say unscrambling strings of 128 bits or more could take billions or trillions of years. However, even after the adoption of AES, privacy issues and questions of data encryption and digital certificates in e-commerce will remain. After May 15, NIST will "study all available information and propose the AES, which will incorporate one or more AES algorithms selected from the finalists," according to the NIST Web site. NIST aims for universal adoption of AES. (American Banker 08/16/99)

[MK adds: Bruce Schneier published an excellent review of the situation in his Crypto-gram 99-08 < http://www.counterpane.com/crypto-gram-9908.html >.]

Category 44.1 *Crypto algorithms*

1999-10-01 **encryption e-mail Web startup new company service**

National Post (Canada)

Zero-Knowledge Systems of Montreal announced that three major venture capital companies had decided to invest in its Freedom 1.0 software project that will provide Internet users with strong encryption and privacy protection against tracking by Web site operators.

Category 44.1 *Crypto algorithms*

1999-12-15 **crypto algorithm fast matrices**

CNN news.com http://www.news.com/News/Item/0,4,30930,00.html

Sixteen year old genius Sarah Flannery of Cork in Eire invented a new approach to encryption that uses 2x2 matrices and looked to be even faster than the widely-used RSA algorithm for public key encryption. Cryptographers expressed interest but warned that it would be some years before the strength (resistance to cryptanalysis) of the new algorithm could be evaluated. In fact, however, Flannery herself cracked the algorithm and published the results in December 1999, eliciting praise from professional cryptographers.

Category 44.1 *Crypto algorithms*

2000-06-30 **encryption anonymity distributed systems free speech**

NewsScan, Washington Post http://www.washingtonpost.com/wp-dyn/articles/A21689-2000Jun29.html

Researchers at AT&T Labs have created a system called Publius that will make it very difficult trace the authorship or to remove files placed on the Internet without the direct participation of those who created them. The technology is described at www.cs.nyu.edu/waldman/publius, and works by encrypting and dividing files into pieces and then distributing them over a number of servers throughout the Web. A file's creator would be able to decide who and when it could be reassembled or removed. Called "Publius," the technology has been named in honor of American Founding Fathers Alexander Hamilton, John Jay, and James Madison who used that pseudonym when they anonymously published their famous "Federalist Papers." (Washington Post 30 Jun 2000)

Category 44.1 *Crypto algorithms*

2000-10-03 **encryption algorithm standard open**

NewsScan, New York Times
http://partners.nytimes.com/2000/10/03/technology/03CODE.html

The U.S. Department of Commerce . . . picked a new encryption standard to replace DES, the algorithm used for decades to scramble and unscramble messages and data between computer users. A play on the names of the two Belgian computer scientists who developed it (Vincent Rijmen and Joan Daemen), Rijindael is described in http://www.nist.gov/aes, along with the discussion surrounding its selection. The scientists are making their algorithm freely available. "We both make enough to have a decent life. We can buy the things we want to buy," said Mr. Rijmen. Ms. Daeman, looking to the future, added: "This makes us known. The fact that people know you as an expert, you can gain money, if you play it in the right way... I hope, I hope." (New York Times 3 Oct 2000)

Category 44.1 *Crypto algorithms*

2001-02-12 **encryption stream cipher**

NewsScan

VANISHING ENCRYPTION
Harvard computer science professor Michael Rabin and his doctoral student Yan Zong Bing have developed a way of sending messages using an encryption scheme that can not be broken, because the code is created from a stream of random numbers that are never stored in the computer's memory and in effect vanish at the same time a message is coded or decoded. Dr. Richard Lipton of Princeton and Georgia Tech says: "It's like in the old 'Mission Impossible,' where the message blows up and disappears." But some computer scientists, such as Professor Dorothy Denning at Georgetown, say that the technique is impractical for large messages, while Dr. Peter G. Neumann at SRI International suggests that cryptography's role in protecting privacy is more cosmetic than real: "If you think cryptography is the answer to your problem, then you don't know what your problem is." (New York Times 20 Feb 2001)
http://partners.nytimes.com/2001/02/20/science/20CODE.html

Category 44.1 *Crypto algorithms*

2001-11-26 **encryption algorithm intellectual property movies audio distribution**

NewsScan

DOROTHY DENNING AND THE DEVELOPMENT OF GEO-ENCRYPTION
Among the "next wave of innovators" identified by Time magazine, Georgetown computer science professor Dorothy Denning was chosen for her previous accomplishments in computer security as well for current work in pioneering a new field she calls geo-encryption, which provides a way to keep information undecipherable until it reaches its location. With geo-encryption, movie studios could be assured that when they used the Internet to distribute films they films would end up at movie theaters rather than in the hands of pirates, and the State Department could be assured that classified messages could only be decoded at embassies, and not by terrorists. (Time 26 Nov 2001)
http://www.time.com/time/magazine/article/0,9171,1101011126-184999,00.html

---

Category 44.1 *Crypto algorithms*

2002-10-04 **quantum cryptography telecommunications research development progress**

NewsScan

QUANTUM CRYPTOGRAPHY FOR SECURE GLOBAL COMMUNICATIONS
British researchers have been able to use quantum cryptography keys encoded in photons of light to communicate through air for 23 kilometers, and the expectation is that by March of next year this capability will be extended to 1000 kilometers — far enough to reach all LEO satellites. Because any measure of a photon will alter its quantum properties, quantum cryptography guarantees that any attempt to intercept a message will be evident. (New Scientist 2 Oct 2002)
http://www.newscientist.com/news/news.jsp?id=ns99992875

Category 44.1 *Crypto algorithms*

2003-06-06 **hack-proof communications cryptography bacnk government Quantum research Toshiba Cambridge**

NIPC/DHS

June 06, vnunet.com — 'Hack-proof' cryptography goes quantum.

Researchers have developed new technology that could allow companies to implement hack-proof communications in three years. The technology, based on quantum cryptography, was demonstrated by UK-based Toshiba Research Europe last week working over distances of 100km for the first time. Research laboratory group leader Andrew Shields explained that the technology will be applicable for large organizations such as banks and government departments needing highly secure links between local sites. Quantum cryptography allows users on an optical network to guarantee security by encoding each transmitted bit with a single particle of light. Commercial products could be available in less than three years, according to Shields. The Department of Trade and Industry (DTI) in London, England, is partially funding further research into the technology by Toshiba, the University of Cambridge and Imperial College, London.

Category 44.1 *Crypto algorithms*

2004-05-17 **quantum cryptography European Union EU response Echelon**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/story/0 ,10801,93220,00.html

May 17, Computer World — EU seeks quantum cryptography response to Echelon.

The European Union (EU) plans to invest $13 million during the next four years to develop a secure communication system based on quantum cryptography, using physical laws governing the universe on the smallest scale to create and distribute unbreakable encryption keys, project coordinators said on Monday, May 17. If successful, the project will produce the cryptographer's Holy Grail -- absolutely unbreakable code -- and thwart the eavesdropping efforts of espionage systems such as Echelon, which intercepts electronic messages on behalf of intelligence services. "The aim is to produce a communication system that cannot be intercepted by anyone, and that includes Echelon," said Sergio Cova, a professor from the electronics department of Milan Polytechnic and one of the project's coordinators. "We are talking about a system that requires significant technological innovations. We have to prove that it is workable, which is not the case at the moment." Major improvements in geographic range and speed of data transmission will be required before the system becomes a commercial reality, Cova said.

Category 44.1 *Crypto algorithms*

2004-05-17 **key exchange quantum cryptography NIST speed of light**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/25948−1.html

May 17, Government Computer News — NIST doing crypto key exchanges at the speed of light.

The National Institute of Standards and Technology (NIST) is pushing the speed limit on cryptographic key exchanges on its new quantum communications test bed. The May 3 issue of Optics Express, the online journal of the Optical Society of America, described a demonstration of NIST's quantum key distribution system that delivered usable bits in the form of individual photons at the rate of 1Mbps. The process involves sending individual photons—elemental particles of light—in different polarizations and orientations to represent individual bits. The laws of physics declare that observing an elemental particle such as a photon changes it, making eavesdropping essentially impossible. "Detecting a photon involves its destruction," said Charles Clark, chief of the Electron and Optical Physics division. "If someone tried to eavesdrop, they would induce an error rate that would be so high it would be noticed." The system does not encrypt data; it only exchanges bits that can be used for an encryption key.

Category 44.1 *Crypto algorithms*

2004-08-17 **cryptographic algorithm weaknesses found MD5 SHA-1 US Digital Signature Standard DSS PGP SSL**

DHS IAIP Daily; http://news.com.com/Crypto+researchers+abuzz+over+flaws/2100 −1002_3− 5313655.html?tag=nefd.lede

August 17, CNET News.com — Crypto researchers abuzz over flaws.

News that mathematical functions embedded in common security applications have previously unknown weaknesses have recently surfaced in encryption circles. French computer scientist Antoine Joux announced Thursday, August 12, that he had uncovered a flaw in an algorithm called MD5, often used with digital signatures. Then four Chinese researchers released a paper that reported a way to circumvent MD5 and other algorithms. Eli Biham and Rafi Chen, researchers at the Technion institute in Israel, reported some early work toward identifying vulnerabilities in the SHA-1 algorithm at the Crypto 2004 conference in Santa Barbara, CA on Tuesday, August 17. SHA-1 is embedded in popular programs like PGP and SSL. It is certified by the National Institute of Standards and Technology and is the only signing algorithm approved for use in the U.S. government's Digital Signature Standard. The MD5 and SHA-1 algorithms are known to computer scientists as hash functions. They take all kinds of input, from an e-mail message to an operating-system kernel, and generate what's supposed to be a unique fingerprint. If a malicious attacker could generate the same fingerprint with a different input stream, the cloned fingerprint -- known as a hash collision -- would certify that software with a back door is safe to download and execute. It would help a crook who wanted to falsely sign an e-mail instructing that someone's bank account be emptied.

Category 44.1 *Crypto algorithms*

2004-10-15 **quantum encryption authentication research Boston University BBN Bolt Beranek Newman photons**

NewsScan; http://theage.com.au/articles/2004/10/14/1097607360143.html

NETWORK SECURITY SET FOR QUANTUM LEAP

It's a hacker's nightmare but a dream for bankers and spies: A computer network so secure that even the simplest attempts to eavesdrop will interrupt the flow of data and alert administrators to the snooping. The work by researchers at Harvard University, Boston University and BBN Technologies is the closest scientists have come to a realworld quantum encryption system that uses light particles called photons to lock and unlock information instead of random-number "keys."

Category 44.1 *Crypto algorithms*

2005-02-07 **National Institute of Standards and Technology NIST SHA-1 hash algorithm change SHA-256 SHA-512 no emergency**

DHS IAIP Daily; http://www.fcw.com/fcw/articles/2005/0207/web−hash−02−07−05. asp

NIST PLANNING TO CHANGE WIDELY-USED CRYPTOGRAPHIC HASH FUNCTION

Federal agencies have been put on notice that National Institute of Standards and Technology (NIST) officials plan to phase out a widely used cryptographic hash function known as SHA-1 in favor of larger and stronger hash functions such as SHA-256 and SHA-512. The change will affect many federal cryptographic functions that incorporate hashes, particularly digital signatures, said William Burr, manager of NIST's security technology group, which advises federal agencies on electronic security standards. "There's really no emergency here," Burr said. "But you should be planning how you're going to transition — whether you're a vendor or a user — so that you can do better cryptography by the next decade."

Category 44.1 *Crypto algorithms*

2005-02-20 **new cryptographic protocol secure wireless network delayed password disclosure Indiana University source code release 2005**

DHS IAIP Daily; http://www.newscientist.com/article.ns?id=dn7037

NOVEL CRYPTOGRAPHIC PROTOCOL COULD HELP SECURE WIRELESS COMPUTER NETWORKS.

Markus Jakobsson and Steve Myers of Indiana University demonstrated a new security scheme, dubbed "delayed password disclosure," at the American Association for the Advancement of Science meeting in Washington, DC, on Saturday, February 19. Existing security protocols focus on securing the link between two machines to counteract eavesdropping. But making sure that a computer is connected to a legitimate access point in the first place is also important. If a hacker uses his computer as a fake access point and then relays the messages on to a real one, the information can be stolen covertly. The delayed password disclosure protocol counteracts this threat by allowing both parties to use a pre-arranged password or pin for authentication, but prevents this from being revealed during communications. Jakobsson adds that the scheme would be not be noticed by users, as they are only notified when the wireless link seems suspicious. Computer code for the protocol will be released in the next couple of months and a version for mobile phones should also be ready by the end of 2005.

44.2 Crypto products

Category 44.2 *Crypto products*

1997-08-20 **disaster recovery Internet backup storage**

COMTEX newswire

Netstore Data Recovery Service allows automated backup of data on portables, desktop PCs, workstations and servers over the Internet. Since only 7% of the UK's PC users back up their data regularly, such a service could be useful. User data are encrypted before being transmitted to the backup site using 40-bit DES encryption and access to the stored data is severely limited by multiple passwords.

Category 44.2 *Crypto products*

1998-10-22 **nanotechnology chip lock restriction logon encryption**

EDUPAGE, http://www.mdl.sandia.gov/micromachine/

EDUPAGE editors summarized some interesting developments on the nanotechnology front.

LOCK-ON-A-CHIP
Researchers at Sandia National Laboratories have developed a way to build a microscopic mechanical lock into computer chips, blocking hackers from accessing whatever information that chip is handling, including data on the hard drive. The lock's tiny gears are created as part of the chip-making process, and only by typing a combination of six letters selected by the computer owner will the chip turn on. The chip lock design, which will cost only about a dollar more per chip, will be perfected and brought to market in about two years, say the researchers. (Wall Street Journal 22 Oct 98)

Category 44.2 *Crypto products*

1998-11-04 **encryption tool package software commercial Blowfish**

http://www.internetnews.com/prod-news/1998/11/0403-indian.html

Using the Blowfish encryption algorithm developed by U.S. cryptographer Bruce Schneier, the Signitron Company of Calcutta, India <http://www.bangaloreit.com/software_scenario.htm> placed a new encryption package on the market. EMD Armor (sold as Sigma 2000), the software costs about $38 but is claimed to provide strong (447-bit keyspace) encryption for PCs at a substantial speed (60Mb per minute).

Category 44.2 *Crypto products*

1998-11-24 **VPN encryption e-commerce firewall hardware encryption**

CNET news.com http://www.news.com/News/Item/0,4,29197,00.html

Check Point firewalls received a performance boost when Check Point codeveloped hardware encryption accelerators to speed the operations of virtual private networks. Working with Chrysalis-ITS, the two companies provided alternatives to a competing product pair, the Cisco Systems PIX firewall teamed with the Ravlin hardware encryption accelerator from RedCreek.

Category 44.2 *Crypto products*

1999-01-19 **cryptography embedded encryption chip processor export**

Washington Post

INTEL TEAMS UP WITH SECURITY COMPANY
hrough an alliance with the computer encryption company RSA Data Security Inc., chip maker Intel Corp. Will develop and manufacture high-performance chips with embedded RSA encryption technology. One question yet to be resolved is whether the chips will meet various export restrictions imposed by the U.S. Government, which fears that such technology could fall into the hands of international criminals or terrorists. Industry analyst David Wu says, "These high-performance chips are going to make Internet commerce more safe. It helps the overall computer industry, but Intel may have to use good, persuasive lobbyists and lawyers in Washington to get them accepted." (AP/Washington Post 19 Jan 99)

Category 44.2 *Crypto products*

1999-01-28 **laptop security smart cards inactivation theft encryption**

EDUPAGE; TechWeb

SECURITY-CONSCIOUS THINKPADS
IBM is offering a new feature on its popular ThinkPad laptops — a two-layer security system to protect the mobile machines and their files. The IBM Smart Card Security kit provides software that automatically encrypts data as it is stored on a computer, and a personal ID smart card that carries the encryption key for decoding the information. In addition, an Asset ID tag prevents access to data if the computer has been removed without authorization from the designated premises. Companies can place sensors around doorways that will inactivate the computer the computer through a wireless radio-frequency transmitter. "Now you can tie the face to the asset," says Sam Dusi, IBM's worldwide marketing director for ThinkPads. "It's not just who left the building but what they left with." According to the Computer Security Institute, companies incurred losses of more than $11 million in stolen laptops during 1996 and 1997. (TechWeb 28 Jan 99)

Category 44.2 *Crypto products*

1999-02-15 **random number generator chip processor encryption algorithms**

Crypto-gram 99 02

Bruce Schneier, famed cryptographer and author of the Crypto-gram monthly free newsletter (see < http://www.counterpane.com for> details and back issues) hailed Intel's inclusion of a random-number generator on the new Pentium III chip. He wrote, "This is excellent news. I know nothing about how it works (or even if it is any good), but using techniques such as Yarrow, we can take even a mediocre hardware random number generator and turn it into something that is good for cryptographic applications." [Yarrow is Bruce Schneier and John Kelsey's pseudo-random number generator algorithm, available free from Counterpane Systems. See < http://www.counterpane.com/yarrow.html > for details.

Category 44.2 *Crypto products*

1999-02-23 **hardware encryption antivirus product access control**

PR

RVT Technologies, Inc. announced what they described as revolutionary PC-card based encryption, anti-virus and access-control technology for PCs.

Category 44.2 *Crypto products*

1999-03-15 **encryption algorithm public-key cryptosystem cryptography portable hand-held**

Crypto-gram; PC Week 99 3
http://www.zdnet.com/pcweek/stories/jumps/0,4270,383613,00.html

The Palm VII palm computer from 3-Com included elliptic curve public-key cryptography from Certicom.

Category 44.2 *Crypto products*

1999-04-15 **LINUX operating systems cryptography VPN virtual private**

Wired
http://www.wired.com/news/print_version/technology/story/19136.html?wnpg=all

Linux aficionados gained a new tool for secure communications when the Linux Free S/Wan project released its new server software for virtual private networking over the Internet. Funded in part by the Electronic Frontier Foundation, the largely Canadian team of software engineers wrote the product despite resistance from elements in the law enforcement community who fear secure communications among criminals will make evidence-gathering much harder.

Category 44.2 Crypto products

1999-05-15 **encryption algorithms tools kits**

Crypto-gram, http://www.eskimo.com/~weidai/cryptlib.html 99 05

Crypto++ v3.1 was released in May 1999. According to the notes on < http://www.eskimo.com/~weidai/cryptlib.html >, "Crypto++ is a free C++ class library of cryptographic schemes. Currently the library consists of the following, some of which is other people's code, repackaged into classes:
* a class hierarchy with an API defined by abstract base classes
* AES candidates: RC6, MARS, Rijndael, Twofish, Serpent
* other symmetric block ciphers: IDEA, DES, Triple DES, RC2, RC5, Blowfish, Diamond2, TEA, SAFER, 3-WAY, GOST, SHARK, CAST-128, Square
* generic cipher modes: CBC padded, CBC ciphertext stealing (CTS), CFB, OFB, counter mode
* stream ciphers: ARC4, SEAL, WAKE, Sapphire, BlumBlumShub
* public key cryptography: RSA, DSA, ElGamal, Nyberg-Rueppel (NR), BlumGoldwasser, Rabin, Rabin-Williams (RW), LUC, LUCELG, Elliptic Curve Cryptosystems
* padding schemes for public-key systems: PKCS#1 v2.0, OAEP, PSSR, IEEE P1363 EMSA2
* key agreement schemes: Diffie-Hellman (DH), Unified Diffie-Hellman (DH2), Menezes-Qu-Vanstone (MQV), LUCDIF
* one-way hash functions: SHA-1, MD2, MD5, HAVAL, RIPEMD-160, Tiger
* message authentication codes: MD5-MAC, HMAC, XOR-MAC, CBC-MAC, DMAC
* cipher constructions based on hash functions: Luby-Rackoff, MDC
* pseudo random number generators (PRNG): ANSI X9.17 appendix C, PGP's RandPool
* Shamir's secret sharing and Rabin's information dispersal scheme
* DEFLATE (gzip compatible) compression/decompression
* fast multi-precision integer operations
* prime number generation and verification
* various miscellaneous modules such as base 64 coding and 32-bit CRC
* A high level interface for most of the above, using a filter/pipeline metaphor
* benchmarks and validation testing.

Category 44.2 Crypto products

1999-09-28 **encryption standard e-commerce wireless telephony public key infrastructure**

EDUPAGE; Financial Times (London)

IT COMPANIES PROMOTE NEW STANDARD FOR PHONE SECURITY
EDS, France's Gemplus, Sonera, and Ericsson have founded a forum called "Radicchio" to promote a world encryption standard. Known as "public key infrastructure," the technology provides security for mobile phone-based electronic commerce transactions. The technology can be embedded into a silicon chip that is located inside typical GSM handsets. Analysts believe that the mobile commerce market could reach $66 billion in the next four years, but forum founding members are concerned that security issues could impede the emerging market. The European initiative is currently pursuing new members, such as industry players and governments. Members of Radicchio say there could be 600 million mobile phones connected to the Internet by 2004, and easing security fears could go a long way toward making electronic transactions ubiquitous. (Financial Times 09/28/99)

Category 44.2 Crypto products

1999-10-07 **encryption confidentiality privacy e-mail temporary**

EDUPAGE; AP, USA Today

'SELF-DESTRUCT' E-MAIL OFFERS VIRTUAL PRIVACY [EDUPAGE]
The problem of e-mail being stored on computers on both the sending and receiving end as well as along the networks they travel long after being erased by sender and recipient — and sometimes coming back as evidence, as in the Iran-Contra and Microsoft antitrust cases — could become a thing of the past after the introduction of a new system from San Francisco-based startup Disappearing. The Disappearing system creates a temporary "key" for sender and recipient to encrypt and decrypt messages. After a certain amount of time set by the sender, the "key" will be destroyed at Disappearing's site and the e-mail message will no longer be readable. The system should be available in the first part of 2000. (USA Today 10/07/99)

[MK adds: However, anyone who keeps a copy of the decrypted text of the self-destructing e-mail would be able to keep that indefinitely.]

Category 44.2 *Crypto products*

1999-11-16 **secure e-mail privacy self-destruct VPN server retract**

OTC

The 1on1mail.com company announced a new feature for its self-destructing secure e-mail. The server-based VPN e-mail allows cancellation of unread e-mail after it is sent. The PR materials issued by the company made some silly claims, though. Although the "Your Eyes Only" feature prevents Windows copy/paste operations, it may not defeat taking a snapshot using operating system features such as printscreen. The PR announcement also claimed, "1on1mail.com is also the only secure e-mail technology that keeps all messages encrypted in memory, not just to disk
like other e-mail solutions." [The notion that the information is kept encrypted in memory (with implication that it is not decrypted) is silly given that a readable version is on the screen. Where do these marketing droids think the screen version comes from? Mars?] This company also offered anyone capable of deciphering any of its encrypted e-mail "within a reasonable period of time" would be given $50K as a prize.

Category 44.2 *Crypto products*

1999-12-07 **encryption 3DES European**

Reuters

Finnish telecommunication operator Sonera announced in December that it was the first non-US telecommunications firm to use the 168-bit 3DES algorithm in firewalls and virtual private networks (VPNs).

Category 44.2 *Crypto products*

2000-01-27 **encryption algorithm**

NewsScan, ZDNet, NEC press release, Investor's Business Daily
http://www.investors.com/

NEC's new Cipherunicorn-A encryption product was announced at the Encryption and Information Security Symposium in Japan at the end of January 2000. The new approach uses stealth techniques such as generating a number of false keys and varying the encryption keylength from 128 bits to 192 to 256 during the course of the stream encryption process. NEC researchers claimed that the new product would be the most powerful encryption tool in the world today, making practical cryptanalysis extremely difficult.

Category 44.2 *Crypto products*

2000-02-28 **encryption e-mail commercial free source code export restrictions**

Crypto-gram http://www.counterpane.com/crypto-gram-9906.html, CMPnet 99 06

Hushmail < http://www.hushmail.com > and ZipLip offered free encrypted e-mail to anyone. Hushmail published its source code, which was not developed in the US, thus evading all US crypto export regulations. [Note that contrary to some mistaken news reports, it has never been illegal to use encryption in the US or to send encrypted e-mail or anything else encrypted out of the US. The only restrictions were on the encryption algorithms themselves.]

Category 44.2 *Crypto products*

2001-10-12 **PGP NAI sale encryption product**

Wired http://www.wired.com/news/privacy/0,1848,47551,00.html

In Oct 2001, NAI announced that it would sell its PGP division. Sales were poor in part because of the availability of PGP freeware on the Web. [The division was purchased by a newly-formed PGP Corporation in June 2002.
< http://www.pgp.com/company/faqs.html >]

Category 44.2 *Crypto products*

2002-01-20 **broadband wireless encryption**

Security Wire Digest 4 5

CERAGON OFFERS BUILT-IN ENCRYPTION SOLUTION IN WIRELESS SYSTEM
Ceragon Networks, a provider of high-capacity broadband wireless systems for cellular operators, enterprises and communications service providers, last week introduced EncryptAir. The product encrypts data at channel rates of 155 Mbps and above and supports secure connectivity over SDH/SONET, IP and ATM network protocols.

http://www.ceragon.com

Category 44.2 *Crypto products*

2002-03-08 **encryption software**

NewsScan

NETWORK ASSOCIATES DISCONTINUES PGP
It's hard to sell something that's given away free. Networks Associates is shutting down its division responsible for marketing and supporting PGP ("Pretty Good Privacy"), the leading encryption software, because it's available free on the Web, leaving corporate users little reason to pay money for the product. Network Associates will continue support of PGP for existing customers until their contracts expire. (San Jose Meavailabilityrcury News 7 Mar 2002)
http://www.siliconvalley.com/mld/siliconvalley/2814647.htm

Category 44.2 *Crypto products*

2002-04-22 **palmtop computer identification authentication I&A encryption software**

Security Wire Digest 4 31

KASPERSKY LAB INTRODUCES SECURITY FOR PALM OS
Kaspersky Lab, a data-security software developer, last week released Kaspersky Security for Palm OS, which it says is a full-scale defense system for handhelds and mobile devices operating on Palm OS. According to the company, the suite is comprised of two modules; one that controls access to a device using a reliable password structure on the system level and another that controls authorized access on the application level using encrypted data.
http://www.viruslist.com

Category 44.2 *Crypto products*

2002-04-22 **palmtop encryption synchronization software**

Security Wire Digest 4 31

CHAPURA UNVEILS CLOAK 2.0
Chapura, a provider of synchronization software for handhelds, last week introduced Cloak 2.0, encryption software designed to store, protect, retrieve and share personal information using virtually any Palm OS handheld or Windows-compatible PC. According to the company, Cloak 2.0 can share and back up Cloak accounts via secure, encrypted files.
http://www.chapura.com

Category 44.2 *Crypto products*

2002-04-22 **palmtop computer VPN secure communications public key cryptosystem infrastructure PKI PKC**

Security Wire Digest 4 31

FUNK SOFTWARE ANNOUNCES ADMITONE VPN CLIENT FOR POCKET PC
Funk Software, a developer of RADIUS/AAA and wireless LAN security solutions, last week released the beta version of AdmitOne VPN Client for Pocket PC, software that lets handheld users establish a secure connection over a wireless link to enterprise networks. According to the company, AdmitOne VPN Client for Pocket PC implements IPsec and Internet Key Exchange technologies to fully protect the privacy of data being transmitted, and prevents the known security hazards of wireless communications including wireless eavesdropping and channel hijacking.
http://www.funk.com

Category 44.2 *Crypto products*

2002-04-22 **workstation encryption product trade-up programs**

Security Wire Digest 4 31

COMPANIES OFFER TRADE-UP PROGRAM TO PGP USERS
Information Security Corp. (ISC), a developer of cryptographic products, and data protection software developer PC Guardian both last week announced trade-up programs for all current Pretty Good Privacy (PGP) users. Under ISC's terms, PGP users may obtain a copy of the latest version of SecretAgent 5 file encryption utility for a reduced fee. SecretAgent 5 is a multipurpose file encryption utility that allows a user to encrypt and/or digitally sign any type of file. PC Guardian's upgrade offer requires a minimum order of 200 licenses and applies to enterprises that purchased Network Associates' PGP.
http://www.infoseccorp.com
http://www.pcguardian.com

Category 44.2 *Crypto products*

2002-06-01 **PGP Corporation**

PGP Corporation FAQ < http://www.pgp.com/company/faqs.html >

Was PGP Corporation once owned by Network Associates?
PGP technology has been in use for more than 10 years. PGP Inc., a private company, was formed in 1991 and acquired by Network Associates in 1997. Network Associates lacked a technology vision for the PGP product line and sold it to a newly formed, independent PGP Corporation in June 2002.

How was PGP Corporation formed?
PGP Corporation was incorporated in June 2002 by a management team composed of technology industry veterans and former PGP executives, developers, and patent holders. The group raised $14 million of venture funding from DCM-Doll Capital Management and Venrock Associates, two highly respected venture capital firms, to purchase assets, upgrade existing products, and develop new technology.

What is "new" about the new PGP Corporation?
The new PGP Corporation was founded on a completely new vision of securing digital assets. Although existing desktop products are technically excellent and extremely secure, they are impractical for universal deployed because they rely on users to learn how to use the security products and to follow policy by remembering when they must use security. The new PGP Corporation has taken the same trusted core cryptographic product and, through innovative technology, made it transparent to users. With the new PGP Universal product line, email security is now practical to deploy with all users because email is secured, and policy enforced, automatically by the network.

Category 44.2 *Crypto products*

2002-11-04 **quantum cryptography photons fiber optics**

NewsScan

PHOTONIC CRYPTOGRAPHY
A New York-based stat-up company called MagiQ (pronounced like the word 'magic') has developed a cryptographic system in which keys to the code are sent over a fiber optic cable as a stream of photons, which if observed by an intruder would (by the principles of quantum physics) be inevitably altered and thus rendered useless to the eavesdropper. The system will be used only over dedicated fiber cables, and the biggest customer for the system will undoubtedly be the military. Forrester Research analyst Laura Koetzle says, "The Defense Department is going to care, and that's big money for a small start-up to survive on." (New York Times 4 Nov 2002)

Category 44.2 *Crypto products*

2002-11-13 **wireless cellular mobile telephone encryption**

NewsScan

ISRAEL DEVELOPS SECURE MOBILE PHONE SYSTEM FOR MILITARY
Israel's military, in cooperation with Motorola Israel Ltd., has developed a secure mobile phone system called "Mountain Rose" and expects it to be fully operational by the beginning of 2004. The system's designers say that "there are two levels of redundancy so that in the case of a real crisis the person with the device will be able to communicate." The encryption was developed by Israel's Signal Corps, and not even Motorola knows how it works. (Reuters/San Jose Mercury News 13 Nov 2002)

Category 44.2 *Crypto products*

2004-01-16 **Internet browser security VPN VLAN SSL IPSec business**

DHS/IAIP Update

January 14, CNET News — Browser security takes off in VPNs.

Corporations are embracing a simpler, cheaper way of connecting remote workers to their networks -- Secure Sockets Layer (SSL) encryption. SSL is a significant step forward in Virtual Private Network (VPN) ease-of-use as an alternative to Internet Protocol security (IPSec). SSL technology has been embedded in most standard Web browsers for years. SSL VPNs enable access from virtually any Web browser, so they're a natural fit for remote access and extranet applications. For most Web-based applications, users don't have to use a client, making it easier to give access to the network. IPSec VPNs require the installation and configuration of software on all clients and can be clunky when it comes to remote access, often meaning interoperability issues that can leave many frustrated and stranded without access to critical network information. Most experts agree that the technologies are complementary. Though SSL VPN has many benefits, it also has its downside. One important element is end-point security. SSL VPN allows people to enter corporate networks via any Web browser, socompanies need to make sure that it has strong authentication to verify that users are authorized. It also needs strong policy management to ensure that people only access applications for which they have approval. As people can use any Web-enabled device for access, viruses from those machines can be transmitted to the corporate network.

Category 44.2 *Crypto products*

2004-01-16 **Internet browser security VPN VLAN SSL IPSec business**

NIPC/DHS; http://news.com.com/2100−1033_3−5140548.html

January 14, CNET News — Browser security takes off in VPNs.

Corporations are embracing a simpler, cheaper way of connecting remote workers to their networks — Secure Sockets Layer (SSL) encryption. SSL is a significant step forward in Virtual Private Network (VPN) ease-of-use as an alternative to Internet Protocol security (IPSec). SSL technology has been embedded in most standard Web browsers for years. SSL VPNs enable access from virtually any Web browser, so they're a natural fit for remote access and extranet applications. For most Web-based applications, users don't have to use a client, making it easier to give access to the network. IPSec VPNs require the installation and configuration of software on all clients and can be clunky when it comes to remote access, often meaning interoperability issues that can leave many frustrated and stranded without access to critical network information. Most experts agree that the technologies are complementary. Though SSL VPN has many benefits, it also has its downside. One important element is end-point security. SSL VPN allows people to enter corporate networks via any Web browser, socompanies need to make sure that it has strong authentication to verify that users are authorized. It also needs strong policy management to ensure that people only access applications for which they have approval. As people can use any Web-enabled device for access, viruses from those machines can be transmitted to the corporate network.

Category 44.2 *Crypto products*

2004-08-24 **quantum encryption cryptology security improvement NIST optical test bed**

DHS IAIP Daily; http://www.eet.com/article/showArticle.jhtml?articleId=30000
032

August 24, EE Times — Quantum encryption poised to tighten data security.

Quantum cryptology is starting to move out of the labs and into commercial systems that leverage advanced optical-networking technology. Three companies, Quantique SA of Geneva, Switzerland, MagiQ Technologies Inc. of Somerville, MA, and Tokyo-based NEC Ltd. have brought out encryption systems for optical networks that rely on fundamental physical laws to block eavesdropping. Also, a group based at Austria's University of Vienna is quickly moving toward a commercial quantum-encryption system. In a real-world experiment, a commercial bank and Vienna City Hall were connected via a fiber optic link that was run under the streets. The system was able to generate identical random sequences of bits at both ends of the fiber, and the key was used to send a secure bank transfer. However, some quantum-information experts, including experts at the National Institute of Standards and Technology (NIST), question whether quantum-encryption schemes are the absolute barrier to data theft claimed by proponents of the approach. NIST has a large effort in the area of data security and is attempting to stay ahead of the quantum-encryption game with a sophisticated optical testbed.

Category 44.2 *Crypto products*

2005-02-15 **instant messaging IM off-the-record OTR private encrypted chat no trace Gaim plugin AOL proxy University California Berkeley**

DHS IAIP Daily; http://news.zdnet.co.uk/internet/security/0,39020375,39187934,00.htm

INSTANT MESSAGING GETS PERFECT FORWARD SECURITY

Two researchers at the University of California at Berkeley have created an add-on to instant messaging (IM) that they claim will enable the participants to identify each other and have a secure conversation without leaving any proof that the chat occurred. The result, dubbed off-the-record (OTR) messaging by security researchers Ian Goldberg and Nikita Borisov, is a plug-in for the Gaim open source instant-messaging client that enables encrypted messages that do not leave a key that could be used to verify that the conversation happened. That attribute, known in cryptography as perfect forward security, also prevents snoopers from reading any copies of the conversation. In order for a secure and deniable IM conversation to occur, both parties need to have the off-the-record program installed on Gaim or use America Online's Instant Messenger with a server set up to be a proxy with software also developed by Goldberg and Borisov.

Category 44.2 *Crypto products*

2005-05-03 **quantum cryptography single photon light beam stop hackers interception key**

DHS IAIP Daily; http://www.reuters.com/newsSciTech.jhtml;jsessionid=QT1GT4CX50JBYCRBAEZSFFA

SCIENTISTS CLAIM DEVELOPMENT OF CODE TO STOP HACKERS

Australian scientists believe they have developed an unbreakable information code to stop hackers, using a diamond, a kitchen microwave oven and an optical fiber. Researchers at Melbourne University used the microwave to "fuse" a tiny diamond, just 1/1000th of a millimeter, onto an optical fiber, which could be used to create a single photon beam of light which they say cannot be hacked. Photons are the smallest known particles of light. Until now, scientists could not produce a single-photon beam, thereby narrowing down the stream of light used to transmit information. "When it comes to cryptology, it's not so much of a problem to have a coded message intercepted, the problem is getting the key (to decode it)," said university research fellow James Rabeau, who developed the diamond device. "The single-photon beam makes for an unstealable key."

Category 44.2 *Crypto products*

2005-07-26 **VoIP voice over IP Internet telephony surveillance snooping confidentiality data leakage fraud encryption protection defense**

RISKS; http://www.wired.com/news/technology/0,1282,68306,00.html 23 95

PHIL ZIMMERMANN TACKLES VoIP SECURITY

First there was PGP e-mail. Then there was PGPfone for modems. Now Phil Zimmermann, creator of the wildly popular Pretty Good Privacy e-mail encryption program, is debuting his new project, which he hopes will do for internet phone calls what PGP did for e-mail. Zimmermann has developed a prototype program for encrypting voice over internet protocol, or VOIP, which he will announce at the BlackHat security conference in Las Vegas this week.

Like PGP and PGPfone, which he created as human rights tools for people around the world to communicate without fear of government eavesdropping, Zimmermann hopes his new program will restore some of the civil liberties that have been lost in recent years and help businesses shield themselves against corporate espionage.

[Extract from article by Kim Zetter in Wired News]

Category 44.2 Crypto products

2006-02-22 **new security technology quantum cryptography photonic decoys foil hackers**

DHS IAIP Daily; http://www.networkworld.com/news/2006/022206−quantum− cryptography.html 23

STUDY SHOWS HOW PHOTONIC DECOYS CAN FOIL HACKERS.

A University of Toronto professor and researcher has demonstrated for the first time a new technique for safeguarding data transmitted over fiber-optic networks using quantum cryptography. Professor Hoi-Kwong Lo, a member of the school's Center for Quantum Information and Quantum Control, is the senior author of a study that sheds light on using what's called a photonic decoy technique for encrypting data. Quantum cryptography is starting to be used by the military, banks and other organizations that seek to better protect the data on their networks. This sort of cryptography uses photons to carry encryption keys, which is considered safer than protecting data via traditional methods that powerful computers can crack. Quantum cryptography is based on fundamental laws of physics, such that merely observing a quantum object alters it. Lo's study is slated to appear in the Friday, February 24, issue of Physical Review Letters.

Category 44.2 Crypto products

2006-03-13 **mobile computing larger database data theft loss threat encrypt hard drives**

DHS IAIP Daily; http://www.fcw.com/article92554−03−13−06−Print 23

MOBILE COMPUTING AND LARGER DATABASES POSE NEW RISKS FOR UNPROTECTED DATA.

As more companies disclose information losses and data theft, information technology companies have entered the market to sell products that encrypt entire hard drives. Those companies argue that encrypting all data on a disk is the best way to protect it from internal and external threats, including user carelessness. "It means the user can never make a mistake" that jeopardizes data security, such as putting classified material in an unclassified folder or onto a portable storage device, said Matt Pauker, co-founder of Voltage Security.

Category 44.2 Crypto products

2006-04-09 **IBM hardware security technology Secure Blue DRM PowerPC Intel AMD**

EDUPAGE; http://news.zdnet.com/2100-1009_22-6059276.html 23

IBM ADDS SECURITY TO HARDWARE

IBM has developed technology that adds hardware-level encryption to data on a range of electronic devices. Researchers at the company said that the technology, called Secure Blue, encrypts and decrypts data as it passes through a processor. Data are encrypted in RAM, as well, resulting in a high level of security for devices such as personal computers, cell phones, digital media players, and electronic organizers. The flip side to the protection that Secure Blue provides to users is a new level of control offered to other owners of content, such as media companies. Digital rights management (DRM), which dictates how content may be used, could be bolstered by IBM's new technology, allowing music producers, for example, another tool to restrict unauthorized usage of their intellectual property. Secure Blue has been demonstrated with IBM's PowerPC processor and is said to be compatible with processors from Intel and Advanced Micro Devices, though IBM said it is not currently in talks with those companies to add the technology to their chips.

44.3 Steganography

Category 44.3 *Steganography*

2004-06-30 **steganography data hiding software Steganos Germany law enforcement secret services**

NewsScan

STEGANOGRAPHY

The term "steganography" has come to mean the practice of hiding messages within graphics or music files. Fabian Hansmann of the German software maker Steganos explains: "Steganography has one big advantage -- that is you cannot prove that information exists. If you just use encryption, you will always see that there is a file that carries encrypted information." Hansmann characterizes his company's $60 security software suite as a "paranoid option" for advanced users who have the time and interest to hide their data. But Steganos products are under constant scrutiny by law enforcement officials. Hansmann says, "We regularly have inquiries from government agencies of all kinds, from foreign secret services to local police departments in Germany." (Reuters/USA Today 30 Jun 2004)

Category 44.3 *Steganography*

2004-08-15 **cyberspace Internet café Al Qaeda refuge terrorism Homeland Security steganography**

DHS IAIP Daily;
http://news.yahoo.com/news?tmpl=story&u=/latimests/20040815/ts_latimes/cyberspacegivesalqaedarefuge

August 15, Los Angeles Times — Cyberspace gives al Qaeda refuge.

Since Osama bin Laden and his followers were driven from their bases in Afghanistan, the al Qaeda terrorist network has demonstrated an increasing ability to exploit the Internet. Independent al Qaeda cells and the network's loose hierarchy use easily available encoding programs and simple techniques to exchange virtually undetectable messages between Internet cafes in Karachi and libraries in London. Messages can be embedded in image, sound or other files transferred over the Internet through a process called "steganography." The files cannot be distinguished without a decoding tool. The al Qaeda operatives are often people with everyday skills who have harnessed the Internet in a campaign against the United States and its allies. In an effort to gather information on potential recruits and donors, U.S. law enforcement agencies operate Websites that are set up to resemble extremist Islamic sites. Visitors leave an electronic trail when they enter the site. On the other side, al Qaeda can transmit false information to determine whether its members are being monitored by law enforcement.

Category 44.3 *Steganography*

2005-10-21 **steganography printer identification tracking surveillance criminal investigation identification originator**

RISKS; http://tinyurl.com/d9axy; http://www.eff.org/Privacy/printers/docucolor/ 24 08

PRINTER STEGANOGRAPHY

Many color printers (Xerox, HP, etc.) add barely visible yellow dots that encode printer serial numbers and time stamps (down to the minute). Intended primarily to combat counterfeiters, the purportedly "secret" steganographic code in color printer copies has now been decoded by four people at the Electronic Frontier Foundation. (The encoding is straightforward, and includes no encryption.) There are of course various slippery-slope privacy issues.

[Abstract by Peter G. Neumann]

[MK adds: Such tracking information may be helpful in criminal investigation of threats sent through printed documents or frauds involving such documents. In countries with repressive regimes, it may be used by authorities to track down publishers of samizdat (unauthorized newsletters). In corporations, it may be used to identify anonymous whistleblowers.]

45.1 PKI (Digital signatures / certificates)

Category 45.1 *PKI (Digital signatures / certificates)*

1997-03-04 **crypto public key infrastructure e-commerce**

EDUPAGE

GOV'T TESTING PUBLIC KEY INFRASTRUCTURE STANDARDS
The U.S. government is sponsoring public key infrastructure pilot projects in 10 federal agencies in an effort to determine which technologies should be adopted as standards. Agencies currently using encryption employ either the Digital Signature Standard (DSS) or the Digital Encryption Standard (DES). In considering other standards, the government is primarily interested in technologies that are royalty-free and that do not expose digital signatures when encrypting data for confidentiality. The pilot projects will enable the government to test a variety of technologies to determine what will work best before it spends large amounts of money on any particular technology. (BNA Daily Report for Executives 27 Feb 97)

Category 45.1 *PKI (Digital signatures / certificates)*

1997-05-07 **ENTRUST crypto PKI**

Canadian Corporate News

Entrust Technologies Inc. received Network Computing's Software Product of the Year award at Networld+Interop '97 exhibition for its PKI management products and two Network Computing "Well-Connected" awards for best encryption system and key management system. They also won the "Product of the Year" award from Network Magazine for best authentication product.

Category 45.1 *PKI (Digital signatures / certificates)*

1998-08-06 **certificate authorities digital signatures cryptography**

EDUPAGE; http://www.cren.net

EDUPAGE reported succinctly: "The Corporation for Research and Educational Networking (CREN) has begun to provide the academic and research communities with a top-level Certificate Authority Service that will validate certificates issued by other institutions and allow individuals at those institutions to share information and conduct online commerce in a cryptographically secure environment. MIT will be among the first institutions to use the service. See <http://www.cren.net> for more details."

Category 45.1 *PKI (Digital signatures / certificates)*

1998-09-01 **digital signature authentication identification taxes**

EDUPAGE

IRS PICKS VERISIGN FOR DIGITAL SIGNATURE TEST
The Internal Revenue Service has selected VeriSign Inc. for a two-year pilot program to test the use of digital signatures on tax returns filed electronically. If the program is successful, the agency may deploy the technology for wide-scale use in the year 2000. (Wall Street Journal 31 Aug 98)

[MK adds: if, of course, there _are_ any taxes being collected in the year 2000. . . .]

Category 45.1 *PKI (Digital signatures / certificates)*

1998-10-22 **certification authorities banks financial hierarchy**

Computer Wire 3522

In October, ABN AMRO, the Bank of America, Bankers Trust, Barclays, Chase Manhattan, Citibank, Deutsche Bank and Hypo Vereinsbank joined together with e-commerce facilitator CertCo to create a global digital certificate hierarchy for the banking industry. According to an article in _Computer Wire_, "It will establish an interoperable network of financial institutions that will act as certificate authorities. Each member will issue certificates to people and organizations based on a standard set of rules and business practices. Because all the partners contributed to those standards, CertCo reasons, they should be able to trust one another to implement them."

Category 45.1 *PKI (Digital signatures / certificates)*

1998-11-23 **VPN encryption e-commerce certificate authority firewall**

InternetWeek http://www.internetwk.com/news1198/news112398-6.htm

SecureZone 1.1 from Secure Computing Corporation announced virtual private network functions allowing integration of external digital certificate exchange.

Category 45.1 *PKI (Digital signatures / certificates)*

1998-12-15 **public key infrastructure elliptic curve cryptography**

CNET news.com http://www.news.com/News/Item/Textonly/0,25,29972,00.html

Certicom, provider of elliptic curve cryptography for digital authentication — especially of small and mobile devices such as cellular phones and palm-top computers — created a certification body for interoperation of equipment using its software. Competing RSA Data Security Inc., providers of the public key cryptography tools widely used for digital signatures in commercial software, was not invited to join the consortium even though they publicly announced support for elliptic curve cryptography.

Category 45.1 *PKI (Digital signatures / certificates)*

1998-12-15 **cryptography digital signatures authentication government**

Wired http://www.wired.com/news/print_version/business/story/16835.html

Entrust Technologies Inc. won a major contract with the government of Ontario, Canada's most populous province. Starting in 1999, Ontario would begin issuing 11M digital certificates for its residents to encourage secure electronic communications. This announcement signalled the start of a public-key infrastructure development program in Canada.

Category 45.1 *PKI (Digital signatures / certificates)*

1998-12-15 **NIST government standard digital signature commercial**

Federal Computer Week http://www.fcw.com/pubs/fcw/1998/1214/web-rsa-12-15-98.html

In December, NIST finally capitulated to common sense and allowed U.S. government agencies to use products using technology from RSA Data Security Inc. for digital signatures.

Category 45.1 *PKI (Digital signatures / certificates)*

1999-05-15 **encryption trust management public key infrastructure PKI software tools**

Crypto-gram, http://www.cis.upenn.edu/~angelos/keynote.html 99 05

Matt Blaze, Joan Feigenbaum et al. released version 2 beta of KeyNote, a small toolkit for implementing trust relationships. The description at < http://www.cis.upenn.edu/~angelos/keynote.html > includes the following text from RFC 2704:
Trust management, introduced in the PolicyMaker system [BFL96], is a unified approach to specifying and interpreting security policies, credentials, and relationships; it allows direct authorization of security-critical actions. A trust-management system provides standard, general-purpose mechanisms for specifying application security policies and credentials. Trust-management credentials describe a specific delegation of trust and subsume the role of public key certificates; unlike traditional certificates, which bind keys to names, credentials can bind keys directly to the authorization to perform specific tasks.

Category 45.1 *PKI (Digital signatures / certificates)*

1999-07-19 **digital signatures XML standard**

Network World Fusionhttp://www.nwfusion.com/newsletters/sec/0719sec1.html

In July 1999, the IETF (Internet Engineering Task Force) and the W3C (World Wide Web Consortium) agreed on a plan to develop XML standards for digital signatures of documents on the Web. The working group aimed at establishing the new standards by the end of 1999.

Category 45.1 *PKI (Digital signatures / certificates)*

2000-06-13 **e-commerce digital signatures contracts confirmation e-mail legislation proposal amendments**

NewsScan

Proposed legislation on electronic contracts . . . attracted the attention of tinkerers in Congress, who . . . inserted a number of changes in the past few weeks, with one addition requiring Internet users to send a number of repeated e-mails reconfirming their consent to the contract at every stage of a transaction, as well as demonstrating that they had absorbed every bit of legal boilerplate. That change drew protests from the financial community, which viewed it as overly cumbersome, but the extra consumer measures also gave pause to Phil Gramm, chairman of the Senate banking committee. Gramm is less worried by brokerages than by the tendency among his fellow lawmakers to apply the old regulatory culture to the new online frontier, pointing out that the new bill goes beyond anything that already applies in contract law. "What happened to 'Let the buyer beware?'" he asks. "Common law and a thousand years of paper contracts established duties and responsibilities for people participating in commerce. You don't want to change that relationship so that e-commerce undermines contracts and commerce." The bill underwent further change yesterday to remove some of the obstacles, but as one financial expert said, "We have gone from having two different versions of a bill that would have been an A or an A minus, to a low B at best." (Financial Times 13 Jun 2000)

Category 45.1 *PKI (Digital signatures / certificates)*

2000-06-15 **e-commerce digital signature law legislation**

NewsScan

In a vote of 426 to four, the U.S. House of Representatives . . . passed legislation [on 14 Jun 2000] that would make digital signatures legally binding. The bill had faced some opposition from consumer lobbyists, who worried that technology constraints might marginalize some consumers. The final language contains provisions for an "opt in" system where consumers must consent to receiving contracts and related information online. The bill does not specify any particular technology for creating digital signatures, leaving the issue open to competition in the marketplace. The Senate is expected to vote on the legislation in the coming weeks, paving the way for it to become law. (Financial Times 15 Jun 2000)

Category 45.1 *PKI (Digital signatures / certificates)*

2000-06-25 **digital signature e-commerce alliances**

NewsScan, San Jose Mercury News
http://www.sjmercury.com/svtech/news/breaking/merc/docs/080029.htm

Aided by new strategic alliances with Microsoft, IBM, Cisco, Sun and other technology partners, the iLumin Corporation plans to use its Digital Handshake technology to take advantage of recently passed federal legislation that allows "enforceable online transactions" using "signatures" that are actually heavily encoded scripts rather than images of handwritten signatures. The company says that digital signature technology will be used to facilitate $135 billion worth of e-commerce transactions within two years. (Reuters/San Jose Mercury News 25 Jun 2000)

Category 45.1 *PKI (Digital signatures / certificates)*

2000-07-05 **digital signatures e-commerce**

NewsScan, San Jose Mercury News
http://www.sjmercury.com/svtech/news/breaking/ap/docs/167385l.htm

The co-founder of signOnline Inc., one of the tiny companies that hopes to take advantage of the new federal legislation on digital signatures, predicts: "Eventually, we're all going to have digital signatures. You're going to see the whole world transformed. This really does change the world." Who will profit from the expanded use of digital signatures? Besides companies such as signOnline, which sells digital signature technologies and services, the big winners will e-commerce security companies such as VeriSign Inc. and Entrust Technologies Inc., that provide universally recognized digital certificates. But there will be some losers as well, and shipment companies such as Federal Express and United Parcel Service will probably see lesser demand for their overnight document delivery services as the use of digital signatures becomes more common. (AP/San Jose Mercury News 5 Jul 2000)

Category 45.1 *PKI (Digital signatures / certificates)*

2001-03-22 **digital certificates software authenticity fraud bogus impersonation quality assurance revocation list risk management security model**

RISKS 21 29

Many correspondents reported the issuance of bogus digital certificates assigned to Microsoft by Verisign. Jeff Savit's summary was as follows:

"Spoofing hazard: Verisign gave digital certificates under Microsoft name to an individual not from Microsoft. Microsoft issued a bulletin at < http://www.microsoft.com/technet/security/bulletin/MS01-017.asp > that describes the risk of running code that erroneously appears to be signed by Microsoft (eg: ActiveX controls), and discusses the risks due to not having a proper revocation mechanism.

Note that the certs were made available January 30th, so who knows what code has been accepted and executed since then. Microsoft is a victim in this particular instance."

Later contributions to RISKS and BUGTRAQ provided more details of the security breach.
Roy Sinclair pointed to a paragraph from the Frequently Asked Questions at < http://www.microsoft.com/technet/security/bulletin/MS01-017.asp >:

"The update is needed because of a characteristic of VeriSign code-signing certificates. Every certificate issuer periodically generates a Certificate Revocation List (CRL), which lists all the certificates that should be considered invalid. A field in every certificate should indicate the CRL Distribution Point (CDP) - the location from which the CRL can be obtained. The problem is that VeriSign code-signing certificates leave the CDP information blank. As a result, even though VeriSign has added these two certificates to its current CRL, it's not possible for systems to automatically download and check it. "

Sinclair continued, "The first question I have after seeing that is how many of the rest of the 500,000 certificates that Verisign says they have issued also do not have this CRL Distribution Point field properly filled in. In the lack of any information to the contrary I would hazard to guess that it's probably that none of the 500,000 certificates issued by Verisign have supplied the information that should be in this field. If this is truly the case then we have yet another problem of much wider scope than the improper issuance of two certificates, there are a great number of valid certificates which could be stolen or misused and even if Verisign were to add them to their CRL the certificates themselves don't point to the CRL so they won't be properly rejected. Two things need to be done, one is that software which checks certificates must be changed to warn users that certificates lacking a CRL are much more suspect and Verisign needs to re-place all certificates that currently lack this critical information with new certificates that have this field properly filled in. Additional questions that come to mind is how many other certifying agencies have also failed to fill in the information in this field and what percentage of the certificates being used today are unverifiable?"

Michael Sinz pointed to the well-known fallacy of confusing authentication with quality or trustworthiness.: "So, lets see - Microsoft says that ActiveX is secure as long as the software (ActiveX thing) is not from an 'evil' source. To prevent bad software from being used, they use digital signatures to identify the person or company who made the software such that you could either trust them or know who to go after when it does something bad. The OS and system infrastructure does not try to enforce anything other than to check these certificates and warn you based on your settings as to if you want to run unsigned software or any software signed by company 'X' or a number of other possible combinations of warnings. There is no built in security beyond that point. Once you say 'Yes, run it' you are opening up your system to complete control by the ActiveX control. Ok, in a perfect world, with no one wishing to do harm or rob you blind, such a mechanism would work just fine. The Internet is not such a world."

Category 45.1 *PKI (Digital signatures / certificates)*

2001-07-11 **digital certificate authority CA signature trust password single point of failure identification and authentication I&A**

NewsScan

MICROSOFT TO USE VERISIGN TO PROVIDE SECURITY FOR ".NET"
Microsoft's ".NET" and "Hailstorm" paid subscription services -- which will rely on customer willingness to store personal and credit information on a Microsoft system called Passport -- will be protected by the Internet security company VeriSign. VeriSign will provide "digital certificates" over the Passport system when extra security is needed for financial and other transactions requiring strict security protection. Customers will need to remember just a single password, but VeriSign's chief executive insists that simplicity won't take away from security: "The issue you deal with is that customers want ease-of-use but they also want higher levels of trust. Before, those two things were mutually exclusive, but now they can be as simple as one password." (AP/San Jose Mercury News 11 Jul 2001)
http://www.siliconvalley.com/docs/news/svfront/079055.htm

Category 45.1 *PKI (Digital signatures / certificates)*

2001-07-26 **bad PGP digital signature Microsoft security bulletins alerts**

RISKS 21 56

A report published in RISKS pointed to a serious problem with Microsoft security bulletins:

>For at least four months, Microsoft has been sending out security bulletins which fail a popular e-mail authentication system. As a result, the company could be opening the door to counterfeit bulletins from malicious hackers.

To protect against forgery, Microsoft's security response center digitally signs its bulletins with PGP before e-mailing them to subscribers of its security notification service. But since at least March, if recipients attempt to verify the messages' authenticity, PGP will issue a warning that the bulletins contain an invalid signature.

"The problem is that Microsoft's bulletins effectively look as if they're forged. And telling a Microsoft forgery from someone else's is virtually impossible," said Paul Murphy, head of information technology at Gemini Genomics, a genetic research firm in Cambridge, England. [...] <

[MORAL: check the digital signature after you publish a signed document.]

Category 45.1 *PKI (Digital signatures / certificates)*

2002-03-12 **I&A identification authentication digital certificates software**

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/2839790.htm

SUN TO OFFER DIGITAL IDENTIFICATION SERVICE
In a continued rivalry with Microsoft, Sun Microsystems will be offering software, hardware and service to provide corporations a way to offer their employees, customers and vendors user-authentication services and single sign-on procedures to disparate applications, from any device connected to the Internet. Called the Sun Open Net Environment Platform for Network Identity, it will be competing with Microsoft's Passport service. Aberdeen Group analyst Dana Gardner says the effect of the new Sun offering will be to "prevent any one player from getting too much control." The Enterprise Edition of the offering will manage up to 10,000 identities inside a firewall, for a price starting at $149,995; the Internet Edition will manage up to 250,000 identities outside a firewall, and is priced starting at $999,995. (Reuters/San Jose Mercury News 11 Mar 2002)

Category 45.1 *PKI (Digital signatures / certificates)*

2002-04-22 **I&A identification authentication access control digital certificates**

Security Wire Digest; http://www.entrust.com 4 31

ENTRUST LAUNCHES ENTRUST TRUEPASS 6.0
Entrust, an Internet security products and solutions provider, last week launched Entrust TruePass 6.0. According to the company, Entrust TruePass 6.0's zero-footprint software can help organizations securely verify the credentials identity of the individuals who are visiting and using their Web portal and secure the associated transactions. ActivCard, Datakey, GemPlus, Oberthur, Rainbow and Schlumberger are announcing plans to provide Entrust Ready Smart Cards that integrate with Entrust TruePass 6.0.

Category 45.1 *PKI (Digital signatures / certificates)*

2004-01-12 **PKI digital signatures UK European ecommerce internet**

NewsBits; http://www.securityfocus.com/infocus/1756

Digital Signatures And European Laws

Mirella Mazzeo published an extensive article reviewing legal aspects of digital signatures in the European context. She reviews the technology and recent administrative declarations of the European Community and concludes, "The PKI situation in Europe is still not consistent across all countries, however. Some countries, such as Italy, Austria, and Spain have well-developed infrastructure already in place; others such as Finland, Denmark, Germany, and France are still testing their PKI solutions. Further, some countries such as Holland and the United Kingdom have not even started deploying their public key infrastructure."

Category 45.1 PKI (Digital signatures / certificates)

2004-01-13 **VeriSign certificate absence confusion insecure transaction connection**

NIPC/DHS; http://verisign.com/support/vendors/exp-gsid-ssl.html

January 11, The Register — VeriSign dead cert causes net instability.

The expiration of one of VeriSign's master digital certificates on Wednesday, January 7, created confusion for Net users and glitches to the operation of some applications, notably Norton Anti-Virus (NAV). After the cert VeriSign used to sign other certs expired, the chain of trust was broken, leaving some aps unable to set up a secure connection. These apps then defaulted to trying to access Verisign's certificate revocation list server which, faced with a huge extra load, buckled under the pressure. Essentially, where there are problems, traffic needs to be directed to a new Global Server Intermediate Root CA. Users of Java aps and older IE browsers were affected by the issue but NAV users were worst affected. NAV Users saw their computers slow to a crawl and Microsoft office applications not starting properly because of the problem.Verisign has posted an advisory on the problem at the following Website detailing server updates needed to resolve application instability: http://verisign.com/support/vendors/exp-gsid-ssl.html.

Category 45.1 PKI (Digital signatures / certificates)

2004-01-16 **public key infrastructure PKI implementation government security**

NIPC/DHS; http://www.gao.gov/highlights/d04157high.pdf

January 15, Government Accounting Office — GAO-04-157: Status of Federal Public Key Infrastructure Activities at Major Federal Departments and Agencies (Report).

The federal government is increasingly using online applications to provide access to information and services, and to conduct internal business operations. As such, strong security assurances are necessary to properly safeguard data. The Government Accounting Office (GAO) found that Public Key Infrastructure (PKI) and its associated hardware, software, policies, and people can provide greater security assurances than simpler means of authenticating identity, such as passwords. Twenty of the 24 agencies reported that they are undertaking a total of 89 PKI initiatives, now in various stages of development. Agencies continue to face challenges, however, in PKI implementation, many of which are similar to those faced in GAO's 2001 report on the issue. Policy and guidance is often lacking or ill-defined, including in technical standards and legal issues. Insufficient funding for the high cost of PKI technology also is a challenge. Interoperability continues to be an issue, as integrating PKI with other systems at times requires significant change or even replacement. Another challenge is the administrative burden of training personnel for use and management of PKI.

Category 45.1 PKI (Digital signatures / certificates)

2006-03-23 **VeriSign Managed PKI input validation flaw vulnerability cross-site scripting attack**

DHS IAIP Daily; http://securitytracker.com/alerts/2006/Mar/1015813.html 23

VERISIGN MANAGED PKI INPUT VALIDATION FLAW IN 'HAYDN.EXE' PERMITS CROSS-SITE SCRIPTING ATTACKS.

A vulnerability was reported in VeriSign's Managed PKI. A remote user can conduct cross-site scripting attacks. Analysis: The 'haydn.exe' script does not properly filter HTML code from user-supplied input before displaying the input. A remote user can create a specially crafted URL that, when loaded by a target user, will cause arbitrary scripting code to be executed by the target user's browser. The code will originate from the site running the Managed PKI software and will run in the security context of that site. As a result, the code will be able to access the target user's cookies (including authentication cookies), if any, associated with the site, access data recently submitted by the target user via Web form to the site, or take actions on the site acting as the target user. Affected version: 6.0. Solution: The vendor indicates that, as a solution, a default HTML file must be constructed by creating a blank html file in the '/htmldocs/' directory labeled 'fdf_noHTMLFile.html'.

45.2 Digital cash

Category 45.2 *Digital cash*

2000-02-16 **e-commerce payment e-cash e-checks credit card currency**

NewsScan, Wall Street Journal

A new system offered by PayPal.com allows registered users to use an e-mail message to send a cash payment to anyone with an e-mail account on the Internet. The sender writes an amount onto an online form, and that amount is charged to the sender's credit card or bank account. The receiver of the e-mail can then have the amount transferred to his or her bank or credit card account, mailed in the form of a printed check, or kept in the receiver's own PayPal account (which can be set up immediately) for recirculation. One happy customer says: "PayPal is replacing currency. This is becoming the payment service of the Internet." CheckFree and eBay are two other companies that will be offering similar services, and PayPal has signed up 190,000 customers since its launch [in late 1999]. (Wall Street Journal 16 Feb 2000)

Category 45.2 *Digital cash*

2004-06-23 **electronic food stamps US Department of Agriculture debit cards advantages**

NewsScan

FOOD STAMP ERA OVER: THE SYSTEM GOES ELECTRONIC

Agriculture Secretary Ann M. Veneman has declared the end of the "paper era" of the food stamp program: "This month the food stamp program arrived in the 21st century. States are destroying the paper coupons, and we don't anticipate that we'll ever have to print them again." Everybody seems to like the new electronic debit cards -- the recipients avoid the stigma attached to the paper coupons, the grocers get paid faster, and the states find the electronic simpler and less open to fraud. Under the new system, each recipient has an account in which benefits are electronically deposited each month, and can be drawn on at the checkout line of a grocery store by
sliding a plastic card through the same device used for commercial debit or credit cards. One benefits recipient says that when he was a teenager he saw "addicts who would trade food stamps for drugs even though they had sick children starving," whereas with the debit cards "you have no choice but to purchase food."(New York Times 23 Jun 2004)

Category 45.2 *Digital cash*

2004-08-02 **banking Websites e-commerce Internet Explorer vulnerability flaw hole security threat**

NewsScan

TOP BANKING SITES VULNERABLE: RESEARCHER

The Web sites of three of Australia's four big banks are susceptible to cross-site scripting attacks, according to a British tech professional who gained prominence last year when he discovered a URL spoofing flaw in Microsoft's Internet Explorer browser. Sam Greenhalgh, who recently tested the Web sites of several British financial services companies and found many of them susceptible to the same kind of attacks, said the flaw resulted from sites not "sanitizing" information the user submits before displaying the information on the page: "If the information contains HTML, those HTML tags will be included on the site. Among other things this allows an attacker to include a tag that instructs the page to load a JavaScript file from another Web site." Greenhalgh provided demonstrations of injecting HTML on the sites using scripts he wrote himself. (The Age 2 Aug 2004) Rec'd from John Lamp, Deakin U.

[Note: "cross-site scripting:" Causing a user's Web browser to execute a malicious script. One approach is to hide code in a "click here" hyperlink attached to a URL that points to a non-existent Web page. When the page is not found, the script is returned with the bogus URL, and the user's browser executes it. -- from the Computer Desktop Encyclopedia, v18.2. See < http://www.computerlanguage.com >]

45.3 Micropayments

Category 45.3 *Micropayments*

1999-08-05 **e-commerce micropayments credit card phone company ISP Internet service provider**

Wall Street Journal

NEW WAVE OF FIRMS BETS CONSUMERS ARE RIPE FOR INTERNET 'MICROPAYMENTS'
Several new companies are offering ways for consumers to make "micropayments" online, with the aim of encouraging consumers to spend more freely on small items. For example, iPin will announce a plan Monday to enable consumers to roll small purchases onto their monthly ISP bills. Consumers who sign up with iPin will give the company their e-mail address and select a personal identification number. IPin says the use of PINs will be faster than using credit card numbers and will encourage impulse spending. IPin, which has already formed deals with a few small ISPs, is now testing its technology with AT&T's WorldNet Service. Retailers will pay iPin a lower processing fee than they would pay to credit card companies. IPin will then share these retailer fees with ISPs. Using a similar strategy, eCharge includes small purchases on consumers' phone bills. The company has a partnership with AT&T, through which it has access to most U.S. phone users. ECharge collects a fee from retailers, which it splits with AT&T and the local phone company involved. (Wall Street Journal 08/05/99)

Category 45.3 *Micropayments*

2002-11-26 **bandwidth metering spam file sharing copyright violations piracy swapping**

NewsScan

HIGH-SPEED ISPs CONSIDER PUTTING ON THE BRAKES
Many of the largest high-speed ISPs are considering capping the amount of bandwidth that their subscribers can use each month in an effort to put the brakes on rampant file-swapping. "Every major broadband provider is seriously weighing pros and cons of bandwidth consumption caps," says Michael Harris, president of research firm Kinetic Strategies. Leading the way is Bell Canada, whose DSL service has already instituted caps on bandwidth use, charging subscribers about 80 cents for each extra 100 megabytes used. The concept is controversial for several reasons: it requires ISPs to set up a traffic-monitoring system for each account and it forces the subscriber to self-ration bandwidth — a foreign concept to people accustomed to an all-you-can-eat approach to Internet use. Critics note that unwanted content, such as pop-up ads and pornographic spam, could waste subscribers' bandwidth, but Bell Canada says its policy has been a success so far. The company offers tiered levels of service allowing 2GB, 10GB and 20GB of monthly traffic, and the percentage of customers exceeding their allotment in any given month is small — between 6% and 8%. Cable companies are eyeing the Bell Canada experiment with interest, as their subscribers in particular are adversely affected by "bandwidth hogs." Meanwhile, the president of file-swapping company Grokster dismisses the efforts, saying, "They only thing they're going to accomplish is to make their customers angry." (CNet News.com 26 Nov 2002)

Category 45.3 *Micropayments*

2004-09-07 **micrpayments sucessful big business iTunes BitPass**

NewsScan

MICROPAYMENTS MORPHING INTO A MEGABUSINESS

The news that micropayment firm BitPass has just raised $11.75 million in venture capital and attracted former American Express Chairman James Robinson III to its board is signaling a resurgence in interest in micropayment systems that facilitate payment for digital content.
Jumpstarting the move -- following a series of crash-and-burn dot-coms like Flooz and DigiCash -- is the notable success of Apple's iTunes, which last week announced it had sold 125 million music downloads at 99 cents each. A recent study by TowerGroup indicates that the total market for Internet and wireless micropayments -- fueled by demand for digital content -- will increase by 23% annually over the next five years to $11.5 billion by 2009. "What it comes down to is that there simply must be a viable transaction model for smaller-cost products to make a dollar off e-commerce sales, but I think with what we've seen already in digital media, it's clear that people are figuring out how to make it work," says a Jupiter Research analyst. (CNet News.com 7 Sep 2004)

45.4 E-payments; e.g., credit-cards, e-brokers

Category 45.4 *E-payments; e.g., credit-cards, e-brokers*

1997-01-05 **Ecommerce SET**

EDUPAGE

A pilot project got underway in Denmark when Mastercard and IBM established an electronic commerce system for secure use of credit cards over the Internet in collaboration with a Danish bank. The trial applies the Secure Electronic Transaction standard (SET), which is expected to be in use in 50 pilot projects in 20 countries by the end of 1997.

Category 45.4 *E-payments; e.g., credit-cards, e-brokers*

1997-02-11 **electronic commerce smart cards**

EDUPAGE

VISA PLANS SMART CARD TEST
Visa International will launch a major trial of "electronic purse" cards in Great Britain, similar to the one it sponsored at the Atlanta Olympics last summer. Unlike the Olympic cards, the ones issued for the Leeds trial will be equipped with both public- and private-key encryption technology for security against hackers and other criminals. The cards contain a microchip storage capacity that can be credited and debited with a monetary value over a telephone line or at an ATM machine. (Wall Street Journal 10 Feb 97)

Category 45.4 *E-payments; e.g., credit-cards, e-brokers*

1997-07-12 **hackers onlin banking Internet Web**

Guardian Weekly

The Chartered Institute of Bankers in the United Kingdom commissioned an analysis of online-banking risks. The authors, Drs Anthony Gandy and Chris Chapman, pointed out that banking is already practically virtual today: many customers rarely visit their branch and carry on all their transactions using direct-deposit, credit-cards, debit cards and checks. Rational risks analysis would compare the risks of interception and data diddling to real-world risks resulting from widespread user errors such as keeping PINs near one's debit card, losing sight of one's credit card in restaurants, and giving out credit card numbers freely over the phone.

Category 45.4 *E-payments; e.g., credit-cards, e-brokers*

1997-07-20 **e-commerce SET**

EDUPAGE; http://www.visa.com/cgi-bin/vee/nt/ecomm/set/downloads.html?2+0

CREDIT CARD COMPANIES AGREE ON SECURITY STANDARD
Visa and MasterCard say they've agreed on a set of technical standards for secure electronic transactions, called SET 1.0. The two companies are already running pilot programs to test the standards in 25 countries, and hope to introduce the standard to the general market at the end of this year. "If we work together as an industry, this will go a lot faster," says Visa's senior VP for I-commerce. The companies hope that the new standard will be in wide use by next year. (InfoWorld Electric 18 Jul 97)

Category 45.4 *E-payments; e.g., credit-cards, e-brokers*

1997-08-19 **SET e-commerce crypto**

RISKS 19 31

Jerome Svigals, writing in RISKS, criticized the SET process because of three major vulnerabilities: "However, the SET process has three serious exposures - confirmed with IBM and HP/Verifone. The process does NOT know who is presenting the certificate. The process does NOT know if merchant employees have redirected the certificate through another merchant. All of the critical software is directly accessible by the card users, merchant employees and bank employees. Historically, these individuals have been the prime source of fraud in credit card transaction systems."

However, Phillip M. Hallam-Baker retorted that "The purpose of financial cryptography is to control, not eliminate, risk." He also pointed out that future revisions of SET would likely increase security step by step.

Category 45.4 *E-payments; e.g., credit-cards, e-brokers*

1997-10-05 **smart cards banking e-cash**

Reuters

In October, Chase Manhattan Corporation and Citicorp began a coordinated trial of the Visa Cash and Mondex smart cards in the New York City area. The banks hope to demonstrate customer and retail acceptance of the technology and to prove interoperability of the cards with standard hardware.

Category 45.4 *E-payments; e.g., credit-cards, e-brokers*

1997-11-24 **Internet Web security certification logo**

PR Newswire

MasterCard introduced its new "Shop Smart!" logo for certified Web sites dealing with financial information. See <http://www.mastercard.com> for details of certification criteria.

Category 45.4 *E-payments; e.g., credit-cards, e-brokers*

1999-06-14 **online purchase buy e-commerce electronic wallet**

EDUPAGE; Wall Street Journal

COMPANIES AGREE ON SINGLE STANDARD FOR ONLINE 'WALLET'
Microsoft, Sun Microsystems, AOL, and IBM have agreed on an electronic-commerce modeling language (ECML) standard for electronic wallets, which simplify online transactions for consumers. Credit card companies Visa International and MasterCard International will support ECML, and several retailers, including Nordstrom, have also agreed to endorse the format. For years, technology companies have been trying to gain widespread support for proprietary electronic wallet software, which retailers refused to embrace because of the need for special software or the reprogramming of a site. ECML will eliminate the need for retailers to require consumers to re-enter personal information for each purchase. Instead, personal information will be stored on the consumer's Web browser or on an Internet server. (Wall Street Journal 06/14/99)

Category 45.4 *E-payments; e.g., credit-cards, e-brokers*

2000-02-17 **authentication certificates postage encryption online e-commerce**

NewsScan, Wall Street Journal; Stamps.com
http://www.stamps.com/company/news/19991116a/; G2 TOR #193
http://www.g2news.com/BackIssuesTOR/TOR193.html#Stamps.com Loses Big

Event marketers like Ticktmaster.com, Tickets.com and Admission Network are moving quickly to implement technology that will enable customers to print their own tickets to rock concerts, sports events, and movies, but authentication of those do-it-yourself tickets is still an issue. Accordingly, they're turning to online postage sellers E-Stamp and Stamps.com to tap into their encryption technology and bar code techniques for secure online document printing. In response, Stamps.com, with backing from Paul Allen's Vulcan Ventures and some other investors, has formed EncrypTix Inc. to handle sales of event tickets, travel services and financial products like travelers checks. Forrester Research says of the three billion event tickets sold in the U.S. last year, about 10% were sold online — a figure that's expected to grow significantly once the print-your-own model is ready for primetime. (Wall Street Journal 17 Feb 2000)

In a related article, G2 Computer Intelligence's "The Online Reporter" said, "Stamps.com posted an operating loss of $41.8 million for the first quarter on revenues that rose 470% sequentially to $2 million."

Category 45.4 *E-payments; e.g., credit-cards, e-brokers*

2000-03-01 **e-cash electronic payments e-commerce**

NewsScan; http://www.billpoint.com/

Billpoint, a new Internet payment method developed by eBay.com and Well Fargo, will allow individual buyers and sellers using eBay's auction services to complete their transactions using the buyer's credit card and the seller's bank account. Once the sale is completed, the purchase amount will be transferred immediately into the seller's checking account. (Wall Street Journal 1 Mar 2000)

Category 45.4 *E-payments; e.g., credit-cards, e-brokers*

2000-03-09 **e-cash e-money EFT electronic payments**

NewsScan, Los Angeles Times
http://www.latimes.com/business/20000309/t000022823.html

EMoneyMail, a unit of the Bank One Corp. in Chicago, has developed a service that, for a fee of $1, will allow you to transfer to the account of another person (or a merchant) an amount up to $500, which can be withdrawn from designated credit cards, debit cards, or checking accounts and sent via e-mail. The recipient of the transfer links to the EmoneyMail.com Web site, and can then direct the money into the preferred destination account. Jupiter Communications analyst Robert Sterling says, "We are seeing the beginning of a new, credible form of digital cash transfer. This could change the way people interact with their banks and how they use their credit cards." (Los Angeles Times 9 Mar 2000)

Category 45.4 *E-payments; e.g., credit-cards, e-brokers*

2000-04-05 **e-cash digital money electronic funds transfer payment**

NewsScan

The U.S. Postal Service is teaming up with CheckFree to allow customers to pay their bills electronically. The move pits the Postal Service directly against financial institutions like Bank of America and Citibank, which offer electronic bill-paying services, as well as Internet portals, such as Yahoo. Although banks will pose stiff competition to the new USPS service, because customers like to view their account balances before making payments, the postal service is likely to be favored over portals. "The advantage for the post office is the trust and comfort it brings to the table," says a securities analyst. "The post office may get a lot more customers than a Yahoo, which is viewed as fun and frolicky, but perhaps not a place to pay bills." IDC last month predicted that the electronic bill market will grow to $1 billion by 2004. (News.com 5 Apr 2000_)

Category 45.4 *E-payments; e.g., credit-cards, e-brokers*

2000-04-06 **e-commerce electronic funds transfer EFT payment**

NewsScan, Los Angeles Times
http://www.latimes.com/business/cutting/20000406/t000032183.html

The U.S. Postal Service, in conjunction with two corporations that offer electronic bill-paying services, has developed a new system called USPSeBillPay, which customers can use to pay all of their bills online. More detailed information can be found at http://www.usps.gov. (AP/Los Angeles Times 6 Apr 2000)

Category 45.4 *E-payments; e.g., credit-cards, e-brokers*

2000-09-12 **credit card fraud countermeasure one-time account numbers**

RISKS 21 05

Joshua M. Bieber reported in RISKS in September, "American Express will launch a disposable credit-card service in the US next month, designed to answer the worldwide worry of online shopping. The system, Private Payments, enables cardholders to access a random one-use only credit-card number with an expiry date on the AmEx website, to be used in making one online purchase. In the event that the number is illegally accessed during a transaction, it cannot be re-used by a hacker. Visa and MasterCard are also looking at similar ideas."

Category 45.4 *E-payments; e.g., credit-cards, e-brokers*

2000-09-22 **online bill payment digital money e-cash banks financial e-commerce**

NewsScan, E-Commerce Times
http://www.ecommercetimes.com/news/articles2000/000922-1.shtml

The number of households that pay their bills online will balloon from 100,000 currently to 40.2 million by 2005, according a report by Jupiter Research. The reports suggests that banks "forgo selfish interests" and form alliances with online electronic bill payment and presentation services in order to maintain a role in the process. "...Financial institutions must stop watching this market and start driving it. Fast-moving technology companies that want to control the billing and payment process are poised to take over the financial aspects of that customer relationship," says a Jupiter analyst. A report released earlier this year by IDC predicted that by 2004, electronic bill payment services will generate more than $1 billion in revenue worldwide, compared with just $32 million last year. (E-Commerce Times 22 Sep 2000)

Category 45.4 *E-payments; e.g., credit-cards, e-brokers*

2000-09-28 **online bill payment digital money e-cash banks financial e-commerce**

NewsScan, E-Commerce Times
http://www.ecommercetimes.com/news/articles2000/000928-1.shtml

Credit cards will soon begin losing ground to smart cards and other digital payment methods, as consumers grow more comfortable with e-commerce, according to a study by ActivMedia Research. The report predicts that credit cards, which currently account for 98.5% of online transactions, will decline to a 90% market share by next year, as new technologies move into the mainstream. At the same time, transaction volumes for smart cards and e-wallets will grow from $500 million in 2000 to $5.7 billion in 2001, and balloon to $20 billion in 2002. "The ability to add an accentuated level of security is what people are striving for," says ActivMedia's VP for information services. Some credit card companies are already anticipating the shift — witness Visa's new "smart Visa" rollout — and analysts say "hybrid cards," which contain both an embedded chip and magnetic strip or bar code technology, are the next logical step. (E-Commercetimes.com 28 Sep 2000)

Category 45.4 *E-payments; e.g., credit-cards, e-brokers*

2000-10-12 **wireless e-commerce transactions security pact alliance consortium group cooperation**

NewsScan, TechWeb
http://www.techweb.com/wire/story/reuters/REU20001012S0006

Nokia, Motorola and Ericsson . . . [were] joined by Siemens in an alliance to develop secure mobile electronic transactions. The alliance, dubbed Mobile E-Business Technologies (MeT), will offer consumers a simple and safe way to conduct e-commerce transactions over their mobile phones. According to IDC, m-commerce, as it is called, will generate $37.7 billion by 2004, up from $51.2 million this year. (Reuters/TechWeb 12 Oct 2000)

Category 45.4 *E-payments; e.g., credit-cards, e-brokers*

2001-07-27 **electronic commerce e-commerce payment digital identity wallet payment privacy**

NewsScan

AOL CONSIDERS OFFERING 'IDENTITY SERVICE' [27 Jul 2001]
AOL Time Warner is said to be considering creation of "Magic Carpet," a so-called "identity service" to compete against Microsoft's Passport as an Internet gatekeeper that would allow consumers to store all their personal identifying data (including credit information) in one place. Passport now has more than 160 million accounts, and is being challenged in the courts by consumer and privacy groups concerned with how the service would work in conjunction with Microsoft XP, that company's new Internet-oriented operating system. Sun Microsystems chief executive Scott NcNealy welcomes AOL into the fray: "It's a nice alternative choice to Microsoft, and maybe having two companies go at each other will neutralize each other." (Washington Post 27 Jul 2001
http://washingtonpost.com/wp-dyn/articles/A56191-2001Jul26.html

---

Category 45.4 *E-payments; e.g., credit-cards, e-brokers*

2001-08-15 **e-commerce digital signature certificate electronic wallet cash privacy consumer complaints objections**

NewsScan

PRIVACY GROUPS STILL UNHAPPY WITH MICROSOFT
A coalition of consumer and privacy groups, including Junkbusters and the Electronic Privacy Information Center, is making a new assault on Microsoft, objecting to the Microsoft Passport service that will be included in the forthcoming Windows XP: "We charge Microsoft with specific unfair, deceptive and illegal behavior in collecting information [about Passport users], and their [Microsoft's] response is to make merchants use this pseudo-privacy technology. It's just insultingly nonresponsive." Microsoft denies the group's claims, and says that Passport will give people more convenience and control over what information they reveal about themselves. (USA Today 15 Aug 2001)
http://www.usatoday.com/life/cyber/tech/2001-08-15-xp-privacy-complaint.htm

---

Category 45.4 *E-payments; e.g., credit-cards, e-brokers*

2001-09-20 **e-commerce digital cash electronic wallet e-payments**

NewsScan

MICROSOFT PASSPORT SYSTEM OPENS UP TO RIVAL SITES
Microsoft, which has been criticized by privacy groups and others for using its Passport online identification technology to establish a dominant role in e-commerce, says it will make the system compatible with competing offerings by competing companies. A Microsoft executive said: "We do not want to be the one authentication scheme across the Internet. We see ourselves as one of many producers." (New York Times 20 Sep 2001)
http://www.nytimes.com/2001/09/20/technology/20SOFT.html

Category 45.4 *E-payments; e.g., credit-cards, e-brokers*

2002-02-20 **e-payments e-wallets disaster recovery plan failure incompetent fraud losses**

RISKS 21 92ff

Jeff Jonas reported in RISKS on some alarming statistics from Pay-Pal, the firm that lets subscribers exchange money by e-mail, that they had to reveal in their prospectus to comply with Securities and Exchange Commission (SEC) guidelines. Among other problems, the firm identified major damages that could occur from interruption of service, yet their disaster recovery plan seems to allow for outages of "at least several hours." In addition, the company reported serious losses due to fraud: of the "net losses of $264.7 million from our inception, March 8, 1999, through September 30, 2001, and net losses of $90.6 million during the nine months ended September 30, 2001, ... During the four months between July and October 2000, we experienced a significant fraud episode and, as a result, we incurred gross losses due to unauthorized charge-backs totaling $5.7 million. This amount represented 64.0% of total charge-backs due to unauthorized transactions for the year ended December 31, 2000. For the year ended December 31, 2000, the amount of losses with respect to unauthorized use of bank accounts totaled $0.3 million. The gross amount of charge-backs received through September 30, 2001 with respect to unauthorized use of credit cards for transactions that occurred during the nine months ended September 30, 2001 totaled $3.2 million. For the nine months ended September 30, 2001, the amount of our losses with respect to unauthorized use of bank accounts totaled $0.9 million."
According to the home page at < http://www.paypal.com >, the firm had 16 million members worldwide as of June 2002.

Category 45.4 *E-payments; e.g., credit-cards, e-brokers*

2002-02-28 **token identification authentication I&A e-commerce wireless interception man-in-the-middle attacks penetration confidentiality wristwatch**

NewsScan

WRISTWATCHES TO TELL TIME, ORDER HAMBURGERS, PAY FOR GAS
The Timex watch company has developed some wristwatches with Speedpass technology that uses a radio frequency transponder to communicate credit or debit card information allowing customers to pay instantly in places like Exxon and Mobil gas stations and McDonald's restaurants. The watch is currently being test-marketed in Illinois. (AP/USA Today 28 Feb 2002)
http://www.usatoday.com/life/cyber/tech/review/2002/2/28/timex-speedpass.htm

---

Category 45.4 *E-payments; e.g., credit-cards, e-brokers*

2002-03-05 **system design feedback quality assurance QA**

RISKS 21 93

Peter Trei contributed this item to RISKS:

>
A man used City Link more than 220 times without an e-tag, attracting at
least $22,000 in fines, because he did not know it had become a toll road,
the Melbourne Magistrates Court was told yesterday. [...]
http://theage.com.au/articles/2002/02/26/1014704951335.html

Some highways in Australia cannot be legally used without a radio tag. This poor soul hadn't updated his address with the DMV. The RISK lies in building systems which automatically rack up charges without limit, and no backup notification system. A big flashing sign saying 'E-Tag missing!' might have helped.
<

Category 45.4 *E-payments; e.g., credit-cards, e-brokers*

2002-06-27 **e-commerce single logon privacy confidentiality control Web e-payment e-wallet children**

NewsScan; http://partners.nytimes.com/2002/06/27/technology/27SOFT.html

MICROSOFT AGREES TO CHANGE "KIDS PASSPORT" SERVICE
Prodded by criticisms from a watchdog group called Children's Advertising Review Unit of the Better Business Bureau, Microsoft has agreed to make changes in the children's version of its Passport authorization service that allows computer users to sign on only once to use multiple Web sites and services. The group had complained that, despite the suggestion by Microsoft that the service was specially designed to protect children's safety and privacy online, there was nothing unique about the children's version of the software. Microsoft insists it never intended to mislead anyone, and has agree to post various statements clarifying what the software is and isn't. (New York Times 27 Jun 2002)

Category 45.4 *E-payments; e.g., credit-cards, e-brokers*

2002-07-11 **privacy certificates data sharing protection credentials e-payment e-wallet industry coalition group**

NewsScan; http://partners.nytimes.com/2002/06/03/technology/03SOFT.html

LIBERTY ALLIANCE SEEKS LIBERTY FROM WHOM?
The 43-member Liberty Alliance -- whose membership includes American Express, AOL Time Warner, General Motors, Nokia, Sony, and United Airlines -- is sometimes suspected of being simply an anti-Microsoft coalition, because it seemed to be formed as a way of resisting Microsoft's plans to use its ".Net Passport" technology to get a lock on Internet commerce. But the Alliance denies that motivation, and has clarified its objectives. The Liberty Alliance says its main goal is to develop open technical standards to allow Web sites and companies to share data when they have customer permission to do so. Different sets of credentials will be used for different purposes (the way, by analogy, an individual's wallet might contain a driver's license, credit cards, library cards, etc.). (New York Times 3 Jun 2002)

INDUSTRY GROUP TO UNVEIL NEW WEB ID STANDARDS The Liberty Alliance, which includes companies like Sun Microsystems, AOL Time Warner, Sony, American Express, MasterCard and Bank of America, is set to unveil new standards for identity authentication that could make memorizing long lists of Web site passwords a thing of the past. The standard makes it easy to surf between various secure sites -- from e-commerce sites to online banking, for instance -- without having to repeatedly type in password information. A competing standard from Microsoft, the Passport system, currently runs on about 200 Web sites. Microsoft and Liberty Alliance members have discussed the idea of joining forces, but no deal has been struck and some Alliance members have voiced their distrust of Microsoft's motives for wanting to cooperate. Several critics, including Sun and AOL, have suggested that the software giant has a history of "breaking" competing technology standards so they don't work as well as Microsoft's. (AP/Los Angeles Times 11 Jul 2002)

Category 45.4 *E-payments; e.g., credit-cards, e-brokers*

2004-10-15 **credit card fraud software application program server limits rules alerts**

NewsScan; http://theage.com.au/articles/2004/10/15/1097784019869.html

AUSTRALIAN FIRM IN PUSH TO CUT CARD FRAUD

A Queensland-based firm has begun a push to market a locally developed application, which it says can significantly reduce or eliminate credit card fraud. The Credit Card Scanning Protection System runs on the server of the financial institution. Each user is served a page where he or she can set personal parameters -- the type of credit card, level of alert and any additional data that needs to be input in order that a transaction can be completed. For example, apart from merely having a username and a password for gaining entry to one's account, a user can also set up his or her preferences so that a transaction does not go through unless the specified rules are met. Regular debits, and outlets to which regular payments are made can also be specified. And any time a transaction goes through, the customer can receive an alert, either by SMS or email, to a variety of devices.

Category 45.4 *E-payments; e.g., credit-cards, e-brokers*

2004-12-06 **electronic payments checks**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A41858-2004Dec6.html

ELECTRONIC PAYMENTS HAVE OVERTAKEN CHECKS

In 2003, Americans made 44.5 billion payments via electronic transactions, compared to only 36.7 billion payments by paper checks. The trend toward electronic purchases has been accelerated by strong growth in the popularity of debit cards, which can now be used to buy almost anything. Jean Ann Fox of the Consumer Federation of America says, "They're quick and easy. You don't stand there and hold up everybody in line behind you. Plus, folks are moving toward electronic banking and paying bills electronically." But she warns: "It's getting very confusing for consumers, and companies have not upgraded their protections." (Washington Post 6 Dec 2004)

Category 45.4 *E-payments; e.g., credit-cards, e-brokers*

2005-01-10 **credit cards cell phones security e-wallets**

NewsScan; http://www.nytimes.com/2005/01/10/technology/10cellphone.html

CELL PHONES COULD DOUBLE AS CREDIT CARDS

In Asia, cell phone handset makers are already marketing phones with embedded memory devices (a chip or magnetic strip) that can be swiped against credit or debit card readers in much the same way consumers now use plastic, and trials are underway to bring the technology to the U.S. Details are still being worked on important issues such as security -- consumers may be required to punch in an authorization code each time they charge something -- and in two trials users experienced difficulty in aiming their cell phones at the right angle for the card reader to pick up the data. "People got very upset. Pointing your cell phone at a target is very difficult," says Jorge Fernandes, CEO of cellphone software firm Vivotech. That issue will probably be resolved by switching from infrared to low-level radio signals, but the biggest obstacle is likely to be a dearth of card readers able to interact with the phones. "The phones are exciting, but it's going to be a long time" before a widespread base of U.S. merchants and consumers are equipped to use them, says Visa International VP Sue Gordon-Lathrop. (New York Times 10 Jan 2005)

45.5 Digital-rights management (DRM); e.g., copy protection, digital watermarks

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

1997-01-02 **pornography digital authentication**

PA News

A British firm, Highwater Signum, has developed a method for imprinting digital images with an invisible digital signature encoding the serial number of the camera used for taking the picture. A special reader can detect the signature in even small portions of the final image. Hopes are high that such technology, if widely integrated into digital cameras world wide, will interfere with the ability of pedophiles and other pornographers to market or otherwise distribute their pictures with impunity.

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

1998-02-19 **encryption pirating copying intellectual property digital rights management**

EDUPAGE, Los Angeles Times

Intel, Sony, Matsushita, Toshiba and Hitachi announced an encryption system which they claimed would prevent illegal copying of digital movies or music received over satellite services, cable networks, or the Internet.

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

1999-02-03 **e-commerce royalties intellectual property signature music SDMI Secure Digital Music Initiative watermark**

Wired via PointCast

GoodNoise, a Web-based retailer of music, announced in February that it would henceforth brand all songs or albums downloaded from its site with a digital signature. In addition, the firm guaranteed that it would pay $0.07 per song for each download of a track through an agency to the copyright holder. The digital signature was not intended to prevent illegal copying but rather to provide a mechanism for honest purchasers to ascertain that they were acquiring a legally-copied and -distributed file.

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

1999-02-17 **digital watermark copyright copy protection**

New York Times

Hitachi, IBM, NEC, Pioneer and Sony (the "Galaxy Group") announced their agreement on a new digital watermark standard that would embed a cryptographic code in every frame of a digital multimedia work. New digital equipment would not allow copies of such works.

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

1999-06-04 **intellectual property watermark DVD audio copyright piracy**

EDUPAGE; TechWeb

DIGITAL WATERMARKING SHOWDOWN
The 4Cs, an industry group comprising IBM, Intel, Matsushita Electric, and Toshiba is expected to choose a digital watermarking technology for DVD-Audio at its June 11 [1999] meeting. The group will most likely pick between products developed by Aris Technologies and Blue Spike. Both companies have essential patents, and offer solid digital watermarking technologies. Analysts expect that the option chosen for DVD-audio will be indicative of the standard the Secure Digital Music Initiative adopts as copy protection in years to come. Record labels view watermarking as an essential part of copy protection for both Internet and DVD audio. Digital watermarking allows manufacturers to determine who breaks a given encryption system. (TechWeb 06/04/99)

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2000-03-20 **digital watermark software tools e-commerce authentication**

Network World Fusion http://www.nwfusion.com/newsletters/sec/0103sec1.html

Jim Reavis of SecurityPortal wrote a good overview of developments in digital watermarking for the Network World Security Newsletter in January 2000. He summarized the basic requirements for this image- and music-authentication technology: invisibility, accessibility, and resistance to modification. He also reviewed tools for creating and validating digital watermarks as well as developing services such as watermark-tracking, where a firm scans the Web looking for copyrighted works and reports on where they have been found.

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2000-09-13 **criminal hackers contest vulnerability ethics watermark intellectual property IP music video movies encryption cracking vulnerabilities**

NewsScan, Financial Times http://news.ftcom/news/industries/media, CNet http://news.cnet.com/news/0-1005-200-3583337.html http://news.ft.com/news/industries/media

The Secure Digital Music Initiative, a forum of 175 companies in the music, electronics, information technology and telecommunications industries dedicated to developing a secure framework for the digital distribution of music, . . . [offered] a reward of up to $10,000 to the first person to crack its codes. In an open letter to the "alternative" press, SDMI executive director Leonardo Chiariglione challenged hackers to "show off your skills, make some money, and help shape the future of the online digital music economy." SDMI has about 10 different proposals for "watermarking" technology that could be embedded in a digital music file. Portable music players complying with the SDMI standard would only work if the watermark — an inaudible signal — is present. SDMI has also issued the challenge to the technology departments at the University of California at San Diego, MIT, Virginia Tech and Stanford University. "The proposed technologies must pass several stringent tests: they must be inaudible, robust and run efficiently on various platforms, including PCs... So here's the invitation: Attack the proposed technologies. Crack them. By successfully breaking the SDMI protected content, you will play a role in determining what technology SDMI will adopt," said Chiariglione. (Financial Times 13 Sep 2000)

In November, [t]he Secure Digital Music Initiative (SDMI) . . . [said] that three out of five music-protection schemes tested withstood hacker attacks. . . . In announcing the results, SDMI executive director Leonardo Chiariglione refuted an earlier report by Salon.com that said all five technologies had been broken. "I'm an engineer, which means I deal with facts. We conducted all the tests that were planned and did not change the rules as we progressed. We came to the conclusion that not all the (technologies) had been hacked." The group is giving no details on which technologies prevailed, other than to say that both watermark and non-watermark proposals had passed the test. (CNet News.com 8 Nov 2000) http://news.cnet.com/news/0-1005-200-3583337.html

---

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2000-10-24 **criminal hackers scientists contest vulnerability ethics watermark intellectual property IP music video movies encryption cracking vulnerabilities**

NewsScan, Associated Press/MSNBC http://www.msnbc.com/news/480521.asp

A team of computer scientists at Princeton and Rice Universities and the Xerox Palo Alto Research Center (PARC) has been able to remove the invisible "watermarks" used by the 200-company Secure Digital Media Initiative (SDMI) to protect digital music files from pirates. SDMI had offered a prize to anyone who could defeat its various security measures, four out six of which make use of watermarks. SDMI's Tala Shamoon said, "I expected some would have fallen. This is part of an empirical process to get the best technology."

Professor Ed Felten and colleagues at Princeton University defeated all four of the schemes under test.

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2000-11-21 **intellectual property watermark copyright violations**

NewsScan, ZDNet http://msnbc.com/news/493231.asp

Music subscription site EMusic.com has started using "acoustic fingerprint" technology, which it says can spot any of its 140,000 songs that are being illegally traded by Napster users. If such song-swapping is detected, EMusic will send an e-mail warning, asking that the swapping cease. Napster has apparently agreed to block the perpetrator's account if illegal trading persists, and if the user finds a way back into Napster through a different IP address, EMusic says it will try to block that person' Internet access. An analyst with Webnoize says, "This is a warning shot. They are saying they have the technical ability to track their music." He adds that the situation could lead to a lawsuit that would pit the two pioneers — Napster and EMusic — against each other. (ZDNet 21 Nov 2000)

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2001-01-23 **intellectual property protection watermark audit trail privacy contract law**

NewsScan

IBM UNVEILS NEW COPYRIGHT TECHNOLOGY
IBM has added new features to its Electronic Media Management System, which is used by copyright holders to control under what circumstances their music is distributed. "We announced two fundamental enhancements," says IBM VP Steve Canepa. "One is superdistribution, which allows for peer-to-peer file distribution. Once the file gets to the consumer, whether it's on a PC or a PDA or whatever, it can now be passed along. A track has a set of usage criteria that can follow it wherever it goes." Translated, that means that fans who buy a music track encoded with EMMS can pass it along to a friend, but the friend may then have to buy the track. The second enhancement provides more choices for rules set by the content owner. For instance, downloadable tracks could expire on the album's release date in one country, but never expire in another country. Music files can also be tracked so that the content owner knows where each copy is, who acquired it and how, and whether it was passed along to others. (Hollywood Reporter 23 Jan 2001)
http://www.hollywoodreporter.com/convergence/index.asp?ee

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2001-07-17 **copyright content protection video movies standard 5C DTLA Digital Transmission Licensing Administrator**

NewsScan

SONY & WARNER AGREE ON CONTENT-PROTECTION STANDARD [17 Jul 2001]
Sony Pictures and Warner Bros. Studio have agreed to accept the content-protection standard developed by the so-called "5C Group" of manufacturers (Intel, Matsushita, Toshiba, Sony, and Hitachi) who are joined in an alliance called the Digital Transmission Licensing Administrator. The standard specifies a technology for protecting digitized movies and as they are exchanged among set-top boxes, computers, and televisions when the exchange is made over cables. Disney and Vivendi, which have not signed on to this standard, are holding out for the development of a way to protect transmissions even when they are broadcast over the air and received via antennas. (Wall Street Journal 17 Jul 2001)
http://wsj.com (sub. req'd)

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2001-11-08 **digital watermark legal dispute DVD copy protection patent**

NewsScan

DIGITAL WATERMARKING DISPUTE DELAYS DVD STANDARD [8 Nov 2001]
The adoption of a technical standard for DVD copy-protection will suffer delays as Verance and Digimarc, two of the lead digital watermarking companies, head to court over their long-standing intellectual property dispute. Digital watermarking places a unique bit of code into a sound or image file that makes it difficult to play without permission from copyright holders. Verance has now filed a lawsuit charging Digimarc with violating antitrust and unfair competition laws, alleging that Digimarc illegally submitted Verance's digital watermarking technology to a standards group. The suit "is going to delay an adoption of a standard for DVD copy-protection," says a Raymond James Financial analyst. "The longer they hash it out in the Portland courts, the longer it's going to take for the industry to (accept a) solution and get some compliant software out there." Digimarc is a member of the Video Watermarking group, a coalition of consumer electronics companies that includes Hitachi, Macrovision, NEC, Philips Electronics, Pioneer and Sony. The group hopes to set a digital watermarking standard that will allow film studios to distribute content online securely. (CNet News.com 8 Nov 2001)
http://news.cnet.com/news/0-1005-200-7820458.html?tag=lh

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2002-07-17 **digital TV television recording piracy intellectual property**

NewsScan

CONGRESS TO TACKLE DIGITAL TV IN THE FALL
Rep. Billy Tauzin (R-La.), head of the House Energy and Commerce Committee, says he's drafting legislation that he hopes will resolve many of the questions surrounding digital TV. Congress has set a 2006 deadline for television broadcasters to complete switching over to digital signals, but some have dragged their feet, fearing that they could suffer the Internet-based piracy that's plagued the music industry for several years. Meanwhile electronics makers have worried that they could be forced to produce DVD players and other devices laden with so many restrictions that consumers will shun them. The two sides have been working to develop a "broadcast flag" that would allow consumers to record shows for personal use but prevent them from sharing those recordings over the Internet. "It will come down to, 'What are the rules?'" says Gary Shapiro, president of the Consumer Electronics Association. Meanwhile, there are several details still to be hammered out, such as whether consumers should be able to transfer broadcast recordings to vacation home or office computers, or whether new restrictions will disable existing DVDs and other devices. (Reuters/CNN.com 16 Jul 2002)

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2002-07-19 **intellectual property broadcasting recording Internet radio**

NewsScan

RECORD LABELS SEEK TO BLOCK WEBCASTING PIRACY
The Recording Industry Association of America is asking computer and electronics manufacturers to develop an "audio performance flag" similar to the "broadcast flag" technology now under development to protect digital television programs. The flag would act as a marker that would prohibit content that had been digitally recorded from an Internet radio station from being redistributed over the Internet. Internet radio is not a significant source of piracy today, in part because of its lower quality compared to CDs, but the combination of increased broadband connections and lower broadcasting costs is expected to push webcasters toward higher-fidelity feeds. RIAA senior VP Mitch Glazier called the talks "very limited, preliminary discussions." (Los Angeles Times 18 Jul 2002)

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2002-09-06 **Anti-Counterfeiting Amendments CDs DVDs software digital rights**

NewsScan

SENATOR CRITICIZES COPYRIGHT BILL
Sen. George Allen (R-Va.) is pulling his support for the proposed Anticounterfeiting Amendments of 2002 because of last-minute changes made to the legislation before it came to a committee vote. The bill originally targeted large-scale operations that counterfeit "physical features" such fake Windows holograms or the special packaging used to certify software, CDs or DVDs as authentic. But the revised version covers "any feature" used to guarantee authenticity, including technology used in digital rights management. "Opening this legislation to the digital realm has caused the virtually unanimous industry support behind it to evaporate, and it has raised a host of troubling liability issues that cause substantial harm to Internet service providers," says Allen, who chairs the Senate Republican High Tech Task Force. Companies now opposing the bill include Verizon, Microsoft, Apple, eBay and Yahoo, all of whom have voiced their concern over a section that prohibits "trafficking" in or redistributing files that contain compromised digital watermarks. They fear the new language opens up ISPs to prosecution if their subscribers send such files. The revised version has "divided the community, so to speak, the industry, and went far afield from the original intent of the bill," says an Allen spokesman. The bill is set for a full Senate vote, which could come at anytime. (CNet News.com 5 Sep 2002)
http://news.com.com/2100-1023-956811.html?tag=fd_top

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2002-10-01 **digital rights management watermark**

NewsScan

LIQUID AUDIO PATENTS BOLSTER MICROSOFT MEDIA SECURITY
Microsoft has acquired patents from Liquid Audio covering at least two technologies that are aimed at security features for distributing entertainment online. One protects identifying information hidden in a watermark within a digital file, and the other enables online distributors to limit the countries or territories where their files may be delivered. These two restrictions are critical to the music and movie industries' business models, and will boost Microsoft's ability to respond to industry demands for secure online distribution. "The rights that we've acquired today we view as being important to efforts down the road with regard to DRM (digital rights management) technologies," says a Microsoft spokesman. (Los Angeles Times 1 Oct 2002)
http://makeashorterlink.com/?C57F217F1

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2002-11-01 **intellectual property copyright piracy copy protection prevention mechanisms**

NewsScan

MUSIC INDUSTRY: GONNA LOCK LOCK LOCK, 'TIL BROAD DAYLIGHT
Two new digital audio disk formats, Super Audio CD or DVD-Audio, are engineered to be copy-proof, using digital watermarks encoded to lock the recordings on the disks. So far, music lovers have been slow to accept copy-protected disks as just a new fact of life, but Electronic Frontier Foundation intellectual property attorney Fred von Lohmann acknowledges that "copyright owners are entitled to use whatever formats they want to use." (He also notes slyly that "if they really want to protect their content they can go back to vinyl.") The major consumer objection is the failure to label the recordings properly, so that it's clear what's being sold. GartnerG2 industry analyst P.J. McNealy says, "I don't think anybody per se is against copy-protected CDs. I think they're against no-labeled copy-protected CDs. The labels are optional at this point." (AP/San Jose Mercury News 31 Oct 2002)

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2002-11-13 **digital rights management lawsuit**

NewsScan

SONY, PHILIPS HEAD GROUP TO ACQUIRE INTERTRUST
Fidelio Acquisition Co., a group that includes Sony, Philips and other investors, is acquiring InterTrust Technologies, a firm specializing in digital rights management (DRM) technology. DRM software allows copyright holders to specify and enforce rules on the usage of digital text, music, movies or other content. The $453-million deal will "significantly accelerate the ability to ensure secure delivery of digital content and enable the development of many exciting new services for consumers and businesses," says Sony chairman and CEO Nobuyuki Idei. InterTrust is currently locked in a legal battle with Microsoft in which it alleges the software giant violated its patents and company officials have discussed damage figures in the billions of dollars. (Wall Street Journal 13 Nov 2002)

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2002-12-07 **intellectual property music distribution e-commerce digital rights management piracy**

NewsScan

GATEWAY LEADS TO DIGITAL MUSIC
Gateway and Pressplay, the online music subscription service backed by Vivendi Universal and Sony, are teaming up to offer PC buyers a new line of computers already bundled with 2,000 preloaded hit songs. Buyers will receive one to three months of Pressplay's service for free, but will have to pay at least $9.95 a month thereafter to maintain access to the songs. The goal is to make it easy for consumers to sample and buy music without going to the trouble of downloading it from the Internet for free. The preloaded music will be constrained by the digital rights management software that Pressplay uses to deter piracy, however, and users will have to spend an extra $1 per song if they want to move the file to a portable device or copy it onto a CD. "I can't say it's the be-all, end-all distribution model that's going to make people flock to buy access to 2,000 songs," says Gartner analyst P.J. McNealy. "This is interesting, but the portability piece is more important." (Los Angeles Times 6 Dec 2002)
http://shorl.com/dyprenivihoku

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2002-12-23 **broadcast flag copyright intellectual property copy protection**

NewsScan

CONTENT LOCKS ON DIGITAL BROADCASTS
An ongoing policy debate has been swirling around a "broadcast flag" being promoted by the TV industry to protect copyrighted content. The flag would consist of a few bits of information accompanying a digital transmission to signify whether and under what rules the transmitted content (e.g., a movie) may be viewed and copied. Supporters of the flag insist that it will be used merely to restrict redistribution of copyrighted material to large numbers of other people, in violation of existing laws; the idea, they say, is that the flag will "keep people honest." In rebuttal, critics like Cory Doctorow of the Electronic Frontier Foundation charge: "When they say 'This keeps honest people honest,' they mean 'This keeps honest people in chains.'... It addresses a nonexistent problem with an insufficient technical measure at great expense to liberty and innovation." (AP/San Jose Mercury News 22 Dec 2002)

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2003-01-09 **digital rights management copyright copy protection piracy**

NewsScan

REALNETWORKS INCORPORATES DRM TECHNOLOGY
RealNetworks will include its Helix DRM (digital rights management) software in its digital media streaming technology, enabling movie studios and music labels to protect their digital content from copyright violation. Helix DRM is designed to support various digital content standards, including RealAudio, RealVideo, MPEG-4 and MP3. "This breaks the stranglehold that tied a content owner to using a given format if they wanted to use DRM," says Dan Sheehan, VP of media systems at RealNetworks. The move was welcomed by the film and music industries, according to a company statement: "Sony Pictures Digital Entertainment, Starz on Demand and Triggerstreet.com as well as by music label EMI Recorded Music (which includes the EMI, Capitol, Virgin and other record labels) and several Internet media services [will use Helix DRM]." (Reuters 9 Jan 2003)

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2003-02-20 **copyright intellectual property copy protection**

NewsScan

COPY PROTECTION EFFORTS MISGUIDED, SAYS LESSIG
Lawmakers will be making a big mistake if they bow to Hollywood pressure and enact new copyright-protection legislation based on today's Internet use patterns, says Stanford University professor Lawrence Lessig. Currently, millions of consumers are downloading music to their PCs because slow dialup connections make it impractical to stream content quickly to a variety of devices. "In the future, it will be easier to pay for subscription services than to be an amateur database administrator who moves content from device to device. We're legislating against a background of the Internet's current architecture of content distribution, and this is a fundamental mistake," Lessig told participants at the Digital Rights Management Summit held at Intel headquarters. (AP 20 Feb 2003)
http://apnews.excite.com/article/20030220/D7PA785G0.htm

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2003-03-21 **digital watermark copyright music rights management**

NewsScan

SUPER DIGITAL WATERMARK IN THE WORKS
SunnComm Technologies is working with Stealth MediaLabs to develop a kind of super-watermark that could be embedded inside digital music files and would be robust enough to withstand digital compression, or being recorded off the radio or rerecorded through an analog connection. The technology, originally developed at the University of Miami, could also be used to embed other information. "The intention was for protecting the security of intellectual property. Adding pictures and liner notes inside a song is kind of a byproduct," says SunnComm COO Bill Whitmore. The technology works by encoding binary data inside the stereo audio signal itself, taking advantage of acoustical properties and human hearing characteristics to make it imperceptible to the listener. Because the signal is embedded in the sound itself, the data is hard to remove without significantly changing the sound of the song. SunnComm plans initially to market the super-watermark technology to record labels, which could use it to detect which recipients of advance discs are putting songs online before the albums' official release dates. "With that anonymity gone, people will be less willing to put advance songs on file-sharing networks," says Whitmore. (CNet News.com 20 Mar 2003)
http://news.com.com/2100-1027-993588.html

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2003-04-23 **music piracy DRM digital rights management CD ripping protection**

NewsScan

PROTECTION AGAINST CD 'RIPPING'
Macrovision, a company known for helping Hollywood moviemakers prevent their videocassettes and DVDs from being copied, is joining with Microsoft in a project that will allow music companies to make CDs that consumers can copy for themselves but not "rip" them for sharing with others. Because standard CDs are fairly easy to copy, the music industry has seen increasingly declining sales (down 2.5% in 2001 and 8.7% in 2002), and industry analyst Richard Doherty of the Envisioneering Group says fear that such declines will continue has made some music labels "willing to risk consumer playback problems and increased customer wrath." In Europe copy-protected disks have met with strong consumer resistance because some CDs don't play in all playback devices and some get stuck in computers. (USA Today 23 Apr 2003)

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2003-09-18 **piracy music smart cds antipiracy new generation BMG file-sharing copies**

NewsScan

BMG INTRODUCES 'SMART' CDs
BMG Entertainment is launching a new generation of "smart" CDs aimed at thwarting file-sharing while at the same time allowing CD buyers to make a few copies for themselves and friends. The technology will make its debut next week with the release of "Comin' From Where I'm From" by Anthony Hamilton. Buyers of that CD will be able to burn three copies per computer and will be able to e-mail songs to a limited number of people, each of whom can then listen to the song 10 times before it becomes unavailable. The MediaMax CD-3 antipiracy technology is made by SunnComm Technologies in Phoenix. SunnComm rival Macrovision has also developed protective technology that allows limited copying, and the record labels are watching closely to gauge fans' reactions. Meanwhile, civil liberties advocates say the technology is good in principle, but is still too restrictive. "It is inconsistent with how fair use has always been applied," says Cindy Cohn, legal director for the Electronic Frontier Foundation. (AP/Wall Street Journal 18 Sep 2003)

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2003-10-03 **digital rights management DRM protect digitial**

NewsScan

DIGITAL RIGHTS MANAGEMENT
In Amsterdam, a film technology group called MPEG LA says it wants to collect all essential patents that can protect digitized music and movies in order to create new content-distribution models over the Internet. The problem is that at present it is often not known which companies own all the relevant patents, and the uncertainty is discouraging film and music publishers from selling their products in new digital ways. MPEG LA hopes that by early in 2004 it will have collected all essential digital rights management (DRM) patents, so that it can begin licensing them later that year. (Reuters/USA Today 3 Oct 2003)

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2003-10-10 **software protection intellectual property copyright sales boost Fade**

NewsScan

SOFTWARE PROTECTION SCHEME ENDS UP BOOSTING NEW GAME SALES
Companies are using a new software protection system, called Fade, to protect their intellectual property from software thieves. Fade is being introduced by Macrovision, which specializes in digital rights management, and the British games developer Codemasters. What the program does is make unauthorized copies of games slowly degrade, by exploiting the systems for error correction that computers use to cope with CD-ROMs or DVDs that have become scratched. Software protected by Fade contains fragments of "subversive" code designed to seem like scratches, which are then arranged on the disc in a pattern that will be used to prevent copying. Bruce Everiss of Codemasters says, "The beauty of this is that the degrading copy becomes a sales promotion tool. People go out and buy an original version." (New Scientist 10 Oct 2003)

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2004-01-05 **consortium technology companies anti piracy illegal file sharing intellectual property rights protection**

NewsScan

NEW PLAN TO PROTECT AGAINST ILLEGAL FILE SHARING

A consortium of five major information technology companies is planning a new system to protect digital music, video and software from illegal file sharing., The members of the new consortium (dalled Project Hudson0 are Intel, Nokia, Samsung, Toshiba and Matshushita, and the consortium's approach will compete against various other copy protection systems being advanced by Microsoft, Sony and Royal Philips Electronics, Apple, RealNetworks, and others. Leonardo Chiariglione, who founded the group that developed the original MP3 digital audio compression standard, says: "Content should be as transparent as it is today with MP3. It should be movable anywhere and still be protected. If we stay with digital islands people have a legitimate excuse to piracy." (New York Times 5 Jan 2004)

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2004-01-06 **copy protection Europe consumer group lawsuit**

NewsScan

EUROPEAN CONSUMER GROUP SUES OVER LOCKED CDs

Test-Achats, a consumer rights group based in Belgium, says it's received some 200 complaints from music fans angry over copy-protected CDs whose technology prevents them from playing on some CD players. The group has filed suit against major record labels, asking EMI, Universal, Sony and BMG to stop releasing the locked CDs and to reimburse disgruntled buyers. Industry observers say the legal action is the biggest challenge yet to the music industry's efforts to thwart piracy through copy-protection technology. But a statement by the International Federation of the Phonographic Industry says the lawsuit was baseless: "European law is clear that record companies and other copyright holders have the right to protect their works through technical means." The lawsuit is expected to be heard in a Belgium court this week. (BBC News 6 Jan 2003)

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2004-03-03 **filtering technology stop music file sharing peer-to-peer P2P intellectual property rights copyright**

NewsScan

FILTERING TECHNOLOGY COULD PUT AN END TO ILLEGAL FILE-SWAPPING

Audible Magic has been making the rounds on Capitol Hill, touting the capabilities of its technology, which it says can block the swapping of copyrighted music. It works by identifying the "psycho-acoustical" properties of a piece of music — essentially the computer equivalent of listening to the song itself — which enables it to recognize all versions of a song, despite variations in recording qualities or other subtle differences. The company has attracted the attention of the Recording Industry Association of America, which is backing Audible's technology as one possible solution to illegal downloading. In past months, peer-to-peer executives have repeatedly told Congress that is technologically impossible or infeasible to install such filtering systems on their networks, but with the advent of Audible, some are backpedaling on those statements, saying that even if it works, mandating the use of such technology would be a mistake. Requiring filters "would amount to the anointment of a specific technology as the winner in what the (recording) industry has made a file-sharing war," says Adam Eisgrau, executive director of P2P United, a file-swapping trade association. Eisgrau says his group has asked for a demonstration of the Audible Magic technology, and RIAA chief executive Mitch Bainwol says he's happy to oblige: "The peer-to-peer community has said they are serious about filtering. But they've said they can't filter. We're saying, well, the good news is that you can." (CNet News.com 3 Mar 2004)

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2004-03-08 **P2P peer-to-peer filtering testing copyright infringement block**

http://www.nytimes.com/2004/03/08/technology/08music.html?th=&pagewanted=print&position=

The RIAA publicized a new technology from AudibleMagic to identify copyrighted materials during transfer and block it. John Schwartz of the New York Times wrote, "Audible Magic executives say that their software can be used in devices that attach to computer networks, or it can be written into the file-sharing software from companies like Kazaa and Grokster. . . . File-sharing companies have argued that they cannot control copyright infringement on their networks. . . . Record industry executives, who have said that they are against government-ordered technology fixes for copyright problems, said that they are not asking Congress to act, at least at this time. Instead, Mr. Bainwol said, his industry would like to see the 'peer-to-peer' companies add the software to their wares." Two universities had already signed up to examine the new technology at the beginning of March 2004.

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2004-05-08 **peer-to-peer P2P file sharing music piracy flooding denial of service**

http://www.wired.com/news/print/0,1294,63384,00.html

A computer science professor and graduate student at the University of Tulsa have been awarded a patent for a method of thwarting illegal file sharing on peer-to-peer networks by flooding the network with bogus files that look like pirated music. The software creates bogus files with attributes—such as file names and description tags—that make them look like the real thing, but they are in fact white noise, low-quality recordings or advertisements to buy the song. What's more, the software sends out thousands of decoys to frustrate P2P users with fruitless downloads.

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2004-07-29 **Apple Real hacker corporate information warfare copyright infringement digital rights management DRM violation**

NewsScan

APPLE ACCUSES REALNETWORKS OF USING HACKER TACTICS

Apple has accused RealNetworks, a provider of digital-media services, of offering software that lets online music buyers play on a variety of devices songs intended for use only on Apple's iPod devices. Apple says that it's "stunned that RealNetworks has adopted the tactics and ethics of a
hacker to break into the iPod." The RealNetworks software in question is called Harmony, which Real describes as "the world's first digital-rights-management translation system that music buyers can use to transfer music from one secure music device to another. It supports devices made by Creative, iRiver, palmOne, RCA, Rio, Samsung, and others. Legal experts seem to think that unless Apple can prove that RealNetworks reverse-engineered Apple's iPod software, a case under the Digital Millennium Copyright Act (DMCA) would be very hard to win. But Mark Rasch, former head of the U.S. Department of Justice's computer crimes unit (and now senior VP of security services firm Solutionary Inc.) says: "The problem with the DMCA is that it gives more protection than copyright law and it allows companies to skew the market with a form of protectionism. It allows technological protectionism to be legally adopted, and it works to prevent people from coming to market with cheaper compatible products." (InformationWeek 29 Jul 2004) Rec'd fr. John Lamp

---

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2004-08-16 **digital rights management DRM meaning copyright ownership intellectual property rights bootleg online Internet**

NewsScan

THE NEW MEANING OF OWNERSHIP IN THE DIGITAL AGE

When you buy a CD from a store, you "own" that music, and as long as you don't bootleg it or charge lots of people money to listen to it, it's yours. But if you purchase that same playlist online, in most cases you're purchasing the "rights" to the content which is "locked" by some type of
digital rights management software. Not only that, but those rights may change over time, dictated by the whims of the music company you get them from. For instance, Apple Computer recently upped the number of computers on which its iTunes music files can be concurrently installed from three to five, but there's nothing stopping it from making its DRM more restrictive in the future -- although the company says that's unlikely. Meanwhile, customers of RealNetwork's Rhapsody music service "rent" their songs for a monthly fee but can play them only on their PCs, not their MP3 players. All these variables mean that consumers will need to be better informed in the
future about what it is they're actually getting for their money, says Alan Davidson, associate director of the Center for Democracy and Technology: "DRM underscores the point that consumers are going to have to become a lot more sophisticated about what they're buying." (Wall Street Journal 16 Aug 2004)

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2004-08-24 **digital rights management DRM Microsoft Time Warner EU**

NewsScan

MICROSOFT/TIME WARNER DRM PLANS QUESTIONED IN EUROPE

The European Commission is examining a proposed agreement by Microsoft and Time Warner to acquire joint control of the U.S. firm ContentGuard, a company that develops digital rights management (DRM) technology. The purpose of DRM software is to protect digital files (including movies and music files) from illegal copying and use. (Reuters/USA Today 24 Aug 2004)

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2004-12-03 **watermarks movies iTrace piracy video compression authentication**

NewsScan; http://www.usatoday.com/tech/news/techinnovations/2004-12-03-piracy-watermarks_x.htm

WATERMARK TECHNOLOGY SEEKS TO STAMP OUT FILM THIEVERY

Scientists at Sarnoff Labs have developed a "watermarking" technology called iTrace aimed at reducing video piracy perpetrated by moviegoers who secretly tape new films with handheld video cameras in the movie theater. Sarnoff's Jeffrey Lubin used his background in perceptual psychology to devise a watermark that not only would be invisible to the movie viewer, but would also survive several generations of crude copying. "The Holy Grail example is someone takes a camcorder into a movie theater and pirates a movie, and then compresses it on a digital file and puts it on the Internet," says Lubin. The iTrace watermark emerges gradually, over a 5-second interval, to exploit the tendency of human vision to compensate and ignore images that change slowly, he says. The watermark is actually a sequence of shifting blobs that get either lighter or darker and endure throughout the film. Each copy has its own unique watermark that enables studios to track the origin of a pirated copy. "The applications for watermarking are not just for the final result, but it also gives us freedom to move images around during production so that if they get into the wrong hands, they can be traced back to the last rightful owner," says Larry Birstock, executive VP of postproduction firm Post Logic Studios. (AP/USA Today 3 Dec 2004)

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2005-01-19 **anti-piracy DRM digital rights management consumer electronics hardware standards software Coral Consortium Marlin**

NewsScan; http://online.wsj.com/article/0

CONSUMER ELECTRONICS GIANTS UNITE AGAINST PIRACY

Some of the biggest names in consumer electronics, including Sony, Samsung Electronics, Philips Electronics and Matsushita Electric Industrial, have teamed up with Intertrust Technologies to form the Marlin Joint Development Association, which will coordinate their efforts to develop standard specifications for antipiracy software. The motivation behind the united effort is to impose some kind of uniformity on the consumer electronics industry, thereby avoiding the confusing array of digital rights management software options currently being used by computer hardware and software makers. "The CE industry has been pretty quiet," says Intertrust CEO Talal Shamoon. Now, they're "detonating their DRM." Intertrust was jointly purchased in 2003 by Sony, Philips and other investors. The Marlin effort comes on the heels of an earlier venture called the Coral Consortium, which was designed to ensure that different DRM programs were interoperable. (Wall Street Journal 19 Jan 2005)

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2006-02-03 **British UK library worry electronic content access digital rights management DRM copyright intellectual property right issues**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4675280.stm 23

BRITISH LIBRARY WORRIES ABOUT ACCESS TO ELECTRONIC CONTENT

In comments submitted to the All Party Parliamentary Internet Group, which is investigating digital rights management (DRM) technologies, the British Library has expressed strong concerns about the long-term viability of electronic resources. Content producers increasingly use DRM to limit unauthorized access to electronic materials, but officials from the library said the protections also threaten legitimate uses of content. Use of materials held by libraries constitutes an important exception to copyright laws, according to Clive Field, the British Library's director of scholarships and collections, but DRM tools inadvertently upset the balance between appropriate exceptions and the rights of content owners. Moreover, long-term access is at risk. Even when copyright expires for a work, the DRM tools applied to its electronic version will still be in place. If the owner cannot be contacted, there might be no way to unlock materials that are no longer covered by copyright. "This will fundamentally threaten the longstanding and accepted concepts of fair dealing and library privilege," according to the British Library's statement, "and undermine...legitimate public good access."

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2006-02-09 **Fraunhofer Institute German research MP3 anti-piracy tool development**

EDUPAGE; http://www.pcworld.com/news/article/0,aid,124676,00.asp 23

CREATORS OF MP3 DEVELOP TOOL TO COMBAT PIRACY

A German research group that developed the MP3 format in the late 1980s has developed a watermarking technology that it says will help curb illegal file sharing. Officials from the Fraunhofer Institute said that their technology is better than digital rights management (DRM) tools in that it does not require special hardware to play protected files and is less susceptible to hacking. Instead, the institute has developed a method of watermarking MP3 files and software to track those files. The result is that rather than identifying individuals who download protected files, the application tracks who has uploaded files that have been marked. According to Michael Kip, a spokesperson for the institute, "If, for instance, you purchase and download a CD, burn a copy, and give it to a friend, and that person puts it on a file sharing network, our system will trace that music back to you." That scenario, said Kip, could result in legal action against the person who originally bought the CD, depending on that person's country of residence and applicable copyright laws.

Category 45.5 *Digital-rights management (DRM); e.g., copy protection, digital watermarks*

2006-03-13 **University of Maryland digital right management DRM software anti-piracy tool collaborator identification**

EDUPAGE; http://www.pcworld.idg.com.au/index.php/id;92233453;fp;2;fpid;1 23

MARYLAND RESEARCHERS UNVEIL DRM TECHNOLOGY

Researchers at the University of Maryland's A. James Clark School of Engineering have developed digital rights management (DRM) technology that they say is highly resistant to the dilution that afflicts other DRM tools when many users collude on piracy. With most DRM technology, if 100 users work together to create a pirated copy of a movie, for example, the digital "fingerprint" is diluted 100 times, making it very difficult to identify those responsible. According to Assistant Professor Min Wu at the Clark School, with the new technology, if a group of users collude to copy a protected file, the researchers can identify all of those who participated. The new DRM technology can be used to protect movies, songs, images, and other documents. Sony BMG, which was recently involved in a brouhaha over attempts to add its own DRM protection, has expressed interest in the technology, as has the U.S. Department of Defense.

45.6 Smart cards and other e-commerce security measures

Category 45.6 *Smart cards and other e-commerce security measures*

1997-01-30 **electronic commerce**

EDUPAGE

DELOITTE, MERCHANT GROUP TO DELIVER SECURE E-MAIL DOCUMENTS
Accounting firm Deloitte & Touche is teaming up with private merchant group Thurston Group to provide an electronic service called NetDox Inc., which will offer banks, insurance companies, law firms and others a means of transferring legal documents via a secure electronic system. NetDox will track the documents through delivery, will return a receipt to the sender, and will retain an electronic "thumbprint" of the document in case any questions regarding its authenticity or delivery time arise. The service should be operational by summer. (Wall Street Journal 30 Jan 97)

Category 45.6 *Smart cards and other e-commerce security measures*

1997-02-12 **e-commerce smart card**

Reuters

Fischer International Systems Corp. introduced a $60 device that fits into a normal floppy drive to allow PCs to interact with smart cards. The company foresees major applications in electronic commerce, where the smart cards can serve as authentication devices and also as electronic wallets for electronic cash.

Category 45.6 *Smart cards and other e-commerce security measures*

1997-03-17 **electronic commerce smart cards e-commerce**

RISKS 18 91

David Randolph, a correspondent for RISKS, reviewed a paper entitled "Facing the Smart-Card Security Issue" from _Card Technology_ magazine; the key point was that smart card security can be cracked in a few days or a few hours once the system were in place. Randolph wrote, "Based on that, I believe that the challenges to smart cards are very real and that the cost of breaking a smart card is low enough to make it worth while for organized crime to use."

Category 45.6 *Smart cards and other e-commerce security measures*

1997-03-27 **network computer access control smartcard e-commerce**

EDUPAGE

"SMART CARD" STANDARD FOR NETWORK COMPUTERS
IBM, Netscape, Oracle, Sun and Network Computer Inc. have formed an alliance to develop products using a "smart card" technology called OpenCard Framework designed to give people the ability "to access any network computer with any smart card, regardless of the (type of) computer or smart card they're using." Instead of carrying around a laptop computer, a person would just carry the smart card for insertion into any computer that has been adapted for the new technology. To address security concerns, the new technology scrambles the information being transmitted; a person would have to have a personal identification number, or PIN, to use the card. In contrast with a similar project announced last year by Microsoft, Hewlett-Packard, Groupe Bull and Schlumberger, this alliance is targeted to network computers (NCs) rather than personal computers. (AP 26 Mar 97)

Category 45.6 *Smart cards and other e-commerce security measures*

1997-05-04 **Internet law commerce**

EDUPAGE

Quoted from EDUPAGE (written by John Gehl and Suzanne Douglas) with addition of * to mark points:

ADMINISTRATION FAVORS HANDS-OFF APPROACH TOWARD INTERNET
The Clinton administration is working on a White Paper outlining its position on electronic encryption and Internet commerce issues, says Ira Magaziner, senior advisor to the president for policy development. A number of principles will be articulated in the White Paper, including:
* The Internet should be a tax- and duty-free zone; governments of the world should agree to avoid regulating electronic payments systems;
* Private sector consortia, rather than governments, should set technical standards;
* a uniform commercial code should be developed;
* protection of intellectual property on the Internet is important;
* voluntary ratings and filtering systems should be used rather than government-imposed censorship of indecent material on the Internet; and
* a market-oriented approach to privacy is Preferable to government regulation.
(BNA Daily Report for Executives 30 Apr 97)

Category 45.6 *Smart cards and other e-commerce security measures*

1998-08-18 **e-commerce smart cards retailing purchase buy e-cash**

EDUPAGE

MCDONALD'S DISHES UP SMART CARDS
More than 800 McDonald's restaurants in Germany will participate in a pilot project that allows customers to pay for their food using smart cards. The smart card terminals use VeriFone's Transaction Automation Loading and Information Systems technology. An initial rollout at 55 restaurants earlier this year resulted in more than 30,000 transactions during the first 10 weeks of the trial. "This move by the biggest retail food seller in the world portends the future for the United States," says Internet analyst Vernon Keenan. "We're looking at a momentum thing here and VeriFone is not just going to the banks and financial institutions, but they're trying to create a critical mass between the retailers, financial institutions, and other money processors, such as First Data Corp." (Computer Reseller News 18 Aug 98)

Category 45.6 *Smart cards and other e-commerce security measures*

1998-08-23 **e-commerce e-cash buy retail purchase consumer**

EDUPAGE

CYBERCASH CHANGES WALLETS
CyberCash says it's abandoning its client-side software "wallets" in favor of InstaBuy, an automated payment interface supporting Secure Sockets Layer encryption. The digital wallet concept had never really caught on with consumers, who were required to download multimegabyte-sized software and configure it in order to use the service. Despite the change, analysts are still cautious. "InstaBuy solves some problems but also leaves major questions on the table," says an analyst at Keenan Vision. "It piles costs onto the merchant," by requiring them to pay set-up fees, monthly access fees, and between 10 and 30 cents per sale. InstaBuy's commercial release is slated for October, and CyberCash says it expects to sign up a critical mass of the top 100 Internet retail sites and five selected banks. (InternetWeek 21 Aug 98)

Category 45.6 *Smart cards and other e-commerce security measures*

1999-05-10 **e-commerce Web credit card fraud heuristics AI detection**

Wall Street Journal

HNC Software Inc. announced extension of its credit-card monitoring services to Web merchants. Using neural nets for heuristic pattern-recognition of fraudulent transactions, the company has amassed a database of more than 260M credit card accounts' spending habits.

Category 45.6 *Smart cards and other e-commerce security measures*

1999-05-15 **smart card vulnerabilities common criteria protection profile credit-card**

Crypto-gram 99 05

According to Bruce Schneier, "Visa has issued a draft of the `Visa Smart Card Protection Profile,' as part of the Common Criteria. It contains a very nice list of smart card attacks. The document is a draft, and they want comments. < http://www.visa.com/nt/chip/accept.html http://jya.com/drpp-v.pdf >"

Category 45.6 *Smart cards and other e-commerce security measures*

1999-09-29 **secure PC encryption identification authentication access control smart card**

Business Wire

IBM announced its PC 300PL product line for secure electronic commerce. The secure desktop computers come equipped with an embedded security chip, smart-card access and data encryption.

Category 45.6 *Smart cards and other e-commerce security measures*

2000-09-23 **artificial intelligence pattern recognition faulty design assumptions reasoning credit card fraud prevention algorithm foolish**

RISKS 21 06

The CIBC (Canadian Imperial Bank of Commerce) has software that monitors buying patterns for its users. Unfortunately, a user and her husband discovered that their card had been frozen when they paid for a ferry to Vancouver, BC and the anti-fraud team received no answer at their home phone (because they were both on the ferry!). Rodger Whitlock commented in RISKS, "Badly thought-out computer wonkism strikes again."

A follow-up response from Perry Bowker suggested that actually, such pattern recognition really does stop fraud and that a solution to the problem described above is to carry two different credit cards, with one as a backup.

Category 45.6 *Smart cards and other e-commerce security measures*

2000-12-01 **e-commerce litigation jurisdiction fraud complaint lawsuit regulation legislation**

NewsScan, The Standard
http://www.thestandard.com/article/display/0,1151,20526,00.html

European justice ministers passed a law on Thursday that allows online shoppers to pursue disputes with e-commerce merchants in their own countries, rather than having to incur the expense and aggravation of dealing with a foreign legal system. The law, dubbed the Brussels I regulation, is essential to help get e-commerce off the ground in Europe, argued the justice ministers and the European Commission, which drafted the legislation. "A lack of consumer confidence is the main thing holding up the development of e-commerce here," said an EC spokesman. But industry representatives say this approach will create problems for smaller e-tailers: "For large companies it isn't a problem, because they have offices and lawyers in all EU countries. The SMEs (small and medium-sized enterprises) would be burdened with substantial legal and insurance costs if they took protection against litigation from outside their home market," says Wim Mijs, VP of EU affairs at Dutch bank ABN Amro. "As a result, venture capitalists might be a little more cautious about investing in a European Web venture." The EC regulation preempts less-stringent cross-border legislation currently under debate at the Hague Convention. (The Standard 1 Dec 2000)

Category 45.6 *Smart cards and other e-commerce security measures*

2000-12-21 **copy protection intellectual property hardware equipment politics protest**

RISKS, TheRegister.com http://www.theregister.co.uk/content/2/15620.html 21 17

John Gilmore published an anguished attack on the possibility that hardware vendors Intel and IBM were working on integrating copy protection into disk drives to preclude illegal copying of proprietary programs or data.

Category 45.6 *Smart cards and other e-commerce security measures*

2001-01-04 **e-commerce dispute resolution alternative arbitration**

NewsScan

E-COMMERCE PROTOCOL AIMS AT QUICK DISPUTE RESOLUTION

In an effort to speed up e-commerce dispute resolution, a number of major companies, including AT&T, DaimlerChrysler and Microsoft, are signing on to an "e-commerce protocol" drafted by the American Arbitration Association. The document, being released today, lists only vague principles, such as "fairness," "continuity of business" and "commitment to technology," but arbitration association president William K. Slate II says his organization will be rolling out over the next several months "proprietary" technologies that will make it possible to resolve disputes quickly. (Wall Street Journal 4 Jan 2001)
http://interactive.wsj.com/articles/SB978566423262962375.htm

Category 45.6 *Smart cards and other e-commerce security measures*

2001-04-21 **copyright intellectual property digital rights management DRM patent infringement lawsuit**

NewsScan

INTERTRUST SUES MICROSOFT FOR PATENT INFRINGEMENT [27 Apr 2001]
InterTrust Technologies, which makes copyright-protection technology, has sued Microsoft for patent infringement, alleging that the software giant's Windows Media product violates a patent issued to InterTrust in February. The case focuses on digital rights management (DRM) technology, which typically is used in conjunction with downloadable music and other intellectual property to limit access to paying customers. DRM can also be used to enforce any rules set by copyright holders, for instance, allowing a customer to listen to a song three times for free and then cutting off access until a credit card number is submitted. InterTrust has tried unsuccessfully to get Microsoft to license its technology, but Microsoft has continued to ship its own DRM software as part of Windows Media. "InterTrust has invested quite heavily in its patent portfolio," says an InterTrust division president. "We believe we've made seminal investments that relate to the digital-rights management space." A Microsoft spokesman said the company is reviewing the complaint, but that it had been developing its own content-protection technology for years. (Wall Street Journal 27 Apr 2001) http://interactive.wsj.com/articles/SB988324594170991932.htm

---

Category 45.6 *Smart cards and other e-commerce security measures*

2001-08-20 **encryption movie Internet distribution copyright intellectual property**

NewsScan

HOLLYWOOD TO OFFER VIDEO-ON-THE-NET [17 Aug 2001]
Hoping to ward off movie piracy over the Internet, Hollywood studios Warner Bros., MGM, Paramount, Sony Pictures, and Universal Studios are entering into a joint venture that will be used to distribute their products over the Internet to personal computers. The transmissions, which will take 20 to 40 minutes for downloading of a feature-length film, will be encrypted to prevent them from being intercepted. One executive involved in the joint venture calls the plan "an offensive move by the studios," intended both to create "a new distribution platform through the PC," and also to offer "a high-quality, legal, convenient, user-friendly service for movies over the Internet." (New York Times 17 Aug 2001)
http://washingtonpost.com/wp-dyn/articles/A23001-2001Aug16.html

[And a few days later, a report on a way to transfer the download to a normal DVD player:]

HP UNVEILS FIRST DVD+RW DRIVE [20 Aug 2001]
Hewlett-Packard next month will debut the first commercially available DVD drive for PCs that allows users record a movie, watch it on a typical home DVD player, and then erase and record again on the same disc. The DVD-writer dvd100i will carry a price tag of $599, and PC and electronics makers are hoping the new product will jumpstart holiday sales as consumers seek out the latest gadgetry to complement their home entertainment centers. Dataquest estimates that 2.1 million DVD rewritable drives will ship by the end of next year, and that by 2005, that number will reach 14.3 million drives. In addition to HP's backing, the DVD+RW format has the support of Dell, Sony, Philips Electronics, Mitsubishi, Ricoh, Thomson Multimedia and Yamaha. (ZDNet News 20 Aug 2001)
http://news.excite.com/news/zd/010820/07/hp-plays-first

Category 45.6 *Smart cards and other e-commerce security measures*

2001-12-17 **copy protection incompatibility uncopiable**

NewsScan

MORE MUSIC, LESS RIPPING AND BURNING [17 Dec 2001]
To protect itself against people who try to make illegal copies of music, the recording company Universal Music is issuing its newest release ("Fast & Furious: More Music") in a copy-protected form intended to prevent consumers from "ripping" tracks in digital MP3 format. The disk will also be unplayable on Mac computers, DVD players, and game consoles. Hilary Rosen of the Recording Industry Association of America says, "Unfortunately, phenomena like Napster and the ease of 'ripping and burning' are causing artists and record companies real harm... Most movies and video games sold today have some form of protection -- musicians are an exception to the case and do not enjoy the same protection. It is not surprising, therefore, that the recording industry is taking steps to get in tune with the rest of the entertainment field." (San Jose Mercury News 17 Dec 2001)
http://www.siliconvalley.com/docs/news/svfront/cd121701.htm

Category 45.6 *Smart cards and other e-commerce security measures*

2002-01-10 **e-commerce magnetic stripes counterfeit fraud**

RISKS 21 86

Tim Christman was reading an article about the magnetic-stripe cards being used as gift certificates by some retailers when he realized that they are subject to easy fraud. He wrote,
>Ideally, the purchase of a gift card would result in a database being updated to reflect the balance associated with the card's unique account number.

Some retailers are using sequential account numbers and have no provisions to protect against a thief using a mag-stripe reader/writer to re-program a stolen card or small denomination card so that it matches the account number of a larger valued card purchased by someone else. Many retailers even provide a convenient 1-800 number so that the thief, knowing many valid account numbers, can "shop" for a card of significantly greater value.

The RISK: A form of fraud, difficult to trace, involving a minimal investment in equipment by the thief. Also note that the thief only requires the ability to query the back-end database (through the toll-free number), not the ability to manipulate the records. Perhaps more ominously, the risk is angry family members who find a zero balance on their gift cards!<

Christman recommended adding bar codes to the cards and adding check digits to the magnetically-encoded account numbers but not to the visible account numbers.

Category 45.6 *Smart cards and other e-commerce security measures*

2002-05-18 **anti-piracy technology copy-protected CD damage legal liability**

RISKS 22 07ff

A series of interesting contributions in RISKS debated possible liability for damage caused by copy-protected music CDs that include additional data tracks designed to crash computers when the disks are inserted in CD-ROM players. Manufacturers of the protected disks are trying to prevent music piracy, but many contributors protested that playing CDs on their computers was perfectly normal and that they had never stolen any music at all. One correspondent pointed out that Apple explicitly disclaims any responsibility for damage to their systems from inserting such disks (which typically crash their computers and get stuck in the CD-ROM drive) and describes using these disks as misapplication and therefore out of warranty. Several correspondents urged class-action lawsuits against the makers of copy-protected CDs for failing to include adequate (or any) warnings about not inserting these disks into computer CD drives.

Category 45.6 *Smart cards and other e-commerce security measures*

2002-05-21 **intellectual property copyright music copy-protection CD magic marker**

NewsScan; FindLaw Download This 86

HI-TECH CDs YIELD TO LOW-TECH FELT-TIP MARKER TRICK

Sony's elaborate "Key2Audio" CD copy-protection technology has succumbed to a decidedly low-tech felt-tip marker used to scribble around the rim of a disc. Internet postings say that tape or even a sticky note can be used to cover the security track, typically located on the disc's outer edge. The technology prevents users from playing the CDs on a computer by adding a track that contains bogus data. Because computer drives are programmed to read data files first, the PC tries to play the bogus data file over and over again and never gets to the music files elsewhere on the disc. The result is a CD that will play on standard CD players, but not on CD-ROM drives, some portable devices and even some car stereo systems. Sony has shipped more than 11 million copy-protected CDs in Europe, with the largest number going to Germany -- a market executives say is a hotbed of illegal CD-burning. (Reuters 20 May 2002)
http://www1.excite.com/home/technology/tech_article/0,2109,237089

CD CRACK: MAGIC MARKER INDEED
London -- Technology buffs have cracked music publishing giant Sony Music's elaborate disc copy-protection technology with a decidedly low-tech method: scribbling around the rim of a disk with a felt-tip marker. Internet newsgroups have been circulating news of the discovery for the past week, and in typical newsgroup style, users have pilloried Sony for deploying "hi-tech" copy protection that can be defeated by paying a visit to a stationery store.
http://www.wired.com/news/technology/0,1282,52665,00.html

Category 45.6 *Smart cards and other e-commerce security measures*

2002-06-06 **copyright intellectual property digital content TV decoders smart cards set-top box**

Security Wire Digest 4 44

*MODULE FLOATED AS SOLUTION TO DIGITAL TV HACKS
Europe hopes to come up with an affordable solution to counter the upswing in hacked smart cards to decode digital television networks. As many as a third of all digital TV viewers in some European countries access subscriber services with hacked smart cards, according to a BBC news report. The solution touted by at least one vendor is a removable Conditional Access Module, which includes both a smart card for unscrambling television signals and hardware that fits into a slot on all set-top boxes. Subscribers can download "anti-hacking" updates to the box from a telephone line or replace the module itself if a hack occurs, according to SCM Microsystems CEO Robert Sneider. Previously, the only alternative was the costly replacement of the entire set-top box. An IDC analyst expressed doubt that such a generally available device will reduce hacking since crackers can access the same tools to break the new technology.

Category 45.6 *Smart cards and other e-commerce security measures*

2002-06-20 **TCPA Trusted Computing Platform Alliance surveillance privacy identification**

NewsScan

ENCRYPTION DEBATE
Cambridge University computer scientist Ross Anderson has rekindled the computer encryption debate by expressing fierce skepticism about the motives of the Trusted Computing Platform Alliance (TCPA), an organization formed in 1999 by Compaq, HP, IBM, Microsoft and Intel. Anderson suggests the Alliance simply provides a smokescreen that allows those mainstream computer companies to create a new form of censorship by allowing manufacturers to track and identify information about the computer hardware and operating system software of individual users: "The TCPA appears likely to change the ecology of information goods and services markets so as to favor incumbents, penalize challengers, and slow down the pace of innovation and entrepreneurship." (New York Times 20 Jun 2002)
http://partners.nytimes.com/2002/06/20/technology/20CODE.html

---

Category 45.6 *Smart cards and other e-commerce security measures*

2002-06-28 **standards security Web**

NewsScan

SUN JOINS MICROSOFT, IBM IN TECH STANDARDS
Sun Microsystems is joining rivals Microsoft and IBM in developing the WS-Security Web Services technical standard designed to ensure Web services transactions are secure. Sun made the decision to cooperate on the standard after receiving assurances that other companies would not be charged licensing fees for the technology. (Reuters/Los Angeles Times 28 Jun 2002)
http://www.latimes.com/technology/la-fi-techbrfs28.3jun

Category 45.6 *Smart cards and other e-commerce security measures*

2002-09-11 **e-commerce cigarette vending machine artificial intelligence AI verification age adult child**

NewsScan

CIGARETTE VENDING MACHINES GET HIGH-TECH MAKEOVER
The cigarette vending machine, which had faded into obscurity after criticism that it offered minors easy access to tobacco, is back — this time with high-tech twist designed to discourage underage purchasing. Brown & Williamson's new machines feature a virtual reality sales clerk who talks the buyer through the process, asking customers to swipe their ID and credit card to verify they're 18 or older. If either one fails the test, the clerk delivers a stern rebuke: "I'm sorry, but I can't sell you smokes if you're under 18. Now go home before I call your mama." The company is currently testing the machines in Los Angeles and Cleveland, and plans to install them in bars, nightclubs and restaurants. (CNN.com 11 Sep 2002)

Category 45.6 *Smart cards and other e-commerce security measures*

2003-10-22 **Sony smart card cell phone pay FeliCa**

NewsScan

SONY LOOKS FOR WAYS TO GET SMARTER
Sony is working on ways to extend its smart card payment system — dubbed Edy for "euro, dollar, yen" — to cell phones, allowing customers to pay train fares, pick up the restaurant tab and pay for their dry cleaning via their cell phones. A Sony spokesman acknowledged the company's efforts to migrate its FeliCa smart card technology over to the wireless realm but was close-mouthed about the details: "We're looking into the possibility of integrating FeliCa into mobile phones but beyond that we don't wish to comment." Currently, about 2.7 million Edy cards are in circulation. (AP/Los Angeles Times 22 Oct 2003)

Category 45.6 *Smart cards and other e-commerce security measures*

2003-12-14 **credit cards MasterCard American Express PayPass system store financial data RFID chips**

NewsScan

CREDIT CARDS DO THE WAVE
MasterCard and American Express have been testing "contactless" versions of their credit cards that use an embedded RFID chip rather than a magnetic strip to store financial data. The cards can simply be waved in front of a reader to complete the purchase. "In some instances it's faster than cash. You're eliminating the fumble factor," says a MasterCard VP. The company plans to roll out its PayPass system next year, beginning in fast food joints and other venues where customers tend to be in a hurry. Forrester Research predicts it will take several years for the contactless cards to go mainstream, citing consumers' security concerns and unfamiliarity with the technology as impediments to change. (AP/Wired.com 14 Dec 2003)

Category 45.6 *Smart cards and other e-commerce security measures*

2004-05-03 **smartcard smart card ID Transportation Security Authority TSA Florida**

DHS IAIP Daily;
http://www.thetrucker.com/stories/05_04/0503_smart_card.html

May 03, The Trucker — Prototype 'smart card' ID developed in Florida.

The Transportation Security Administration (TSA), the Florida Trucking Association and Florida state agencies are cooperating on a prototype "smart card" ID to be used at all 14 of the Sunshine State's deep-water ports and eventually by truckers and other transportation workers across the country. In 48 to 72 hours from the time a trucker applied, he or she would get the card containing his or her embedded fingerprints and a chip that could be activated for each port, according to Sandra Lambert, director of the division of driver's licenses for the Florida Department of Highway Safety and Motor Vehicles. The card would be issued after a background check that would include sending pertinent information such as Social Security number, date of birth, and criminal background if any to the FBI in Washington, who would then return the data to local officials who would create and ultimately activate the card unless the driver had committed certain felonies, which would prohibit use of an access card.

Category 45.6 *Smart cards and other e-commerce security measures*

2004-05-16 **virtual account numbers credit card protection one-time hash temporary account e-commerce**

http://www.nytimes.com/2004/05/16/business/yourmoney/16cred.html?th

Users of credit cards from Citibank, MBNA America (which sponsors some 5,000 different affinity cards) and Discover can ask for temporary credit-card numbers that are linked to their real account but expire after a single use. Users can either download software to generate these one-time cryptographic hashes of their account number or they can visit their supplier's Web site to obtain one on demand. In addition to preventing fraudulent misuse of their credit-card number, these temporary card numbers can also stop retailers from unauthorized renewals of subscription services.

SINGLE-USE CREDIT CARDS
To combat identity theft, credit-card issuers sometimes issue virtual account numbers, which you typically obtain by signing up at the company's Web site and then download software to your computer to get a new disposable account number before each purchase you make. The number can only be used at one merchant, whether for a single purchase or for a service with a recurring monthly charge. MNBA executive Jim Donahue says, "It certainly has yet to capture the majority of cardholders, but those who use it are very loyal to it." However, since account holders normally don't have to pay for fraudulent purchases made to their accounts, many of them see no personal advantage to going through the extra step of obtaining a virtual account number. (AP/USA Today 10 May 2004) [NewsScan]

Category 45.6 *Smart cards and other e-commerce security measures*

2004-10-01 **smart cards Matsushita memory RAM e-cash identification authentication I&A**

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/9809932.htm

MATSUSHITA'S SMART CARDS

Japanese electronics company Matsushita Electric Industrial is adding smart-card capabilities to its memory cards, in which an integrated-circuit (IC) chip inside the card connects wirelessly with a special reader-machine to enable cashless payments, open locks, and read personal IDs. In a demo of the card's capabilities, Matsushita showed how a soccer-game ticket could be downloaded to a memory card on a personal computer, transferred to a cell phone, and then used at the stadium gate to get in instantly.

Category 45.6 *Smart cards and other e-commerce security measures*

2004-10-07 **smart cards Matsushita memory RAM e-cash identification authentication I&A**

NewsScan; http://apnews.excite.com/article/20041007/D85IJ5C80.html

ALL-IN-ONE MEMORY CARDS

Matsushita Electric Industrial Co., which makes Panasonic brands, is now developing memory cards that can be used for a variety of purposes -- from making cashless payments to opening locks. In Japan, people are already using smart cards to board commuter trains, and cell phone models enable users to buy drinks from vending machines, pay restaurant bills and play games at a Tokyo arcade. Matsushita's smartSD Card features 128-megabytes of memory, compared with Sony's FeliCa smart cards, which have only 32 kilobytes of storage. The enhanced Matsushita model will enable users to download movies or music and provide secure storage for documents, says Matsushita director Masaki Akiyama.

45.7 Sales taxes on Internet commerce

Category 45.7 *Sales taxes on Internet commerce*

1998-02-26 **electronic commerce states tax Internet**

EDUPAGE

GOVERNORS WANT TO TAX INTERNET; CLINTON URGES MORATORIUM
Because he believes the Internet is spurring the growth of new industries and helping create a new economy based on high technology, President Clinton is opposing the National Governors' Association's call to Congress to enact legislation for a uniform system to collect state taxes on sales conducted via Internet. The Governors say that without such legislation the states will increasingly be deprived of a valuable source of revenue, but Clinton supports a moratorium on taxing Internet commerce, to allow for long-term discussion of the issues. (New York Times 26 Feb 98)

Category 45.7 *Sales taxes on Internet commerce*

2002-11-13 **Internet e-commerce taxation government regulations standards**

NewsScan

STATES TAKE MAJOR STEP TOWARD NET SALES TAX
More than 30 U.S. states have approved the Streamlined Sales Tax Project, giving a boost to efforts aimed at creating a system to impose state and local sales tax on items sold via the Internet. The agreement sets unified definitions of products, which previously had varied from region to region, and also requires participating state and local governments to impose only one statewide tax rate for each type of product by 2006. "This is the end of the beginning," said Frank Shafroth, head of state and federal relations at the National Governors Association. "The next step is doing the heavy lifting and getting the state legislatures to actually enact legislation." According to estimates from the Institute for State Studies, state governments could lose some $45 billion in revenue in 2006 and $55 billion in 2011 if online vendors continue to be exempt from collecting taxes on sales to consumers in states where the e-tailer has no physical presence. Detractors of the plan, including the Direct Marketing Association, charge that the agreement is flawed, and could double the number of tax rates to 15,000 rather than reduce them to 200, as claimed. (Reuters/CNet 12 Nov 2002)
http://news.com.com/2100-1017-965554.html

Category 45.7 *Sales taxes on Internet commerce*

2003-02-07 **Internet sales taxes Web e-commerce states**

NewsScan

SALES TAXES CREEP ONTO THE WEB
Internet sales traditionally have been exempted from sales taxes, providing the buyer lived in a different state than the e-tailer they purchased from. But a collective push by states to institute Internet sales taxes is gaining momentum, and several big-name retailers — including Marshall Fields, Target and Wal-Mart — are cooperating. The retailers say they're simply streamlining bookkeeping to accommodate situations where customers purchase on the Web and then return or exchange those items at their physical stores. But according to washingtonpost.com, the retailers have ulterior motivations. In return for collecting the taxes, "38 states and the District of Columbia agreed to absolve the retailers for any liability for taxes not previously collected on Internet sales." And while the stakes are high for states — a University of Tennessee report estimated that states could collectively lose more than $45 billion in Internet sales tax revenue in 2006 — there's no groundswell of opposition from consumers. Jupiter Research yesterday released a study that indicates most online shoppers are indifferent to the issue, with most online shoppers unaware that they can shop around on different sites to avoid the extra charge, and some respondents saying they wouldn't choose one retailer over another just because there was no sales tax. (Washington Post 6 Feb 2003)

Category 45.7 *Sales taxes on Internet commerce*

2003-02-20 **Internet sales taxes interstate e-commerce law**

NewsScan

OREGON SENATOR MOVES AGAINST INTERNET TAXES
Sen. Ron Wyden (D-Ore.) is pushing legislation that would make permanent an existing moratorium on Internet taxes. The current moratorium is set to expire this fall, but Wyden says the pressures on state governments to raise new funds could spark a stampede toward e-commerce sales taxes. "There are thousands of taxing jurisdictions and if all of them, or a significant portion of them, can take a bite out of electronic commerce, I think the consequences would be staggering." (Wall Street Journal 20 Feb 2003)

Category 45.7 *Sales taxes on Internet commerce*

2003-05-12 **internet sale taxes Amazon.com CFO predicts rates Tom Szkutak**

NewsScan

INTERNET SALES TAXES 'INEVITABLE'
Amazon executives believe that collecting sales taxes on Internet purchases is something that is bound to happen, but not anytime soon. Amazon.com chief financial officer Tom Szkutak said at an investment conference that such a development is "inevitable and it's certainly something we support doing — provided that the process is drastically simplified." The current complexity is due to the fact that there are more than 7,500 taxing jurisdictions across the U.S., with varying tax rates and different administrative rules. (AP/USA Today 12 May 2003)

Category 45.7 *Sales taxes on Internet commerce*

2003-05-16 **internet tax ban John Snow multiple discriminatory**

NewsScan

GOV'T OFFICIALS ADVOCATE KEEPING NET TAX BAN
Treasury Secretary John Snow and Commerce Secretary Don Evans are urging Congress to extend the current moratorium on Internet taxes that is set to expire in November. "Government must not slow the rollout or usage of Internet services by establishing administrative barriers or imposing new access taxes," said Snow and Evans in a letter to Rep. James Sensenbrenner (R-Wisc.), chairman of the House Judiciary Committee. The ban on "multiple and discriminatory" taxes on Internet access fees and online traffic is separate from the controversial issue of sales taxes on goods and services sold over the Internet, which are currently prohibited under a 1992 Supreme Court decision. Cash-strapped states and other sales tax advocates have sought to link the two issues in an effort to boost support for online sales taxes. (Reuters/CNet 16 May 2003)

Category 45.7 *Sales taxes on Internet commerce*

2003-09-18 **ban taxes internet access house of representatives bill H.R.49**

NewsScan

HOUSE VOTES FOR PERMANENT BAN ON TAXES FOR INTERNET ACCESS
With bipartisan support, the House of Representatives has passed a bill (H.R. 49) that makes permanent a ban on taxing Internet connections of any kind, including all types of Internet dialup connections and ones made through high-speed DSL or cable access. Rep. Chris Cannon (R-Utah) said: "This bill would broaden access to the Internet, expand consumer choice, promote certainty and growth in the IT sector of our economy and encourage the deployment of broadband services at lower prices." Rep. Gene Green, who was one of several Texas Democrats who opposed the bill, said Texas would lose $45 million a year in tax revenue. "I don't need to remind my colleagues of the fiscal crisis that our states are currently finding ourselves in, including the state of Texas." (AP/San Jose Mercury News 18 Sep 2003)

Category 45.7 *Sales taxes on Internet commerce*

2004-07-12 **New Hampshire Internet chat room tax service providers unhappy**

NewsScan

NEW HAMPSHIRE PLANS TO TAX INTERNET CHAT ROOMS, ETC.

New Hampshire's tax collecting agency is proposing a 7% tax on telephone and Internet services, including chat rooms, voice mail, Web mail and instant messaging. Carol Miller, president of the New Hampshire Internet Service Providers Association, says the rule would be a huge burden to providers and is "far beyond the scope of what the tax was meant for." Verizon spokesman Erle Pierce agrees with Miller: "This is like changing the way you collect a turnpike toll: Instead of taxing the vehicle, we're going to put a tax on all the passengers… You pay not only for the vehicle, but
for what you are carrying in it. I don't think that's what the legislative intent was." But New Hampshire's tax collectors insist the change is just an upgrade to technology that "has forged ahead at a dramatic pace." (AP/USA Today 12 Jul 2004)

Category 45.7 *Sales taxes on Internet commerce*

2005-01-07 **taxes LA Los Angeles Internet lawsuit scam theft embezzlement**

NewsScan; http://www.usatoday.com/tech/news/2005-01-06-travel-suit_x.htm

L.A. SUES INTERNET TRAVEL SITES FOR ROOM TAXES

The city of Los Angeles is suing Internet travel sites Travelocity, Hotwire, Priceline, Expedia and Orbitz for failing to pay millions of dollars in hotel room taxes. The way it works is this: the travel sites negotiate discount rates for bulk purchase of rooms, mark up the rates for online sales of individual rooms, and then pay the city taxes on the negotiated rates rather than on the marked-up rates. A spokesperson for the city says, "The Web sites can't have it both ways. They can't charge consumers taxes based on retail price but give back to the city only part of the money." The defendants call the allegations in the lawsuit are "entirely without merit." (AP/USA Today 7 Jan 2005)

Category 45.7 *Sales taxes on Internet commerce*

2005-01-28 **Internet sales tax state online purchases tracking software registration merchants surveillance**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A44057-2005Jan28.html

PLANS FOR TAXING THE INTERNET

Forty state governments and the District of Columbia have issued bids from technology companies to design the software and Web-based networks for tracking online purchases and processing sales tax payments. Technology and consulting companies hoping to work on the project include Accenture, EDS, KPMG and PriceWaterhouseCoopers, along with software companies Taxware, Tax Matrix Technologies, and Vertex. Maureeen Riehl of the National Retail Federation notes: "A lot of businesses said they didn't want anyone running the registration system who could use the information as an opportunity to go after merchants for other things." (Washington Post 28 Jan 2005)

Category 45.7 *Sales taxes on Internet commerce*

2005-08-23 **FCC Internet telephone VoIP tax proposal Universal Service Fund USF**

EDUPAGE; http://news.zdnet.com/2100-1035_22-5842237.html

FCC PROPOSES USF TAX ON NET PHONE USERS

A Federal Communications Commission proposal released to public notice by the FCC's federal-state joint board on universal service recommends requiring more companies to pay taxes into the Universal Service Fund (USF). The shift would mostly affect Internet telephone providers, which don't currently pay into the fund. Internet-based services such as chat and instant messaging that don't link to the public telephone network would continue to be exempt from USF taxes, according to the proposal. The USF subsidizes telephone services in rural and high-cost areas, and companies that currently pay into the fund pass the costs on to their customers. ZDNet, 23 August 2005

Category 45.7 *Sales taxes on Internet commerce*

2005-12-14 **Internet phone VoIP tax FCC Universal Service Fund USF**

EDUPAGE; http://news.zdnet.com/2100-1035_22-5995488.html

FCC CHAIR PUSHES NEW INTERNET PHONE TAX

Chairman Kevin Martin said that imposing new taxes on more Internet phone users will probably be a priority next year for the FCC. The issue arose with regard to the Universal Service Fund (USF), which subsidizes services in rural and other high-cost areas, schools, and libraries. Long-distance, pay, wireless, and regular telephone services pay into the fund. Not determined are how such taxes will affect voice over Internet protocol (VoIP) providers and other telecommunications services. Some of the companies that provide VoIP services already contribute to the USF, but no regulations require such participation. "We need to move to collection for the Universal Service Fund that is technology-neutral," said Martin. Congress also is expected to address changes to universal service reform in 2006. ZDNet, 14 December 2005

45.8 E-commerce laws

Category 45.8 *E-commerce laws*

1999-01-15 **privacy government international standards business regulate**

EDUPAGE; Miami Herald

MEDIA GROUPS WORK TO ESTABLISH E-COMMERCE GUIDELINES
Top executives from America Online, Time Warner, Vivendi and Bertelsmann have established a working group to advocate ways of keeping global Internet trade free of government regulations. "We are convinced that the best way is through self regulation and business-oriented policies," says Bertelsmann's Thomas Middelhoff, who adds that his group is in sharp disagreement with the European privacy initiative, which restricts database exchanges with countries that have a lower level of consumer privacy guarantees than the EU. The working group will tackle issues such as privacy safeguards, building consumer confidence, legal responsibilities, taxes and tariffs, jurisdiction, infrastructure and intellectual property rights. Other U.S. companies that have joined the group include IBM, Hewlett-Packard, MCI WorldCom, and Netscape. (Miami Herald 15 Jan 99)

Category 45.8 *E-commerce laws*

1999-04-12 **law legislation Congress digital commerce signature contract**

Internet World, Reuters

LEGISLATION SEEKS TO SPELL OUT LEGALITY OF DIGITAL SIGNATURES
A bipartisan group of Congressmen have introduced legislation known as the Millennium Digital Commerce Act that could potentially make electronic contracts legally binding. The bill would also allow the parties to decide among themselves what type of electronic signature they use. The bill, introduced by Senators Spencer Abraham (R-Mich.), John McCain (R-Ariz.), and Rep. Anna Eshoo (D-Calif.), should provide a uniform approach for regulation of digital signatures among several discrepant laws enacted in more than 40 states. The Information Technology Association of America's John Englund says that such legislation will foster companies' trust in the medium. (Internet World 04/12/99)

Category 45.8 *E-commerce laws*

1999-04-13 **information warfare survey fraud theft gambling music piracy intellectual property law**

The Times of London

In Britain, pressure began to mount for government intervention in e-commerce. An article in _The Times of London_ reported, "The National Fraud Information Centre's list of leading Internet crimes includes web auctions (items bid for but never delivered); charges for services thought to be free; empty promises of business opportunities or franchises; false promises of credit cards to people with bad credit histories; and phony job agencies wanting fees to match people to jobs. Other cons range from bogus investments and false vacation offers to fake scholarship search services and fraudulent prize offers."

Category 45.8 *E-commerce laws*

2003-11-07 **FTC Federal Trade Commission MSN messenger microsoft pop-ups security backdoor administrator messages windows**

NewsScan

FTC TAKES AIM AT MESSENGER POP-UPS
The Federal Trade Commission has obtained a temporary restraining order against D Squared Solutions, accusing it of "high-tech extortion" for its annoying marketing campaign, which bombards Microsoft Windows users with pop-up ads touting its $29.95 pop-up blocker software designed to prevent such intrusions. The company set out "to create a problem for consumers and then try to charge them for a solution," said Howard Beales, head of the FTC's consumer protection unit. The FTC is seeking to recoup "hundreds of thousands" of dollars that beleaguered consumers paid to D Squared Solutions for the ad-blocking software. The ads take advantage of a security feature in Microsoft's Windows Messenger service that was originally designed to enable corporate network administrators to send internal messages. These messages are different from the ones imposed on users who visit a Web site, said Beales. "What we are challenging is this 'backdoor' kind of advertising, particularly when it is done in a way and with a frequency that threatens to impair consumers' ability to use their computers." (Los Angeles Times 7 Nov 2003)

Category 45.8 E-commerce laws

2005-01-06 **Canada Internet prescription drug sales ban proposal law legislation pharmacies**

NewsScan; http://www.latimes.com/technology/ats-ap_technology16jan06

CANADA CONSIDERS BAN OF INTERNET DRUG SALES

Canadian health officials have drafted a proposal that would ban Internet sales of prescription drugs to U.S. consumers and effectively destroy a $700 million industry that has become increasingly popular with patients in search of cheaper medicine. Within Canada's socialized medical system, the Canadian government sets drug prices lower than those charged in the U.S., and Canadian doctors now co-sign prescriptions for U.S. patients without examining them in person. The new proposal would prohibit prescriptions for foreigners who are not present in Canada. (AP/Los Angeles Times 6 Jan 2005)

45.9 E-shopping carts

Category 45.9 *E-shopping carts*

1999-04-22 **privacy credit card Web quality assurance ISP Internet Service Provider QA bug error**

AP, http://www.infobeat.com/stories/cgi/story.cgi?id=2559272284-9a6

Joe Harris, a computer technician at the Seattle-area "Blarg! Online" ISP, discovered that improperly-installed shopping-cart software used widely on the Net to simplify shopping can allow anyone to see confidential data such as credit-card numbers. Security analysts pointed out that the plain ASCII file where such data are stored should not be on the Web server at all, or if it is, the file should be encrypted. Initial evaluation suggested that the weakness affects at least several hundred and possibly many thousands of e-commerce sites where the software installations were improperly done.

Category 45.9 *E-shopping carts*

2000-02-03 **shopping cart vulnerability data diddling**

TheRegister.com http://www.theregister.co.uk/000203-000006.html

According to Internet Security Systems (ISS), 11 shopping-cart software packages in use on the Net allow hackers to modify prices of goods when they are added to the order. One vulnerability involves using hidden fields in HTML forms to hold information about the products sold; since it is possible to see and modify HTML source locally, criminals can alter the prices before ordering. Another hole involves similar fields for discount information. A third occurs when programmers put the price in the URL, so that altering that parameter alters the price for the shopping cart.

Category 45.9 *E-shopping carts*

2001-06-06 **QA quality assurance e-commerce Web shopping cart software bug data entry error refund**

RISKS 21 46

Steve Loughran, writing in RISKS, reported that the shopping cart software for a particular Web site allowed him to enter negative quantities into an order form, resulting in apparent refunds. He was too honest to continue with the order to find out if he really would get a check.

Category 45.9 *E-shopping carts*

2004-11-09 **e-commerce shopping carts flash usability utility ease-of-use user resistance frustration abandon give up quit**

NewsScan; http://online.wsj.com/article/0

FLASH-BASED SHOPPING CARTS AIM TO CLOSE E-SALES

A recent study by DoubleClick shows that for every dollar spent on e-commerce sites, $4.10 is left in abandoned shopping carts, and now a handful of e-shopping sites are taking steps to recapture some of those sales. The key is a streamlined checkout process that allows the shopper to perform more functions -- from changing the color of a clothing item to filling out credit card information -- without leaving the page. Proponents of the new systems say that by preventing shoppers from jumping from screen to screen in the final stages of a purchase, consumers are less likely to become frustrated and quit. And while the new checkout screens look just like a Web page, they're actually small software programs written using Macromedia's Flash software that dynamically update the bottom line -- including tax and shipping costs -- as the customer adds or deletes items. Billing and other information is verified as it is entered to prevent customers from moving forward in the process without valid data. The Flashbased carts are being used by TJX Companies, owner of the T.J. Maxx and HomeGoods chains, and by PC Connection, among others. "This technology is very much in keeping with our sense of wanting to make it convenient for customers to shop our stores," says TJX VP Sherry Lang. "Even in our stores, we have a bank of cash registers so customers are able to check out very easily." (Wall Street Journal 9 Nov 2004)

Category 45.9 E-shopping carts

2005-04-22 **WebAPP e-cart module vulnerability command injection attack no update issued**

DHS IAIP Daily; http://secunia.com/advisories/15054/

WEBAPP E-CART MODULE SHELL COMMAND INJECTION VULNERABILITY

A vulnerability has been reported in the E-Cart module for WebAPP, which can be exploited by malicious people to compromise a vulnerable system. Input passed to the "art" parameter in "index.cgi" isn't properly sanitised before being used in an "open()" call. This can be exploited to inject arbitrary shell commands via the "|" character. The vulnerability has been reported in version 1.1. Other versions may also be affected. There is no solution at this time.

46 Cryptography exports from US; Key escrow

Category 46 *Cryptography exports from US; Key escrow*

1996-12-31 **Crypto exports**

RISKS 18 75 ff

Anxiety rose quickly in the security world when readers of the new US cryptographic export restrictions realized that practically all security software is theoretically banned from export without a license. This restriction apparently includes anti-virus software. Export has been redefined to making such software available on the World Wide Web or via FTP.

Category 46 *Cryptography exports from US; Key escrow*

1997-01-14 **crypto exports**

EDUPAGE

Bill Larson, McAfee Associates CEO, criticized the US administration's restrictions on crypto exports, saying that export controls are completely futile. "If there were any terrorists who wanted to get 180-bit encryption, all they would have to do is walk into any U.S. store and buy our PCCrypto product. They could put one floppy into a briefcase and get on an airplane."

Category 46 *Cryptography exports from US; Key escrow*

1997-01-30 **crypto exports key escrow**

EDUPAGE

The Information Technology Association of America criticized the Administration's key escrow proposals, saying that such regulations "could have a detrimental effect on international trade and the world's ability to use the Internet for international commerce."

Category 46 *Cryptography exports from US; Key escrow*

1997-02-11 **crypto exports**

EDUPAGE

Under the marginally relaxed new rules governing crypto exports, Digital Equipment Corp., Cylink Corp. and Trusted Information Systems were granted permission by the Department of Commerce of the U.S. to export 56-bit keylength strong cryptography.

Category 46 *Cryptography exports from US; Key escrow*

1997-02-14 **Cryptanalysis**

RISKS 18 82

In early February, Germano Caronni, a graduate student at the Swiss Federal Institute of Technology coordinated the efforts of 3,500 computers to decrypt a message encrypted using a 48-bit RC5 key. The search took 312 hours to test 57% of the keyspace.

Category 46 *Cryptography exports from US; Key escrow*

1997-03-13 **crypto escrow**

RISKS 18 90

Mark Seecof of the LA Times attacked Professor Dorothy Denning for supposedly refusing "to recognize the possibility of misconduct or incompetence by escrowed-key holders or the governments to which they may be subject." He accused her of tarring anyone who disagrees with her position as "crypto-anarchists" and of claiming that encryption would completely stymie police investigations. Dr Denning rebutted this attack, writing that the criticism was directed at a two-year old paper and that her views are constantly evolving (see <http://www.cs.georgetown.edu/~denning/crypto/> for all her papers). Far from believing that key escrow could not be subverted, she had already written that strong safeguards are essential for government access to keys (GAK) to be tolerated. She does not perceive people who disagree with her as evil; and she reported that she was in the process of investigating the link between encryption, crime and law enforcement in much more detail than heretofore.

Category 46 *Cryptography exports from US; Key escrow*

1997-03-25 **crypto escrow law**

EDUPAGE

Four bills dealing with cryptology are pending in the US Congress. The latest attempts to define a key management infrastructure and specifically proposes to allow the use of any encryption at will within the US and the legal procedures for requiring that keys be surrendered to law enforcement agencies.

Category 46 *Cryptography exports from US; Key escrow*

1997-03-27 **crypto export escrow policy**

EDUPAGE, news wires

The OECD responded with mixed signals to the US proposals for key escrow.

Category 46 *Cryptography exports from US; Key escrow*

1997-03-31 **crypto export**

Dow Jones

At the end of March, McAfee Associates announced that it had received permission under the federal Export Administration Regulations to sell 56-bit encryption products overseas.

Category 46 *Cryptography exports from US; Key escrow*

1997-05-08 **crypto export laws**

Wired

At the American Bankers Association meeting in Washington, Undersecretary William Reinsch outlined an Administration plan to allow banks to export direct-home-banking products with arbitrarily-long encryption keys. The allowance applies only to individual banks, not to software companies supplying banks. All third-party encryption software that could be used for general purposes would have to abide by strict government restrictions on encryption technology. SET-compliant programs would be expected to qualify for export under the new rules.

Category 46 *Cryptography exports from US; Key escrow*

1997-05-09 **crypto laws cryptanalysis**

Netly News

Declan McCullagh publishes a blistering attack on the Kerrey bill, The Secure Public Network Act. Criticism focused especially on the criminalization of cryptanalysis, which experts believe to be at the heart of effective evaluation of cryptographic strength.

Category 46 *Cryptography exports from US; Key escrow*

1997-05-09 **crypto export law key recovery**

Wired

Senator Bob Kerrey's (D - Nebraska) Secure Public Network Act supports the White House's approach to cryptography: strict export controls, key recovery, and criminalization of encryption used in a crime. In addition, the proposed legislation would include a Presidential override with no restrictions other than a requirement to report the waiver within 30 days to Congress. The proposed law conflicts with other encryption initiatives that liberalize (some say rationalize) US crypto policy; e.g., SAFE, by Rep. Bob Goodlatte (R-Virginia), and Pro-CODE, by Sen. Conrad Burns (R-Montana) and Sen. Patrick Leahy (D-Vermont).

Category 46 *Cryptography exports from US; Key escrow*

1997-05-18 **SAFE law crypto exports**

EDUPAGE

In mid-May, the House Judiciary Committee approved the "SAFE" bill — "Security and Freedom Through Encryption Act" that would remove restrictions on export of encryption using keyspaces of up to 56 bits. The bill would also stop the US government from making key escrow systems mandatory. However, more problematically, the bill would also attempt to make it a felony to use encryption to conceal evidence when carrying out a felony.

Category 46 *Cryptography exports from US; Key escrow*

1997-05-20 **crypto export**

EDUPAGE

Sun Microsystems got around the stupid US cryptography-export laws by contracting with Russian programmers for cryptographic code to be included in software for overseas customers. According to John Fontana, writing in _Communications Week_, "the product Sun will OEM is Secure Virtual Private Network for Windows. Developed by Moscow-based ElvisPlus Co., the product will be sold through Sun channels under the name PC SunScreen SKIP E+. The software is based on Sun's Simple Key Management for IP (SKIP) encryption and key management technology. It will ship with algorithms for 56- and 64-bit DES, two- and three-key triple DES and 128-bit ciphers for both traffic and key encryption."

Category 46 *Cryptography exports from US; Key escrow*

1997-05-22 **crypto export key escrow recovery**

EDUPAGE

A committee of 11 respected cryptographers and computer security experts released a report condemning the proposed US regulations tying permission for export of strong cryptography to implementation of key-recovery technology. See <http://www.cdt.org> for the full text of the report. William Reinsch, Bureau of Export Administration in the Department of Commerce, retorted that the computer scientists were demolishing a straw man and that the Administration has no intention of mandating a centralized key-recovery system. Instead, said Reinsch, the intention is to require individual organizations to maintain their own key-recovery systems; these could then be used under court order to satisfy the requirements of law enforcement agencies.

Category 46 *Cryptography exports from US; Key escrow*

1997-05-22 **crypto exports law**

Communications Week

The Clinton Administration was apparently dubious about the legality of the Sun Microsystems deal with a Russian cryptography company. The White House statement said, "We are reviewing our regulatory posture with Sun to ensure that their arrangement with the Russian encryption company is in compliance with U.S. export controls."

Category 46 *Cryptography exports from US; Key escrow*

1997-05-29 **crypto key recovery escrow law**

RISKS 19 19

The final version of the important report, "The Risks of Key Recovery, Key Escrow and Trusted Third-Party Encryption" was put on the Web at <http://www.crypto.com/key_study> at the end of May. The authors include Hal Abelson, Ross Anderson, Steve Bellovin, Josh Benaloh, Matt Blaze, Whit Diffie, John Gilmore, Peter Neumann, Ron Rivest, Jeff Schiller, and Bruce Schneier; the report looked at the technical implications, risks, and costs of the key recovery, key escrow and trusted third-party encryption systems proposed by various government bodies and came down pretty hard against their practicality and advisability.

Category 46 *Cryptography exports from US; Key escrow*

1997-06-03 **crypto export**

EDUPAGE

PGP Inc. finally got permission from the U.S. Department of Commerce to export its products with up to 128-bit keyspace to 100 foreign offices of large U.S. corporations.

Category 46 *Cryptography exports from US; Key escrow*

1997-06-18 **crypto key escrow recovery US**

NYT

The Clinton administration began ten pilot projects to create key-recovery systems for its own use. As predicted by critics of key escrow policies, the plans quickly abandoned a centralized escrow agency because the different parts of government wanted no one who had access to their particular encryption keys. Furthermore, none of the internal key-recovery systems under development would store the private keys used to authenticate documents with digital signatures; they would store only the temporary "session keys" used to encrypt specific documents in transit.

Category 46 *Cryptography exports from US; Key escrow*

1997-06-19 **crypto export law**

EDUPAGE, RISKS 19 23

The McCain-Kerrey "Secure Public Networks Act" was introduced in the Senate, proposing to establish a public infrastructure to implement key recovery. The bill would allow licensed export of strong encryption but would allow the Department of Commerce to impose arbitrary export restrictions on any product if (in the words of the EDUPAGE editors) there were "evidence that the product was destined for military, terrorist or criminal use, or for re-exportation to third countries, or for acts against the national security, the public safety, transportation systems, communications networks, financial institutions or other essential interstate commerce systems." Peter G. Neumann added in RISKS 19.23, "The bill was slipped through the committee as a substitute for ProCode, with essentially no discussion. It appears that there are many lurking issues that were not adequately understood by the Senators. Serious study seems urgently needed. [(PGN's note) See http://www.epic.org and http://cdt.org for text and analyses of the bill. . . .]"

The Center for Democracy and Technology issued a blistering analysis of the bill. See <http://www.cdt.org/> for details.

Category 46 *Cryptography exports from US; Key escrow*

1997-06-24 **crypto exports**

PR Newswire

In June, Netscape announced that the Department of Commerce had granted it permission to export Netscape Communicator browser software with 128-bit encryption.

Category 46 *Cryptography exports from US; Key escrow*

1997-06-25 **crypto exports law**

AP

Microsoft and Netscape received an exemption from the Commerce Department's Export Administration Regulations to sell sophisticated cryptographic programs overseas for use in banks. Microsoft's Mike Dusche, financial services industry manager for Microsoft, explained, "There seems to be a trusted relationship between banks in most countries and the U.S. That trusted relationship allows that type of encryption to be available."

Category 46 *Cryptography exports from US; Key escrow*

1997-07-10 **crypto key escrow law FBI**

AP

In early July, FBI Director Louis Freeh told the Senate Judiciary Committee that "Law enforcement is in danger of being outwitted by criminals inside and outside the United States who are using computer data-scrambling devices to traffic in drugs and distribute child pornography," according to Cassandra Burrell of Associated Press. On 24 September, the House Commerce Committee rejected 35 to 16 a proposed bill supported by Freeh, Drug Enforcement Administrator Thomas Constantine and Treasury Undersecretary Raymond Kelly that would have mandated access to cryptographic keys such as key escrow or back doors. The Clinton Administration said in July that any such interference with mandatory key escroew would "severely compromise law enforcement's ability to protect the American people from the threats posed by terrorists, organized crime, child pornographers, drug cartels, financial predators, hostile foreign intelligence agents and other criminals."

Category 46 *Cryptography exports from US; Key escrow*

1997-07-31 **crypto export**

EDUPAGE

Entrust Technologies posted its encryption software, "Solo," on its Web site for free and unrestricted access worldwide.

Category 46 *Cryptography exports from US; Key escrow*

1997-07-31 **encryption law restriction export**

AP

Administration officials protested H.R. 695 (sponsored by Rep. Bob Goodlatte, R-VA), a bill to relax export restrictions on cryptography and which was approved by both the House Judiciary Committee and the International Relations Committee. Opponents of the bill, including the DoD and the FBI, pointed to increased difficulty in wiretapping international criminals; supporters, including the Business Software Alliance, ridiculed the notion that preventing exports in any way inhibits criminals from obtaining and using encryption software.

Category 46 *Cryptography exports from US; Key escrow*

1997-08-12 **eavesdropping FBI wire-tapping**

EDUPAGE

The FBI's proposed to force telecommunications companies to include technological facilities for full wire-tapping of all calls. Civil libertarians and telephone companies objected.

Category 46 *Cryptography exports from US; Key escrow*

1997-08-13 **encryption policy law export restrictions**

ZDNN

In Oslo, opponents of crypto exports posted the source code for the current version of Pretty Good Privacy (PGP 5.0), the famous encryption program that cannot legally be exported in electronic form from the United States. However, the Export Administration Regulations (EAR) that govern encryption exports apparently do not apply to paper source code, so the product was legally sent out of the country on 6,000 pages of printout, scanned back into ASCII, and proofread by an international team of programmers before being posted on the World Wide Web.

Category 46 *Cryptography exports from US; Key escrow*

1997-08-26 **Crypto export policy law controls free speech**

EDUPAGE, UPI, Reuter, MSNBC, AP, CNN

At the start of the year, Professor Daniel Bernstein's lawyers demanded that the US government not enforce its new export restrictions until they have been examined in a court of law to establish their constitutionality. In June, the federal judge whose ruling on the unconstitutionality of the Computer Decency Act in 1996 presaged the Supreme Court's rulings in the same matter said that she expected to rule in favor of plaintiff Daniel Bernstein, a Professor at University of Illinois in Chicago. Prof. Bernstein is furious that current cryptography export regulations have interfered with his ability to publish encryption algorithms in international journals and to teach classes in cryptography to foreign students at his University. In August, Judge Marilyn Patel of the U.S. District court in San Francisco ruled against the Export Administration Regulations, saying that the US governments rules lack all logic in allowing printed source code to be exported but interfering with electronic versions. The government quickly obtained a temporary stay of the judgement pending appeal.

Category 46 *Cryptography exports from US; Key escrow*

1997-08-26 **crypto policy law export controls**

AP

U.S. District Judge Marilyn Hall Patel ruled in late August that the Administration's new export controls on cryptography were a violation of free speech. Patel issued an injunction prohibiting enforcement against Professor Daniel Bernstein and anyone else who wants to use, publish, or discuss the Snuffle encryption algorithm.

Category 46 *Cryptography exports from US; Key escrow*

1997-09-08 **crypto law key escrow back door trap policy**

RISKS 19 37

Congress' proposed legislation to ban domestic US encryption unless the algorithm includes a back door allowing decryption on demand by law enforcement authorities moved famed Ron Rivest to satire. Writing in RISKS, the co-inventor of the Public Key Cryptosystem and founder of RSA Data Security Inc. wrote, "Congress is apparently considering legislation that would make it illegal to post portions of the Bible on the Internet. FBI Director Louis Freeh wants to make it illegal to use secret codes on the Internet that the FBI can't break, and some members of Congress have been drafting legislation in support of Freeh's position. However, such a law might have startling consequences." He explained his _cryptic_ remark with, "A recent best-selling book, "The Bible Code," claims that the Bible is full of secret messages and codes. These messages are only partially decoded so far. If true, the proposed legislation would make it illegal to post the Bible on the Internet, unless someone provides the FBI with a way to decode all of these secret messages contained within the Bible. In addition, perhaps "smiley faces" would have to be registered, as would the sale of all computers, since they are universally devices ". . .that can be used to encrypt communications or
electronic information. . . ."

Category 46 *Cryptography exports from US; Key escrow*

1997-09-09 **crypto key escrow back door policy law**

EDUPAGE

The Clinton administration proposed a new law that would mandate a back door for decryption of all domestic encryption. In addition, the proposal would force telcos and ISPs to implement a bypass for decryption of all traffic encrypted by their chosen protocols (e.g., Secure Sockets Layer).

Category 46 *Cryptography exports from US; Key escrow*

1997-09-09 **crypto export law**

AP

Speaking to the Software Publishers' Association in September, Vice President Al Gore Tuesday reaffirmed the Clinton administration's policy against restricting the sale in the United States of high-tech devices that maintain the privacy of computer messages.

Category 46 *Cryptography exports from US; Key escrow*

1997-09-18 **crypto export foreign law**

EDUPAGE

Ross Anderson, famed British cryptographer and gadfly, criticized the US for weakening cryptography around the world. He cited weaknesses caused by enforcing small (and thus weak) keys in "the Europe-wide Global System for Mobile Communications telephone networks, commercial banking networks and television broadcasting networks."

Category 46 *Cryptography exports from US; Key escrow*

1997-09-25 **crypto policy law export escrow**

EDUPAGE

James Barksdale, CEO of Netscape, lashed out at proposed restrictions on encryption. As reported in the Wall Street Journal, he said, "By taking away encryption as we know it today, the FBI proposal would expose computer users to assault by hackers intent on economic espionage, blackmail and public humiliation. At a recent congressional hearing, one witness testified that with ... $1 billion and 20 people using existing technology, he could effectively shut down the nation's information infrastructure, including all computer, phone and banking networks. . . . The FBI cannot catch every hacker. But there will be fewer and fewer of them trying to penetrate sensitive networks if those networks are adequately protected and communications secured through the use of strong encryption."

Category 46 *Cryptography exports from US; Key escrow*

1997-09-25 **crypto policy law export escrow**

EDUPAGE

According to Alan McDonald of the FBI, people opposing the Administration's policy on restricting strong encryption are elitist, nondemocratic threats to law enforcement.

Category 46 *Cryptography exports from US; Key escrow*

1997-09-25 **crypto law regulation policy**

EDUPAGE

Several professional organizations including the American Association of the Advancement of Science, the American Mathematical Society, the Institute of Electronics and Electrical Engineering, and the American Association of University Professors issued a letter opposing the Administration's proposals for restrictions on encryption technology. A few days later, Netscape CEO James Barkdale cam down hard against the proposed restrictions, saying it could seriously damage US pre-eminence in software. The executive said, ""By taking away encryption as we know it today, the FBI proposal would expose computer users to assault by hackers intent on economic espionage, blackmail and public humiliation. At a recent congressional hearing, one witness testified that with the $1 billion and 20 people using existing technology, he could effectively shut down the nation's information infrastructure, including all computer, phone and banking networks... The FBI cannot catch every hacker. But there will be fewer and fewer of them trying to penetrate sensitive networks if those networks are adequately protected and communications secured through the use of strong encryption."

Category 46 *Cryptography exports from US; Key escrow*

1997-11-24 **digital signatures policy federal government states**

Reuters

At the end of October, the Clinton administration opposed any moves to enact uniform laws covering digital signatures. Speaking at the House Science Committee's Technology Subcommittee, Andrew Pincus (General Counsel of the Department of Commerce) stated that the federal government does not yet know enough about digital signatures to force states into compliance with a general standard. Industry spokespersons such as Jim Bidzos of RSADSI argued strongly that lawmakers should distinguish clearly between keys used for encryption and keys used for digital signatures; any legislation requiring mandatory key escrow should explicitly exclude allowing access to keys used for digital signatures.

Category 46 *Cryptography exports from US; Key escrow*

1997-11-24 **cyberspace crime FBI criminals crypto policy**

Reuters

FBI Director Louis Freeh continued pushing for legal restrictions on stron g cryptography in a speech at the Intl Assoc. of Chiefs of Police in Orlando, FL. Freeh pointed out that criminals can communicate securely with each other via encrypted e-mail and that it is impossible for law enforcement officials to read these messages in a timely fashion, if at all. Freeh complained that the Clinton Administration and "very powerful industry forces" oppose his proposed policies.

Category 46 *Cryptography exports from US; Key escrow*

1997-11-25 **encryption controls regulations laws banking**

EDUPAGE

Reports surfaced in November that the Clinton Administration might support conventional banks and law enforcement agencies in their attempt to block the use of powerful encryption technology in the financial sector.

Category 46 *Cryptography exports from US; Key escrow*

1997-12-23 **crypto export escrow authentication**

RISKS 19 52

John Gilmore issued a blistering challenge to the US cryptographic export regulations by publishing cryptographic authentication code online and issuinga scathing press release attacking the whole idea of cryptographic export controls.

Category 46 *Cryptography exports from US; Key escrow*

1998-01-15 **crypto regulation law restriction**

EDUPAGE

Rep. Robert Goodlatte's (R-VA) Security and Freedom Through Encryption (SAFE) Act had 250 sponsors by January 1998 but attacks continued from the FBI and from national security interests.

Category 46 *Cryptography exports from US; Key escrow*

1998-02-13 **encryption crypto policy government regulations debate**

RISKS 19 59

Whitfield Diffie and Susan Landau published a new book entitled, _Privacy on the Line - The Politics of Wiretapping and Encryption_ published by The MIT Press (Cambridge, MA). ISBN 0-262-04167-7. Peter G. Neurmann, moderator of the RISKS list, wrote, "Excellent book. I read it cover to cover, and it held my attention better than many spy novels."

Category 46 *Cryptography exports from US; Key escrow*

1998-02-27 **encryption crypto export restriction regulation government**

RISKS 19 60

Former NSA Director Admiral Mike McConnell said in an interview published on the Web that he opposes the administrations restrictive attitude towards strong encryption. See <http://www.us.net/softwar/mcc.html>.

Category 46 *Cryptography exports from US; Key escrow*

1998-03-08 **encryption privacy coalition government policy surveillance**

EDUPAGE

The fight over domestic restrictions on strong encryption grew more fierce as a wide-ranging coalition of unusual political bedfellows formed Americans for Computer Privacy. Liberals and conservatives united in opposing Clinton Administration proposals — fueled by demands from the FBI — for restraints on the private use of encryption.

Category 46 *Cryptography exports from US; Key escrow*

1998-03-31 **encryption regulations restriction academic freedom lawsuit**

EDUPAGE

In March, Peter Junger, a professor at Case Western Reserve University, got his lawsuit against US government cryptography export restrictions back on "the fast track" in federal court. The case began in April; in July, US district court Judge James Gwin ruled that software is not speech and therefore not protected by the first amendment of the US constitution.

Category 46 *Cryptography exports from US; Key escrow*

1998-04-16 **encryption export restriction law policy**

EDUPAGE

In a startling development, Commerce Secretary William M. Daley admitted publicly that he disagrees with current attempts to restrict the export of strong cryptography from the US. The New York Times reported him as saying, "There are solutions out there. Solutions that would meet some of law enforcement's needs without compromising the concerns of the privacy and business communities. But I fear our search has thus far been more symbolic than sincere... The cost of our failure will be high. The ultimate result will be foreign dominance of the market. This means a loss of jobs here, and products that do not meet either our law enforcement or national security needs."

Category 46 *Cryptography exports from US; Key escrow*

1998-05-21 **encryption policy restrictions US sales cryptography laws**

EDUPAGE

The Economic Strategy Institute published a report estimating that current cryptographic export restrictions will cost US cryptographic firms about $9B in lost sales in the next five years.

Category 46 *Cryptography exports from US; Key escrow*

1998-06-02 **encryption policy export restrictions US law FBI**

EDUPAGE

In June, top executives of major high-technology companies (including AOL, Microsoft, Netscape, and Sun among others) met Louis Freeh, Director of the FBI. Their mission: convince the feds to back off their insistence on cryptographic export restrictions and insistence on mandated key escrow or back doors in encryption software.

Category 46 *Cryptography exports from US; Key escrow*

1998-06-05 **encryption FBI domestic ISP strong terrorists back door**

TechWeb http://www.techweb.com/wire/story/TWB19980605S0018

FBI director Louis Freeh met in June with the nation's top computer executives in Washington, D.C., to discuss disagreements over domestic use of encryption. America Online chairman Steve Case, AT&T chairman C. Michael Armstrong, MCI president Timothy Price, Microsoft chairman Bill Gates, Netscape CEO James Barksdale, and Sun CEO Scott McNealy made a strong case for unrestricted use of the security technology; Freeh continued to argue that terrorists and other criminals were making use of encryption to evade law enforcement.

Category 46 *Cryptography exports from US; Key escrow*

1998-06-10 **key recovery escrow cryptography export law encryption**

RISKS 19 80

The updated report on "The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption" originally published in May 1997 by the luminaries known as the "11 Cryptographers" was put on the Web at <http://www.crypto.com/key_study>. The preface includes the following trenchant observations: "One year after the 1997 publication of the first edition of this report, its essential finding remains unchanged and substantively unchallenged: The deployment of key recovery systems designed to facilitate surreptitious government access to encrypted data and communications introduces substantial risks and costs. These risks and costs may not be appropriate for many applications of encryption, and they must be more fully addressed as governments consider policies that would encourage ubiquitous key recovery."

Category 46 *Cryptography exports from US; Key escrow*

1998-07-07 **key escrow cryptography regulation government FIPS**

RISKS 19 84

The Administration's continuing attempt to develop key-escrow rules for domestic applications of encryption hit another barrier in June when, according to Alan Davidson of the Center for Democracy and Technology: The 22-member U.S. Government Technical Advisory Committee to Develop a Federal Information Processing Standard for the Federal Key Management Infrastructure (TACDFIPSFKMI) has failed in a two-year effort to design a federal computer security system that includes "back doors," a feature that would enable snooping by law enforcement agencies. Addressing Commerce Secretary William Daley, the panel wrote that it "encountered some significant technical problems that, without resolution, prevent the development of a useful FIPS. ... Because the focus of this work is security, we feel that it is critically important that we produce a document that is complete, coherent, and comprehensive in addressing the many facets of this complex security technology.. The attached document does not satisfy these criteria." However, said the chair of TACDFIPSFKMI (say that one severa times quickly), given that the report was not ready for publication, it was wrong to characterize the decision as a failure. "In the letter," he wrote, "the committee noted that it had made significant progress in its efforts and that committee members were willing to continue work on the document. Many expressed a belief that the document could be successfully completed.

Category 46 *Cryptography exports from US; Key escrow*

1998-07-09 **encryption cryptography export restrictions US law controls**

EDUPAGE

Commerce Secretary William Daley announced in July that financial institutions in 45 nations could henceforth obtain strong encryption from US suppliers without having to prove that they will implement key escrow or back doors ("law enforcement keys").

Category 46 *Cryptography exports from US; Key escrow*

1998-07-14 **encryption cryptography key escrow back door law enforcement**

EDUPAGE

Cisco Systems, Hewlett-Packard, Network Associates, Novell, Sun Microsystems and other firms banded together to propose a compromise on encryption to the FBI. The proposals provide back doors into the encrypted data stream. Administration officials expressed interest.

Category 46 *Cryptography exports from US; Key escrow*

1998-07-21 **encryption restrictions policy US export regulations**

EDUPAGE

When in doubt, advertise. Americans for Computer Privacy, despite the down-home, grass-roots name, is actually a group of 90 high-tech companies fed up with US government interference with their ability to compete with foreign firms using strong encryption in their products. In July, the ACP launched a series of new ads in which apparently normal middle-class Americans seriously and articulately attack the Export Administration Regulations. I suppose that we can hope someday to see advertisements in which ordinary Americans debate the value of key escrow versus mandatory back doors in much the way they currently discuss vans versus sport-utility vehicles.

Category 46 *Cryptography exports from US; Key escrow*

1998-09-17 **encryption export restrictions US government administration**

EDUPAGE

The Administration announced looser restrictions on encryption used in insurance and health care. Products providing key recovery and limited to a 56-bit keyspace would henceforth be exportable without a special license. In October, the Commerce Dept authorized 10 high-tech compannies (Ascend Communications, Bay Networks, 3Com, Cisco Systems, Hewlett-Packard, Network Associates, Novell, Red Creek Communications, Secure Computing, and Sun Microsystems) to export such key-escrow encryption products.

Category 46 *Cryptography exports from US; Key escrow*

1998-12-29 **EAR Export Administration Regulations strong encryption**

InternetWeek
http://www4.zdnet.com/intweek/stories/news/0,4164,2179665,00.html

In December, the U.S. Commerce Department announced that it would relax the Export Administration Regulations to allow encryption products with a much large 128-bit keyspace to be sold by U.S. vendors to foreign purchasers (except for seven "terrorist nations"). In addition, e-commerce, financial and medical applications would be unrestricted (after a 15-day review period following application) and could use the strongest available encryption technology for clients in 42 named countries.

Category 46 *Cryptography exports from US; Key escrow*

1999-01-06 **encryption Export Administration foreign programmers EAR**

CNET news.com http://www.news.com/News/Item/Textonly/0,25,30590,00.html

RSA Data Security Inc. (RSADSI), one of the leading US encryption firms, neatly evaded US export restrictions on strong encryption products by establishing an Australian subsidiary to sell encryption abroad. The U.S. Department of Commerce authorized the business as long as no U.S. employees or technology was used in the Australian business unit. However, there was some question about whether the Wassenaar agreement might impede RSA DSI Australia's success.

Category 46 *Cryptography exports from US; Key escrow*

1999-02-15 **cryptographic export restrictions US government proposals**

Crypto-Gram; EPIC http://www.epic.org/crypto/export_controls/bxa-regs-1298.html 1999 02

On January 1, 1999, the Department of Commerce put into effect modified Export Administration Regulations with slightly more liberal allowance for commercial cryptography exports. The allowance for e-commerce involving banks was extended to merchants, insurance companies and medical applications. In addition, US corporations were permitted to use the same encryption tools for their foreign subsidiaries and some foreign partners.

Category 46 *Cryptography exports from US; Key escrow*

1999-02-26 **encryption key escrow export committee law legislation proposal bill**

Benton; CyberTimes (New York Times), EPIC ALERT

Reps. Bob Goodlatte (R-VA), Zoe Lofgren (D-CA) and 205 other sponsors presented the Security and Freedom through Encryption Act (SAFE) for consideration by the Congress. The bill would eliminate restrictions on exports of encryption tools.

Category 46 *Cryptography exports from US; Key escrow*

1999-04-08 **crypto export controls laws legislation bills**

NEWSBYTES NEWS NETWORK

Jim Lewis, the director of the Office of Strategic Trade in the Commerce Department's Bureau of Export Administration, predicted in April that "Any more major administration changes to US encryption export control policy are unlikely in 1999, along with any relaxation measures getting through Congress either." He was wrong.

Category 46 *Cryptography exports from US; Key escrow*

1999-04-09 **encryption policy regulations restrictions law export**

CMP TechWeb

Shortly after warning that the Administration would NOT reconsider its export controls on encryption, Commerce Department official Jim Lewis, director of the Office of Strategic Trade at the Bureau of Export Administration, admitted that maybe it was time to change after all. According to a survey of 100 countries, "Only a handful of countries actually restrict encryption products," said David Banisar, policy director of EPIC, the Electronic Privacy Information Center. He was speaking at the 1999 Computers, Freedom, and Privacy Conference, a major annual meeting covering issues of privacy and technology. On 1999-4-19, John McCain and colleagues in the Senate of the US introduced a bill to liberalize cryptographic exports.

Category 46 *Cryptography exports from US; Key escrow*

1999-04-15 **encryption legislation law proposal amendment key-escrow blocked debate**

Crypto-gram; ABC, Wired, CDT 99 04

In March 1999, a battle (but not the war) over key-escrow was won in the House Judiciary Committee. H.R. 850, the Security and Freedom through Encryption (SAFE) Act proposed by Rep. Lofgren (D-CA) was under attack by Rep. McCollum (R-FL), who proposed an amendment forcing mandatory key escrow as a condition for exporting encryption products. The amendment was blocked by Rep. Goodlatte (R-VA).

Category 46 *Cryptography exports from US; Key escrow*

1999-05-15 **encryption exports restrictions teaching algorithms publishing free speech first amendment constitution law court judge**

Crypto-gram, Wired 99 05

In 1997, Professor Dan Bernstein won a ruling that declared his Snuffle algorithm a form of speech and therefore not bound by the Export Administration Regulations. The government appealed the decision. In May 1999, the Ninth Circuit Federal Court of Appeals ruled in favor of the original ruling.

Category 46 *Cryptography exports from US; Key escrow*

1999-06-10 **encryption exports restrictions foreign crypto products sales**

New York Times

A study by George Washington University computer scientists found that US restrictions on high-quality encryption software had not impeded the development and availability of strong cryptography in other countries.

Category 46 *Cryptography exports from US; Key escrow*

1999-06-24 **encryption relaxation restriction bill legislation proposal law**

BENTON, Senate of the US http://www.senate.gov/~commerce/press/106-82.htm

In the US Senate, the Committee on Commerce, Science, and Transportation passed S.798, the PROTECT Act, a bill to promote electronic commerce. According to the press release (quoting directly), [t]he bill would do the following: 1) Direct the National Institute of Standards and Technology (NIST) to complete the establishment of an advanced encryption standard by January 1, 2002; 2) Allow for immediate exportation of encryption of key lengths of up to 64 bits; 3) Permit the exportation of non-defense encryption (above 64 bits) to responsible entities and governments of North Atlantic Treaty Organization (NATO), Association of Southeast Asian Nations (ASEAN), and Organization for Economic Cooperation and Development (OECD); 4) Allow for liberalization of export controls for encryption by creating an Encryption Export Advisory Board to review applications for exemption of encryption of over 64 bits and give recommendations to the Secretary of Commerce. The board would be made up of 12 members: the Under Secretary of Commerce for Export Administration, seven individuals appointed by the President (one from the National Security Agency, one from the Central Intelligence Agency, one from the Office of the President, and four representatives from the private sector who have experience in information technology), four representatives appointed by Congress (one by the Majority Leader of the Senate, one by the Minority Leader of the Senate, one by the Speaker of the House, and one by the Minority Leader of the House); 5) Give the Secretary of Commerce 15 days to respond to recommendations. If he rejects a recommended exemption, his decision is subject to judicial review; 6) Reaffirm presidential authority to veto a recommended exemption for national security purposes, and to establish terrorist and embargo controls; 7) Authorize increased funding to law enforcement and national security agencies to upgrade facilities and intelligence; and 8) Give the Secretary of Commerce the authority to prohibit the exportation of particular encryption products to an individual or organization in a foreign country identified by the Secretary.

The bill was then passed by the full Commerce Committee. According to the press release, there were several constraints on exports of encryption: "In approving the bill today, the Committee adopted — all by voice vote — a number of amendments improving the bill. The Committee approved several amendments offered by Mr.Oxley (R-OH); one that allows the Secretary of Commerce to deny the export of encryption products to specific groups and organizations if it would be used to harm national security, used to sexually exploit children or used for illegal activities by organized; another amendment clarifies that despite a company's ability to export a product through encryption capabilities, the Secretary of Commerce may prohibit that product's export for other reasons; and a third amendment requires the Secretary of Commerce to consult with the Secretaries of State and Defense, Director of Central Intelligence and the Attorney General when conducting a technical review of an encryption product for export. The Committee also approved an amendment offered by Mr. Dingell (D-MI) that requires a comparable encryption product be available in a foreign country in order for a U.S. company to export similar encryption technology to that country. The Committee also approved two amendments offered by Mr. Stearns (R-FL); one that prohibits U.S. companies from exporting products to portions of China, specifically to the People's Liberation Army or the Communist China Military; the second amendment requires that if a person has been served a subpoena for access to encrypted information and if the person has the capability to decrypt the information but does not, then that person will be subject to additional criminal penalties."

Category 46 *Cryptography exports from US; Key escrow*

1999-07-14 **encryption relaxation restriction bill legislation proposal law**

Newsbytes

The SAFE bill did not make it safely out of the clutches of the House International Relations Committee in mid-July. Opponents of relaxing encryption controls amended the bill with strict limitations at the behest of the FBI and the DEA. One amendment specifically prohibited all encryption exports to mainland China.

Category 46 *Cryptography exports from US; Key escrow*

1999-07-20 **encryption relaxation restriction bill legislation proposal law**

POLITECH, ITI, Newsbytes

The President of the Information Technology Industry Council (ITI) urged the US House Armed Services Committee not to gut the SAFE bill. Another constituency supporting the SAFE Act was a group of former prosecuting attorneys in Congress. They wrote, "If US encryption continues to be restricted. . . foreign products will soon dominate the worldwide market, hindering our ability to gather intelligence against terrorists and criminals. . . . If cryptography can protect the trade secrets and proprietary information of businesses and thereby reduce economic espionage (which it can), it also supports in a most important manner the job of law enforcement. If cryptography can help protect nationally critical information systems and networks against unauthorized penetration (which it can), it also supports the national security of the United States." Despite the begging, though, the Committee did in fact ruin the bill from the point of view of its sponsors.

Category 46 *Cryptography exports from US; Key escrow*

1999-07-30 **tax benefit encryption key escrow back door**

Wired
http://www.wired.com/news/print_version/politics/story/21014.html?wnpg=all

In July, Reps. Porter Goss (R-FL) and Julian C. Dixon (D-CA) sponsored HR2616, another attempt to encourage key-escrow or law-enforcement-enabled cryptographic software. The bill would give a 15% tax reduction to firms on the costs of developing encryption software with easy access to government-authorized eavesdroppers.

Category 46 *Cryptography exports from US; Key escrow*

1999-08-20 **privacy warrant decryption encryption law enforcement**

Washington Post http://www.washingtonpost.com/wp-srv/business/daily/aug99/encryption20.htm

In August, the Department of Justice proposed the Cyberspace Electronic Security Act, which would allow law enforcement, under warrant, to install software that would disable encryption on personal computers in suspects' homes and offices. The Computer & Communications Industry Association (CCIA) joined with civil liberties organizations in immediately condemning the proposal as a covert intrusion into private homes and offices. [Seems to me that requiring a warrant for installation of the systems and requiring another warrant to read the data provides a pretty strong protection of the citizen. How is this process any weaker than getting a warrant to use binoculars in collecting evidence of wrong-doing?]

Category 46 *Cryptography exports from US; Key escrow*

1999-09-04 **Windows software key NSA controversy overblown rumor jumping conclusions**

Various sources including Washington Post, , New York Times, NTBUGTRAQ.
RISKS

Andrew Fernandes of Cryptonym, a Canadian security firm, seems to have gone off half-cocked when he found a signing key for integrating cryptographic modules into Windows that was labeled "NSA Key." He and other conspiracy buffs interpreted this label to mean that there was somehow a back door into Windows that would allow the National Security Agency to integrate its own cryptographic modules into the operating system yet have the version check out using digital signature verification. Such manipulations could generate versions of Windows with a back door for the NSA. Microsoft denied this interpretation (Aha! Told you!) and claimed that the key was "compliant with the NSA's technical standards." A particularly clear discussion by Russ Cooper <Russ.Cooper@RC.ON.CA> on NTBUGTRAQ pointed out that the conspiracy theory was farfetched but warned that it would be indeed be possible for anyone to insert their own cryptographic modules into Windows and sign them using their own digital key, thus allowing foreign cryptographic code to run under Windows even without signature by Microsoft or approval by the US Dept of Commerce under the Export Administration Regulations.

Category 46 *Cryptography exports from US; Key escrow*

1999-09-30 **cryptography export controls key escrow search seizure fourth amendment constitution law proposal**

USA Today; Crypto-gram 99 10

President Clinton issued a public letter on September 16th addressed to the Congress pushing for passage of the Cyberspace Electronic Security Act of 1999 (CESA), which simultaneously deregulates most encryption software exports and provides for key escrow accessible to law enforcement agencies under warrant.

Category 46 *Cryptography exports from US; Key escrow*

1999-11-24 **cryptography regulations restrictions Department of Commerce limitations export license controls**

New York Times

In mid-November, the Clinton Administration began circulating its proposed new cryptographic export controls. However, according to critics and proponents of unregulated crypto exports, the actual proposals were far less liberal than original indications back in September. In particular, the export regulations continued to enforce license reviews for sales of cryptographic software and hardware to governments overseas.

Category 46 *Cryptography exports from US; Key escrow*

1999-11-24 **encryption relaxation restriction bill legislation proposal law**

EDUPAGE, Washington Post

In September 1999, the Clinton Administration announced its intentions to liberalize encryption exports even further than the changes to the EAR that came into effect in January 1999. By late November, the Administration released another draft for comment, with final regulations due by December 15, 1999. The EDUPAGE editors summarized the situation as follows: "The proposed rules permit the export of retail encryption products with no restrictions on key length. In addition, the draft proposes looser export laws for open source software such as Linux. However, the rules might not apply to encryption software that is part of another program, and full bans would still exist for Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria. Some high-tech firms objected to the draft's unequal treatment of different types of encryption, saying tougher laws would apply to encryption that is built into hardware or software components."

Category 46 *Cryptography exports from US; Key escrow*

2000-01-13 **encryption export restrictions laws regulations**

NewsScan, San Jose Mercury News

In January 2000, the Clinton administration finally gave up on the US government's futile attempts to restrict exports of strong encryption. Henceforth, only crypto sales to foreign governments or military would require US government authorization. What the State Department terms "rogue nations" would still be on the forbidden list (Iran, Iraq, Libya, Syria, Sudan, North Korea, and Cuba).

Category 46 *Cryptography exports from US; Key escrow*

2000-01-15 **encryption relaxation restriction bill legislation proposal law**

Crypto-gram http://www.counterpane.com/crypto-gram-0001.html; PoliTech, Wired http://www.wired.com/news/print/0,1294,33672,00.html 00 01

In January, the newly relaxed encryption export restrictions took effect. The main improvements were that all ordinary "retail" encryption products could be exportable once some paperwork was filled out — except to a list of forbidden terrorist countries. Any product with 65-bit keyspace could be exported without paperwork. Posting source code on the Internet was no longer restricted at all. Famed encryption expert John Young tested the new regulations by posting the binaries for PGP freeware v 6.5.2a for Windows and for Macintosh. The Department of Commerce published a response via Declan McCullagh's POLITECH list stating that in fact there was no problem with such posting.

Category 46 *Cryptography exports from US; Key escrow*

2000-01-15 **encryption export regulations**

Crypto-Gram http://www.counterpane.com/crypto-gram-0001.html 00 01

In January 2000, Bruce Schneier summarized the new cryptography-export regulations as follows: >On the plus side, "retail" encryption products — like browsers, e-mail programs, or PGP — will be widely exportable to all but a few countries "regardless of key length or algorithm." On the minus side, the new regulations are complex (an unending stream of work for the lawyers) and will still make it difficult for many people to freely exchange encryption products. They also do not address the Constitutional free speech concerns raised by encryption export controls.<

He listed major features of the new regulations as follows:
>
* "Retail" encryption products are be exportable, regardless of key length or algorithm, to all but the designated "T-7" terrorist nations. In order to export you need to fill out paperwork. You need to get a retail classification, submit your product to a one-time technical review, and submit periodic reports of who products are shipped to (but not necessarily report end users).

* Export of encryption products up to 64 bits in key length is completely liberalized.

* "Non-retail" products will require a license for many exports, such as to foreign governments or foreign ISPs and telcos under certain circumstances.
<

Category 46 *Cryptography exports from US; Key escrow*

2000-01-18 **operating system Windows 2000 strong encryption export**

Reuters , Wired http://www.wired.com/news/technology/0,1282,33745,00.html

Microsoft announced at the RSA Conference in San Jose, CA in mid-January 2000 that it had received US government authorization to sell its new operating system revision, Windows 2000, with 128-bit encryption enabled.

Category 46 *Cryptography exports from US; Key escrow*

2000-02-02 **Export Administration Regulations EAR restrictions regulations government Commerce**

NewsScan, MSNBC 1 Feb 2000 http://www.msnbc.com/news/364870.asp

The Clinton administration has eliminated restrictions on exporting high-performance computers with speeds below 12,300 MTOPS (millions of theoretical operations per second) to all countries except so-called rogue nations (Iraq, Libya, North Korea, Cuba, Sudan and Syria). Companies exporting computers to "Tier III" nations (including China, Russia, India, Israel and Pakistan) would have to notify the Commerce Department 10 days prior to shipment of any computer operating above 12,500 MTOPS. Exports to "Tier II" countries (South Korea, much of Central and South America and most of Africa) will require licensing above 30,000 MTOPS (previously the threshold was 20,000 MTOPS). Clinton also called for Congress to shorten from six to four months the review period for adjusting export controls, noting the change is needed to "keep up with the rapid pace of technological advance."

Category 46 *Cryptography exports from US; Key escrow*

2000-02-10 **encryption decryption key legal requirement demand penalties prison law proposal**

POLITECH, Slashdot http://slashdot.org/yro/00/02/09/1445242.shtml

In Britain, controversy erupted over proposals for a new law, The Regulation of Investigatory Powers Bill, that would (among other features) require citizens to hand over their decryption keys if subpoenaed by the Crown. Failure to do so could result in imprisonment. Opponents questioned the consequences of forgetting or losing one's key.

Category 46 *Cryptography exports from US; Key escrow*

2000-02-25 **encryption export restriction litigation**

NewsScan, Wall Street Journal
http://interactive.wsj.com/articles/SB951422940442620073.htm

In an about-face, the U.S. government [said] it will allow computer scientist Daniel Bernstein to post the source code for Bernstein's Snuffle encryption software on his Web site. The change of heart came following a district court ruling that in light of the new, liberalized encryption software export restrictions implemented in January, Bernstein should be able to post his code. Bernstein and his lawyer are considering pursuing his lawsuit against the government, however, because "there's an area of ambiguity that remains": the new rules don't address "mirror sites," which copy and publish Web pages automatically to provide speedier access for users in other countries. The rules also require that the source code may be posted as long as residents of countries suspected of supporting terrorism won't have access to the material — an administrative nightmare for any Web operator. (Wall Street Journal 25 Feb 2000)

Category 46 *Cryptography exports from US; Key escrow*

2000-02-26 **encryption export regulations restrictions algorithm posting publication**

RISKS, Reuters http://www.wired.com/news/politics/0,1283,34550,00.html, Wall Street Journal http://interactive.wsj.com/articles/SB951422940442620073.htm 20 82

In February, the US Commerce Department gave up in its futile attempts to prevent Prof. Daniel Bernstein from posting details for his Snuffle encryption algorithm. According to Peter G. Neumann in RISKS, "the residual questions are on areas of ambiguity such as mirror sites and a restriction on access in countries suspected of supporting terrorism."

Category 46 *Cryptography exports from US; Key escrow*

2000-04-05 **encryption export regulations restrictions lawsuit judgement EAR court**

NewsScan, Wall Street Journal
http://interactive.wsj.com/articles/SB954899134353800815.htm

A federal appeals court in Ohio has ruled that encryption software code is protected by the First Amendment because such code is a means of communication between computer programmers. The ruling represents the first time that a federal appellate court has decided software code is protected as free speech, says Raymond Vasvari, legal director of the American Civil Liberties Union: "This is a great day for programmers, computer scientists, and all Americans who believe that privacy and intellectual freedom should be free from government control." The court's decision means a lawsuit filed by Cleveland law professor Peter Junger will be reconsidered. Junger had claimed that the government violated his free-speech rights by requiring export licenses for encryption programs. (Wall Street Journal 5 Apr 2000)

Category 46 *Cryptography exports from US; Key escrow*

2000-07-18 **encryption policy controls regulations restrictions monitoring surveillance Internet traffic law enforcement investigation wiretaps interception**

NewsScan, Washington Post http://www.washingtonpost.com/wp-dyn/articles/A57330-2000Jul17.html

A speech by White House chief of staff John D. Podesta . . . pleased the business community with the Administration's new software encryption policy, which will loosen export controls on encryption technology, but upset civil libertarians with the Clinton Administration's position on allowing law enforcement agencies to monitor Internet traffic. Barry Steinhardt of the American Civil Liberties Union said the government's attempt to expand wiretapping on the Internet "represents a grave threat to the privacy of all Americans by giving law enforcement agencies unsupervised access to a nearly unlimited amount of communications traffic." (Washington Post 18 Jul 2000)

Category 46 *Cryptography exports from US; Key escrow*

2001-01-11 **EAR Export Administration Regulations loosening restrictions high technology supercomputers**

NewsScan

FURTHER RELAXATION OF TECHNOLOGY EXPORT REGULATIONS
The Clinton Administration has relaxed restrictions on the export of high-speed commercial computers, and will now add to the list of so-called "Tier 1" countries that U.S. manufacturers can sell computers without obtaining individual export licenses the countries of Central and South America; South Korea and many other Southeast Asia countries; Slovenia; most countries in Africa; and Lithuania. The new guidelines will be reviewed by the Bush Administration after it takes office. (New York Times 11 Jan 2001)
http://partners.nytimes.com/2001/01/11/technology/11EXPO.html

---

Category 46 *Cryptography exports from US; Key escrow*

2001-06-08 **export administration regulations EAR study**

NewsScan

COMPUTER EXPORT CONTROLS? GIVE THEM UP, SAYS REPORT
A new study by the Center for Strategic and International Studies concludes that this country's 1990s-vintage computer export controls are irrelevant to U.S. security and urges that they be discarded. "Computing power is considerably less important for building modern weapons than is the ability to integrate materials, manufacturing equipment and technology... The problem is that the supercomputer of 1990 -- a computer then manufactured only in the dozens of units -- had by the year 2000 become the laptop manufactured in the hundreds of thousands." (Reuters/San Jose Mercury News 8 Jun 2001)
http://www.siliconvalley.com/docs/news/svfront/001404.htm

Category 46 *Cryptography exports from US; Key escrow*

2002-01-02 **EAR Export Administration Regulations loosening restrictions high technology supercomputers**

NewsScan

BUSH RELAXES COMPUTER EXPORT CONTROLS [2 Jan 2002]
The Bush administration has rolled back restrictions on sales of high-speed computers to Russia, China, India and some countries in the Middle East, more than doubling the allowable processor speed to 195,000 MTOPS (millions of theoretical operations per second). A typical U.S. home PC now sold in retail stores tops out at about 2,100 MTOPS. The change means that those countries will now have access to U.S. computers capable of complex 3D modeling, calculating fluid dynamics, and other advanced applications. The U.S. will maintain its high-tech embargo on exports to North Korea, Iran, Iraq, Libya, Cuba, Sudan and Syria. (Reuters 2 Jan 2002)
http://www1.excite.com/home/technology/tech_article/0,2109,199172|technology |01-02-2002::19:33|reuters,00.html

---

Category 46 *Cryptography exports from US; Key escrow*

2002-04-25 **EAR US encryption expert restrictions controls homeland security infrastructure protection**

Security Wire Digest 4 32

*EXPORT ADMINISTRATION OPERATES UNDER NEW NAME
To better reflect its new role in cybersecurity, the U.S. Bureau of Export Administration is now called the Bureau of Industry and Security. The agency is tasked with preventing certain technologies from being exported to countries hostile toward the United States. The bureau has assumed a more visible role in homeland security since the Sept. 11 terrorist attacks, including coordinating all U.S. Department of Commerce homeland security activities and leading an outreach program to educate private industry on critical infrastructure protections.

47 US computer-crime laws

Category 47 *US computer-crime laws*

2002-09-26 **criminal hacking legislation proposed law bill intellectual property piracy inspection monitoring penetration**

NewsScan

HACKING BY ANY OTHER NAME
A new debate in Congress over legislation proposed by Howard Berman (D-Calif.) will have to struggle to find a definition of the word "hacking." Berman's bill would give the recording industry the right to use network software to inspect people's personal computer files to make sure they do not contain copyrighted music. The congressman says there is "no question" that the "vast majority" of peer-to-peer downloads constitute copyright infringement, but opponents of the Berman bill say it goes too far in invading the rights of individuals. Wayne State University professor and computer security expert Jessica Litman says of the proposed legislation: "What it seems to say is that if the copyright owner doesn't impair the integrity of files, it gets a complete free pass, and if it does impair the integrity of files, it gets a qualified cheap pass." Stan Lebowitz, a management professor at University of Texas-Dallas, comments: "Spoofing seems like a legitimate technique for them to use. Hacking, however, seems to go to far" — and notes that what the bill allows "would still qualify as hacking, under most laws and in most people's minds." (USA Today 25 Sep 2002)
http://www.usatoday.com/tech/news/techpolicy/2002-09-25

Category 47 *US computer-crime laws*

2003-01-08 **California law online Internet business computer security breaches notify customers e-commerce**

NIPC/DHS

January 06, Security Focus — California disclosure law has national reach.

A new California law requiring companies to notify their customers of computer security breaches applies to any online business that counts Californians as customers, even if the company isn't based in the Golden State. So warned Scott Pink, deputy chair of the American Bar Association's Cybersecurity Task Force, in a conference call Monday organized by an industry trade group, Information Technology Association of America, and attended by approximately 50 representatives of technology companies and law firms. The law, called "SB 1386," is intended to combat identity theft. It was passed last September and will take effect on July 1, 2003. To trigger the law, a breach must expose certain type of information: specifically, customers' names in association with their social security number, driver's license number, or a credit card or bank account number. After such an intrusion, the company must notify the effected customers in "the most expedient time possible and without unreasonable delay." The disclosure only needs to be made to California residents. But as a practical matter, Pink said, online businesses may find it easier to notify everyone impacted by a breach, rather than trying to cherry-pick Californians for special treatment. Companies that ignore the law face potential exposure to class action lawsuits. The law addresses a chronic problem in e-commerce - companies that are hacked are often reluctant to go public for fear of bad publicity or civil liability. But in forcing companies to come clean, the California law takes the opposite approach of the Bush administration's emerging cyber security policies, which encourage secret disclosure to government officials, rather than public warnings.

Category 47 *US computer-crime laws*

2003-01-16 **criminal hacker sentence term length federal rules**

NIPC/DHS

January 13, Security Focus — Federal government to seek public input on hacker sentencing.

Last week the presidential-appointed commission responsible for setting federal sentencing rules formally asked the public's advice on the formula used to sentence hackers and virus writers to prison or probation. The United States Sentencing Commission's (USSC) Federal Sentencing Guidelines set the range of sentences a court can choose from in a given case, based on a point system that sets a starting value for a particular crime, and then adds or subtracts points for specific aggravating or mitigating circumstances. Though they're called "guidelines," the rules are generally binding on judges. Computer crimes currently share sentencing guidelines with larceny, embezzlement and theft, where the most significant sentencing factor is the amount of financial loss inflicted. But in a congressional session that heard much talk about "cyberterrorism," lawmakers became convinced that computer outlaws were more than common thieves. Consequently, one of the provisions in the Homeland Security Act passed last November requires the USSC to review the cyber crime sentencing guidelines to ensure they take into account "the serious nature of such offenses, the growing incidence of such offenses, and the need for an effective deterrent and appropriate punishment to prevent such offenses." The USSC's "Issue for Comment" is available on the Commission's Website:
http://www.ussc.gov/. The public comment period ends on February 18th.

Category 47 *US computer-crime laws*

2003-03-26 **state law legislation S-DMCA encryption VPN e-mail proxy server firewall ISP anonymity identification tracking prosecution**

http://www.freedom-to-tinker.com/archives/000336.html

Prof. Ed Felten < http://www.cs.princeton.edu/~felten/ >of the Secure Internet Programming (SIP) Laboratory at Princeton University posted a warning on his law & technology Web site < http://www.freedom-to-tinker.com/ > about state legislation being called the "Super DMCA" or S-DMCA. These laws are so poorly written that they would make the use of firewalls, proxy servers, and VPNs illegal. The lawmakers, under pressure by the Motion Picture Association of America (MPAA), lack the technical knowledge to understand the implications of the following clauses:

SECTION 6.
(a) A person commits an offense if the person intentionally or knowingly manufactures, assembles, imports into the state, exports out of the state, distributes, advertises, sells, or leases, or offers for sale or lease:
(1) a communication device with an intent to:
(B) conceal from a communication service provider, or from any lawful authority, the existence or place of origin or destination of any communication;

It would appear that an unintended consequence of this legislation would slap criminal penalties on innocent people who set their firewalls at high security levels to preclude responses to pings or other mechanisms for identification of their IP connections. Users connecting to a corporate site via virtual private network to send e-mail could theoretically be in trouble because even the SMTP headers are encrypted on their way to the corporate e-mail server, thus precluding the ISP in the middle from identifying the nature of the traffic or its destination.

The EFFhas taken on the responsibility to keep track of this legislation. Web site is

http://www.eff.org/IP/DMCA/states/

Category 47 *US computer-crime laws*

2003-04-30 **war driving insecure network wireless Wi-Fi New Hampshire legal**

NIPC/DHS

April 29, Wired — Licensed to war drive in New Hampshire.

New Hampshire could become the first in the United States to provide legal protection for people who tap into insecure wireless networks. House Bill 495 defines an operator's failure to secure a wireless network as a form of negligence. According to the proposed amendment, "the owner of a wireless computer network shall be responsible for securing such computer network." What's more, if an alleged intruder can prove he gained access to an insecure wireless network believing it was intended to be open, the defendant may be able to get off the hook using an "affirmative defense" provision of the existing law. As a result, some legal experts contend that New Hampshire's proposed amendment to its computer laws could make it harder to throw the book at criminals who take advantage of insecure wireless systems.

Category 47 *US computer-crime laws*

2003-05-05 **anti-piracy law overly broad smart cards free satellite cable internet service MPAA Motion Picture Association of America intellectual property VPN**

NewsScan

WILL NEW ANTI-PIRACY LAWS STIFLE INNOVATION?
According to some critics, several of the newly enacted or proposed state laws to outlaw software for downloading movies without paying or unauthorized use of smart cards to get free satellite, cable or Internet service, will not only stifle innovation but might also be interpreted as outlawing such common devices as video recorders and music players. The Motion Picture Association of America (MPAA) says that some state laws are vague on piracy techniques (e.g., smart cards altered to unscramble transmissions). Robin Gross of IP Justice, a civil liberties group focused on intellectual property, says: "These laws are really talking about trying to regulate what somebody can do with the services they have already paid for." Supporters of such legislation see it differently, and insist that people "are seeing demons in these bills, where there are no demons." But critics are adamant, and say they fear the concealment provisions in new legislation could be used to ban security firewalls, encrypted virtual private networks for telecommuters and systems designed to preserve anonymity and protect privacy. (San Jose Mercury News 5 May 2003)

Category 47 *US computer-crime laws*

2003-06-30 **personal hacking data theft FBI bill law personal data**

NewsScan

BILL WOULD MANDATE NOTIFICATION OF PERSONAL DATA HACKS
Legislation introduced by Sen. Dianne Feinstein (D-Calif.) would require businesses and government agencies to notify consumers when hackers break into corporate computer systems and steal their personal data, such as social security numbers and credit card information. The stipulations of the bill are in direct conflict with efforts by the Bush administration to keep such details hidden from the public, in the hope that hacking victims will notify the FBI and other government agencies when such incidents occur. The FBI director and some top U.S. prosecutors told technology executives recently that they will increasingly work to keep the secret the names of companies that fall victim to major hacking attacks. Consumer groups praised Feinstein's proposed legislation: "It's a really important step forward," said Chris Hoofnagle, deputy counsel at the Electronic Privacy Information Center. "Individuals do not have this right to notice now." (AP/CNN.com 30 Jun 2003)

Category 47 *US computer-crime laws*

2003-10-23 **Senate Governmental Affairs Committee security P2P bill network systems personal information financial defense law enforcement public health citizens business**

NIPC/DHS

October 23, eSecurity Planet — Senate committee approves P2P security bill.

The Senate Governmental Affairs Committee approved a bill mandating federal agencies to develop and implement security plans to protect their network systems from the risks posed by peer-to-peer (P2P) file sharing on Wednesday, October 22. Earlier this month, the U.S. House of Representatives approved the same legislation. Both the House and the Senate have already implemented security measures against P2P security threats through both technical and non-technical means, including firewalls and employee training. The Government Network Security Act of 2003 would give Executive Branch agencies six months to take similar steps. The federal government uses and stores a wide variety of classified and sensitive information, including information vital to national security, defense, law enforcement, economic markets, public health, and the environment. Government computers also contain personal and financial information of U.S. citizens and businesses. Installation of P2P software on government computers can expose this sensitive information to the public. The House Committee on Government Reform issued a staff report in May showing how through a "couple of simple searches" of the most popular P2P programs, personal information such as tax returns, medical records, and confidential legal documents and business files were found.

Category 47 *US computer-crime laws*

2004-05-24 **identity theft insider theft punishments laws**

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml?articleID=20900519

May 24, InformationWeek — Feds want tougher penalties for insider identity theft.

A federal proposal to combat identity theft takes a particularly hard line on people who abuse insider access to information to commit the crime. The House Judiciary Committee earlier this month passed a bill, the Identity Theft Penalty Enhancement Act, that would establish a new crime of aggravated identity theft and increase applicable penalties. The bill also includes an amendment that directs the U.S. Sentencing Commission to revise its guidelines to include stronger punishment for those who abuse a position of trust to commit insider identity theft. According to "Predator Profiles," a forthcoming report from Michigan State University's (MSU) identity-theft research center, at least half of identity theft now results from the theft of personal information stored on business databases. Noting that her organization's research has since been corroborated by two other studies, MSU researcher Judith Collins says that at least 50%, and potentially as much as 70%, of identity thefts originate in the workplace by employees or people impersonating employees. "Our research also showed that the majority of those identities were stolen first and foremost from health-care-related institutions, and secondly from financial institutions," said Collins.

Category 47 *US computer-crime laws*

2005-05-23 **spyware malicious code House of Representatives bill**

EDUPAGE; http://news.com.com/2100-1028_3-5717658.html

HOUSE TAKES TWO STEPS AGAINST SPYWARE

The House of Representatives overwhelmingly passed two separate bills this week designed to address the growing problem of spyware. HR 29, introduced by Mary Bono (R-Calif.), would impose stiff fines on anyone found guilty of distributing computer code that results in browser hijacking, modifying bookmarks, collecting personal information without permission, and disabling security mechanisms. Violators can be fined as much as $3 million per incident. One of only four Representatives who voted against Bono's bill, Zoe Lofgren (D-Calif.) had introduced another bill, HR 744, that also prohibits installing spyware. Lofgren's bill, which passed 395 to 1, would impose fines and jail time to anyone found guilty. Both bills now go to the Senate, which failed to act on a spyware bill sent by the House last year. Senators have said they will not allow a similar situation this year. CNET, 23 May 2005

Category 47 *US computer-crime laws*

2006-01-25 **bogus spyware tool maker lawsuit Washington State Microsoft Secure Computer**

EDUPAGE; http://news.zdnet.com/2100-1009_22-6031108.html 23

LAWSUITS TARGET MAKER OF BOGUS SYPWARE TOOLS

The State of Washington and Microsoft have filed separate lawsuits against Secure Computer, a company they accuse of running a bogus antispyware racket. According to the complaints, Secure Computer used pop-up ads and other tools to tell computer users that their computers were infected with spyware and to offer a service, Spyware Cleaner, that would remove the unwanted software for $49.95. Microsoft and Washington Attorney General Rob McKenna said that the scan that supposedly revealed spyware was bogus and that the removal service in fact left computers more vulnerable to spyware. Moreover, the complaints contend that Secure Computer's messages implied that the service was in some way connected to or endorsed by Microsoft. The lawsuits allege that Secure Computer violated a recently enacted Washington Computer Spyware Act and three other laws. An attorney representing Secure Computer said the company was shocked at the legal action and would respond shortly.

Category 47 *US computer-crime laws*

2006-01-27 **legislation criminalization social engineering**

DHS IAIP Daily; 23
http://www.theregister.com/2006/01/27/schumer_phone_records/

NEW LEGISLATION WOULD CRIMINALIZE SOCIAL ENGINEERING.

New legislation proposed by Senator Chuck Schumer (D-NY) and backed by both major parties, seeks to criminalize both the practitioners and the dupes of "social engineering." Social engineering is a way of smooth-talking someone out of information they shouldn't normally impart, but it has been the most effective technique for scammers, hackers and private eyes over the years. Schumer's bill, the proposed Consumer Telephone Records Protection Act of 2006, makes disclosing a subscriber's phone records an offense. It specifically outlaws making false statements or providing phony documentation to a phone provider in order to obtain the records, and accessing an account over the Internet without the subscriber's authorization. According to the Electronic Privacy Information Center, over 40 Websites including celltolls.com and locatecell.com have been trading in a black market in call records.

Category 47 *US computer-crime laws*

2006-03-31 **Yahoo cybercrime law call legislation illegal use of technology**

DHS IAIP Daily; http://news.zdnet.co.uk/internet/security/0,39020375,39260601,00.htm 23

YAHOO CALLS FOR EFFECTIVE CYBERCRIME LAWS.

Yahoo on Thursday, March 30, called for "effective" legislation combined with industry self-regulation, to deal with online fraud, child abuse, and other cybercrime. The Internet services giant called on policy makers to concentrate on defining illegal use of technology, rather than how an action breaks the law. "The lack of global legislation adds to the complexity of the situation. It's not realistic 17 to have global legislation, but we do need international consistency," said Robin Pembrooke, director of product operations for Yahoo Europe. Pembrooke advocated a combination of legislation and self-regulation of Internet businesses in order to combat cybercrime.

Category 47 *US computer-crime laws*

2006-04-21 **New York wireless security law minimum measures**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/story/0 23
,10801,110762,00.html?SKC=security−110762

NEW YORK COUNTY ENACTS WIRELESS SECURITY LAW.

Westchester County, NY, last week enacted a new law that requires local businesses to implement "minimum security measures" for protecting their wireless networks. The law, which is believed to be the first of its kind anywhere in the country, applies to all commercial businesses that collect customer information, such as Social Security numbers, credit card or bank account information, and that also have a wireless network. Also covered by the law are businesses that offer public Internet access. The mandate was introduced as a measure to protect consumers against identity theft and other types of computer fraud, according to a statement posted on the county's Website. Businesses that collect, store and use personal information have 180 days to comply with the law.

48 Foreign cyberlaws (not cases or sentences)

Category 48 *Foreign cyberlaws (not cases or sentences)*

1997-03-28 **crypto key escrow UK**

RISKS, COMPUTING/I.T. 18 95

Ross Anderson, famed British cryptographer and civil libertarian, sounded a warning when the Department of Trade and Industry of the UK government posted proposals for imposing licensing on the use of encryption tools. The preamble included the familiar language of those prepared to restrict encryption in the name of public safety: "These proposals - aimed at facilitating the provision of secure electronic commerce - are being brought forward against a background of increasing concern, not about the technology, but about the security of information itself. In a world where more and more transactions are taking place on open electronic networks like the Internet, there has been a growing demand from industry and the public for strong encryption services to help protect the integrity and confidentiality of information. These proposals have been developed to address those concerns, but at the same time are aimed at striking a balance with the need to protect users and the requirement to safeguard law
enforcement, which encryption can prevent." Anderson summarized the key issues (with supporting quotations) as follows:
* Licensing will be mandatory;
* The scope of licensing is broad;
* Total official discretion is retained;
* Encryption keys must be escrowed, and delivered on demand to a central repository within one hour;
* Government access to private keys, even if used only for _authentication_, is proposed.

A week later, Cyber-Rights and Cyber-Liberties (UK) and 16 other civil liberties organizations world-wide issued a critical report damning the proposals.

In June, the European Electronic Messaging Association (EEMA) issued a blistering attack on the proposals.

Category 48 *Foreign cyberlaws (not cases or sentences)*

1997-04-13 **law Singapore**

EDUPAGE

"Owners of color photocopiers in Singapore must have a permit to do so, which requires submitting a list of all users, keeping the machine locked up, notifying authorities within a week if it's moved, and keeping a log detailing what is copied, when it was copied, who copied it, etc."

Category 48 *Foreign cyberlaws (not cases or sentences)*

1997-08-05 **hackers Australia firewalls crypto policy**

The Australian

At a seminar in organized by Starcom Group in Australia, several firewall experts urged governments to cooperate in promoting cryptography as a fundamental tool in firewall technology and information security in general. The experts were Paul Emerson, president and co-founder of Global Technology Associates; Dr Stephen Emerson, vice-president of Global Technology; and former deputy director-general of ASIO (Australian Security Information Organization) Gerard Walsh.

Category 48 *Foreign cyberlaws (not cases or sentences)*

1997-10-09 **crypto key recovery escrow law export**

EDUPAGE

The European Commission rejected the Clinton Administration's proposals for key recovery/escrow in encryption systems, dismissing them as not only objectionable because of threats to privacy and commerce but also as ineffective.

Category 48 *Foreign cyberlaws (not cases or sentences)*

1997-10-21 **encryption France law regulation key-recovery**

EDUPAGE

The French government proposed a mandatory key-recovery systems for all encryption used in France despite the opposition of business and of the European Commission.

Category 48 *Foreign cyberlaws (not cases or sentences)*

1998-10-13 **computer crime laws China criminal hacker cracker fraud**

RISKS 20 3

China recently announced increased policing of the Net in an attempt to reduce the growing rate of computer crime and theft. Considering this is a country where people are regularly executed for bribery and fraud, criminal hackers should take note.

Category 48 *Foreign cyberlaws (not cases or sentences)*

1998-12-22 **Wassenaar treaty encryption restrictions international**

Wired http://www.wired.com/news/print_version/politics/story/16999.html

In December, the Internet Architecture Board and the Internet Engineering Group protested the signing of the Wassenaar Arrangement <http://www.wassenaar.org/> in which 32 countries joined the U.S. in restricting the free use of strong encryption. The Wassenaar Arrangement would weaken the Internet and interfere with progress towards a more secure mechanism for TCP/IP. Signatories to the treaty would agree to enforce key-escrow or decryption back-door mechanisms in commercial encryption products to permit law-enforcement access to the cleartext of encrypted communications. Meanwhile, human rights activists protested the Wassenaar Arrangement on grounds that crypto restrictions play into the hands of totalitarian regimes.

Category 48 *Foreign cyberlaws (not cases or sentences)*

1999-01-13 **criminal hacking intrusion penetration law jurisprudence**

http://www.infobeat.com/stories/cgi/story.cgi?id=2558024618-6dd

The Supreme Court of Norway ruled in January 1999 that attempted penetration of a network or computer system is not in itself a criminal act until it succeeds. Critics argued that such a position was, in the words of Doug Mellgren writing for Associated Press, analogous "to allowing a burglar to check all the doors and windows of a house for locks and not prosecuting them until they actually break in."

Category 48 *Foreign cyberlaws (not cases or sentences)*

1999-01-19 **cryptography laws rules restrictions France government**

Crypto-gram; Slashdot http://slashdot.org/articles/99/01/19/1255234.shtml 99 02

In January, the French government relaxed its restrictions on commercial cryptography. The announcement ended the insistence on key escrow and allowed keylengths jumped to 128 bits for single-key encryption algorithms. The US reportedly tried to put pressure on the French through the Wassenaar Arrangement that tries to force strong export controls on encryption among all the signatories. As Bruce Schneier and many other critics of this policy have noted, "This only makes sense if the U.S. is the only source of strong cryptography. But it isn't — overseas security software is now just as good as work done by U.S. programmers. . . ."

Category 48 *Foreign cyberlaws (not cases or sentences)*

1999-01-20 **censorship hacktivism espionage crackdown prosecution**

Washington Post

SHANGHAI MAN GETS RELATIVELY LIGHT SENTENCE IN INTERNET CASE

A Chinese court has given a two-year jail sentence to Lin Hai, the 30-year-old owner of a computer software company in Shanghai, for selling 30,000 e-mail addresses to the Washington, D.C.-based electronic publication VIP Reference, which is critical of the Chinese government. Although the charge on which Lin Hai was judged guilty was "inciting the subversion of state sovereignty," his wife insisted that he had sold the addresses without knowing that they were being used for anti-government purposes. The sentence is part of a renewed government crackdown against dissidents, but it is significantly lighter that other recent sentences for similar offenses. (Washington Post 20 Jan 99)

Category 48 *Foreign cyberlaws (not cases or sentences)*

1999-02-15 **Japan cybercrime penetration law**

ABIX - AUSTRALASIAN BUSINESS INTELLIGENCE

In Japan, rumors surfaced in 1999 that the Diet would draft laws making it illegal for criminal hackers to penetrate computer and network perimeters without permission. Current Japanese laws did not criminalize breaches of confidentiality, only breaches of integrity or of availability.

Category 48 *Foreign cyberlaws (not cases or sentences)*

1999-03-11 **DNS domain name system WIPO law Internet**

RISKS 20 24

Prof. Michael Froomkin (U. Miami) published a blistering attack on the proposals for controlling the DNS (domain name system) put forth by the WIPO (World Intellectual Property Organization); see <http://www.law.miami.edu/~amf/quickguide.htm>. According to Froomkin, the main problems with the WIPO plan are as follows (numbering and some punctuation added):
"(1) Bias. The plan is biased in favor of trademark holders;
(2) Enabling censorship. The WIPO plan fails to protect fundamental free-speech interests including parody, and criticism of corporations;
(3) Zero Privacy. The WIPO plan provides zero privacy protections for the name, address and phone number of individual registrants;
(4) Intimidation. The WIPO plan creates an expensive loser-pays arbitration process with uncertain rules that will intimidate persons who have registered into surrendering valid registrations;
* Tilts the playing field. The WIPO plan would always allow challengers to domain names registrations to appeal to a court, but would often deny this privilege to the original registrant;
* Smorgasbord approach to law. Instead of directing arbitrators to apply applicable law, WIPO proposes using additional, different, rules it selected — rules that will often disadvantage registrants.

Category 48 *Foreign cyberlaws (not cases or sentences)*

1999-04-12 **legislation laws proposals government criminal hacking computer viruses government**

NZ Press Assoc.

Justice Minister Tony Ryall of the New Zealand government announced in April 1999 that he would be proposing changes to the Crimes Act to define four new offences that harm computer users:
* accessing a computer system for a dishonest purpose,
* attempting to access a computer system for a dishonest purpose,
* damaging or interfering with a computer system and
* unauthorised access to a computer, commonly known as hacking or cracking.

Category 48 *Foreign cyberlaws (not cases or sentences)*

1999-04-13 **Internet social policy dangers crime government culture**

THE DAILY STAR (Beirut, Lebanon)

The first pan-Arab conference on Internet security opened in Beirut in mid-April with speakers and participants from Lebanon, Saudi Arabia, Oman, Yemen, Bahrain, Jordan, Syria and Qatar. Speakers described the Internet as "an irreplaceable means of development" but also warned of the perceived perils of unfettered access to the Net. Author Alia Ibrahim, writing for the _Daily Star_ in Beirut, reported, "Saudi scientist Abdel-Rahman Abed Al-Wahed said that it was nonetheless a potentially dangerous technology that needed constant supervision."

Category 48 *Foreign cyberlaws (not cases or sentences)*

1999-04-17 **criminal hackers punishment hanging death penalty execution**

National Post (Canada)
http://www.nationalpost.com/commentary.asp?f=990407/2456715

A Montreal journalist apparently seriously proposed that criminal hackers should be hanged, just like coin clippers in Britain the 18th century or horse thieves in the USA in the 19th century. She argued that these activities all threaten the economic system in fundamental ways and that lenient treatment of the malefactors encourages copy-cat behavior. [MK comments that children and adolescents are among the criminal hackers who cause harm, but children and adolescents are notoriously poor at making rational judgements based on planning for consequences of their actions.]

Category 48 *Foreign cyberlaws (not cases or sentences)*

1999-06-10 **encryption controls restrictions worldwide international study report**

EPIC Alert http://www2.epic.org/reports/crypto1999.html 6 09

The Electronic Privacy Information Center released its second annual survey of encryption restrictions around the world. The paper was available electronically at < http://www2.epic.org/reports/crypto1999.html >. In general, few countries restricted the use, manufacture or sale of encryption products. As yet another slap in the face of encryption-restriction supporters in the US, the report pointed out that at least 167 foreign cryptographic products use strong encryption in the form of these algorithms: Triple DES, IDEA, BLOWFISH, RC5, or CAST-128. The report also identified 512 foreign companies that either manufacture or distribute foreign
cryptographic products in at least 67 countries outside the United States.

Category 48 *Foreign cyberlaws (not cases or sentences)*

1999-10-04 **pedophiles criminal hackers United Kingdom England UK police law enforcement crackdown prosecution detection**

Reuters

In October, the British government announced a far-reaching plan to fight computer crime. "In order for the Internet to thrive it must be a safe place for business and leisure and protect the freedoms of internet users," said the Home Office Minister, Charles Clarke. Police would be working with the privately-funded Internet Watch Foundation, where monitors would alert them to illegal materials on the Web such as child pornography.

Category 48 *Foreign cyberlaws (not cases or sentences)*

1999-11-22 **computer crime legislation punishment severity proposal resport government**

INFOTECH (NZ)

The New Zealand Law Commission recommended that the government define any unauthorized intrusion into a computer system or network as a computer crime. Six months before, they had hesitated and suggested that an intrusion would be a crime only if the prosecutor could prove malicious intent or actual damage. The May 1999 report said, "An intent to cause loss or harm, or an intent to gain a benefit or advantage is needed to avoid trivialising the criminal law by making every unauthorised access a criminal offence." The November version said, "We are now persuaded that that view was too narrow".

Category 48 *Foreign cyberlaws (not cases or sentences)*

2000-01-20 **criminal hacker spam spoofing laws legislation police government**

South China Morning Post

In Hong Kong, lawyers with the Department of Justice's Computer Crime Team proposed new laws with criminalization and severe penalties for cybercrime, including spamming, spoofing and unauthorized access to computer systems. Penalties ranged up to 14 years in prison.

Category 48 *Foreign cyberlaws (not cases or sentences)*

2000-01-25 **crypto registration international law regulations**

NewsScan, Wall Street Journal
http://interactive.wsj.com/articles/SB948739893578536271.htm

The Chinese government tried to get all foreign companies to register the type of encryption they were using. New rules also forbade Chinese companies from using foreign cryptographic software. Interpreted narrowly, such rules would hamper further development of Internet commerce in that country. However, NewsScan's John Gehl and Suzanne reported, "If everyone covered by China's new regulations on encryption registration had complied, about nine million Internet users would have shown up in one tiny government office to hand-deliver a form specifying what kind of encryption they used on their computers. Instead, only a handful of people showed up. Chinese officials have said there will be no extension of the deadline, but apparently have not yet decided what to do about the companies that missed it — a group that includes virtually every Chinese and foreign company doing business in China. (Reuters/New York Times 1 Feb 2000)
http://www.nytimes.com/library/tech/00/02/biztech/articles/01china-encryption.html"

48.1 Non-US cryptography laws

Category 48.1 Non-US cryptography laws

1998-06-05 **e-commerce digital certification authentication origin**

TechWeb http://www.techweb.com/wire/story/TWB19980605S0008

In June, the European Electronic Messaging Association launched an initiative this week to counter Europe's fragmented policy on digital certification. The current setup puts Europe at a disadvantage in the fast-growing e-commerce market, according to the group. The EEMA announced the European Certification Authority Forum aimed at implementing common standards for message and transaction authentication.

48.2 Non-US computer-crime laws

Category 48.2 *Non-US computer-crime laws*

1997-01-24 **phone fraud**

PA News

In Britain, the Telecommunications Fraud Bill cleared the Commons and the Lords. The law makes telecommunications fraud and the possession of equipment to perpetrate such fraud an arrestable offense, punishable by up to five years' in jail.

Category 48.2 *Non-US computer-crime laws*

2003-03-05 **hacktivism criminal hacking laws punishment Europe**

NewsScan

ONLINE VANDAL OR ONLINE ACTIVIST: NO DIFFERENCE IN EU LAWS
New laws enacted by the 15-member European Union requiring member states to make it a crime to illegally access or interfere with an information system are intended to punish vandalism and deter viruses, and those laws give no special dispensation for hackers whose motives are social or political protest rather than pure vandalism. Attorney Leon de Costa in London says that the new code "criminalizes behavior which, until now, has been seen as lawful civil disobedience." (New York Times 5 Mar 2003)

Category 48.2 *Non-US computer-crime laws*

2003-12-12 **Peer2Peer P2P Copyright Board of Canada legal Apple iPods MP3**

NewsScan

CANADA RULES P2P DOWNLOADING LEGAL
The Copyright Board of Canada has ruled that downloading copyrighted music from peer-to-peer networks is legal in that country, although uploading files is not. The decision is intended to clarify what had been a somewhat ambiguous area of Canadian law. "As far as computer hard drives are concerned, we say that for the time being, it is still legal," says Claude Majeau, secretary general of the Copyright Board. Meanwhile, the Canadian Recording Industry Association is disputing the ruling: "Our position is that under Canadian law, downloading is also prohibited. This is the opinion of the Copyright Board, but Canadian courts will decide this issue," says a lawyer for the group. The decision has also rankled the U.S. recording industry, which has been aggressively battling music downloading on its own turf. In the same ruling, the Copyright Board imposed a per-unit fee of $15 to $25 on digital music players such as Apple iPods and MP3 players but declined to extend the fee to computer hard drives. The fees are used to compensate musicians and songwriters. (CNet News.com 12 Dec 2003)

Category 48.2 *Non-US computer-crime laws*

2003-12-24 **DVD anti-copying Jon Johansen DCMA tougher copyright law enactment Europe Canada Australia Central South America**

NewsScan

COPYRIGHT ACQUITTAL COULD SPUR CHANGES IN LAW
A Norwegian court's recent acquittal of Jon Johansen on charges of writing a software tool that can be used to circumvent DVD anticopying technology may spark a wave of tougher copyright law enactment in Europe, Canada, Australia and Central and South America, where such legislation is proposed. Critics of the U.S. Digital Millennium Copyright Act (DCMA) say the DCMA's tendency to protect content owners at the expense of consumers is flawed and the Norwegian court's action should serve as the basis for further debate over the shortcomings of the U.S. law. "The acquittal is a great development. The whole notion of prohibiting acts of circumvention or circumvention devices when it's not directly tied to infringing conduct is the wrong approach. The point is, there may be lawful reasons why someone would want to circumvent a technology," says intellectual property attorney Jonathan Band. Meanwhile, Hollywood has mounted an aggressive drive to win greater global conformity in copyright law, using the precepts of the DCMA as a bargaining chip with potential trade partners. The European Union has begun implementing such legislation and U.S. negotiators are pushing for similar laws as part of the pending Free Trade Area of the Americas (FTAA) treaty, which would encompass most of North, Central and South America. Meanwhile, foot-dragging on the part of South Korea and Canada has irritated the U.S. entertainment industry: "The (WIPO) treaty was effectively negotiated a decade ago, and for a country like Korea, or Canada, to say now that they need to start examining these issues is crazy," says Neil Turkewitz, executive VP for international issues at the Recording Industry Association of America. (CNet News.com 24 Dec 2003)

Category 48.2 *Non-US computer-crime laws*

2004-03-03 **data theft prevention government guidelines Japan**

NewsScan

JAPAN MOVES ON DATA THEFT

Concerned about high-profile incidents where customer data has been stolen, the Japanese government has stepped in. Japan's Ministry of Economy, Trade and Industry has drawn up a draft set of guidelines that will require Internet service providers to secure data by appointing security managers. (Daily Yomiuri 3 Mar 2004,rec'd from John Lamp, Deakin University)

Category 48.2 *Non-US computer-crime laws*

2004-04-13 **anti-stalking laws Australia ISP concern Net-hard cyberstalking**

NewsScan

AUSTRALIAN STALKER AMENDMENTS CONCERN ISPS

Tough amendments proposed to Australian federal laws designed to slam the lid on pedophiles and Internet stalkers could leave ISPs carrying the can for "menacing, harassing or offensive" behavior by subscribers. The move -- part of Australia's Crimes Legislation Amendments (Telecommunications Offences and Other Measures) Bill -- adds the weight of criminal law to the Internet content regime, which uses a takedown system to remove offensive material. Internet lobby groups have warned the amendments could force ISPs to make decisions on removing content subject to complaints without an independent review. The amendments have not yet been introduced to Parliament. The proposal to hold ISPs liable for offensive content is a sticking point in the omnibus legislation, which also criminalizes mobile-phone cloning, making death threats online, transmitting child pornography and "grooming" or procuring children. Although the legislation indemnifies ISPs if they are not aware of offensive content, it requires them to remove content they have been made aware of. (The Australian 13 Apr 2004)

Category 48.2 *Non-US computer-crime laws*

2004-06-08 **anti-trust European Union lawsuit Microsoft appeal**

NewsScan

MICROSOFT TO APPEAL EU ANTITRUST DECISION

Microsoft has filed an appeal of the European Union's antitrust decision requiring the company to change business practices deemed detrimental to competition. Microsoft says that to follow the EU's ruling would undermine global innovation: "We believe that the interest of consumers and other European companies should be at the heart of this case. The Commission's decision undermines the innovative efforts of successful companies" -- and would "significantly alter incentives for research and development that are important to global economic growth." EU Competition Commissioner Mario Monti says he's confident that the Microsoft appeal will fail. (AP/USA Today 8 Jun 2004)

Category 48.2 *Non-US computer-crime laws*

2004-07-02 **Microsoft anti trust laws violation China Bill Gates compliance**

NewsScan

GATES UNFAZED BY POSSIBLE CHINESE ANTI-TRUST LAWS

Microsoft chief Bill Gates says he's not concerned about the possibility of China introducing anti-trust laws even as his company faces further accusations of anti-competitive behavior. "We already do business in over 50 countries that have laws like that and we are in full compliance with those laws. I don't expect any problems, nor did it come up [during meetings with Premier Wen Jiabao]." Last month the official Xinhua news agency reported that the central government was considering a draft anti-monopoly law aimed at curbing anti-competitive behavior by multinational companies after a report found firms such as Microsoft have been allegedly "abusing their advantageous positions to curb competition." In March the European Union accused the software giant of abusing its "near
monopoly" with its Windows software. (The Age 2 Jul 2004) Rec'd from John Lamp

---

Category 48.2 *Non-US computer-crime laws*

2004-08-04 **Vietnam Internet censorship police government intervention information access**

NewsScan

VIETNAM SETS UP FORCE TO POLICE NET

A special police taskforce will begin operations next month to fight cyber-crime in Vietnam. A Ministry of Public Security official said: "Firstly we will punish those who develop or intentionally transmit viruses to sabotage the computer network in Vietnam. We will also attempt to prevent
other criminal activities from being conducted over the Internet and will try to block pornographic Web sites." Only around four million people out of a population of 81 million people regularly surf the Internet in Vietnam, mainly through cyber-cafes. (The Age 4 Aug 2004) Rec'd from J Lamp

---

Category 48.2 *Non-US computer-crime laws*

2004-08-11 **new tough cyber crime law Zambia non-US network vandals jail**

NewsScan

ZAMBIAN PARLIAMENT PASSES TOUGH CYBERCRIME LAW

A tough new law enacted unanimously by Zambia's parliament would see convicted network vandals and other cybercrime offenders get jail sentences ranging from 15 to 25 years. The government said the new law would help curb cyber crimes that had become a problem in the poor southern African country where only one in a thousand people have access to computers. (The Age 11 Aug 2004) Rec'd from J. Lamp

---

Category 48.2 *Non-US computer-crime laws*

2005-10-27 **international anti-terror law France Internet activity cybercafe Internet connection data log**

DHS IAIP Daily;
http://news.yahoo.com/s/afp/20051027/tc_afp/internetqaedaatt
acks;_ylt=Am7lXspeLmQoK7GhZWLisvr6VbIF;_ylu=X3oDMTBjMHVqMTQ4
BHNlYwN5bnN1YmNhdA−−

PROPOSED ANTI-TERROR LAW IN FRANCE SEEKS TO CURTAIL TERRORIST ACTIVITY CARRIED OUT ON THE INTERNET

One provision in the proposed law extends the period for which cybercafes have to keep records of Internet connection data. One method of cyber-jihad is the "dead letter box" system, wherein someone creates an e-mail account, gives the password to several members of a group and communicates by saving messages in a draft messages folder without sending them. This type of communication often cannot be monitored because government systems for tracking e-mails work only if someone sends an e-mail. Rebecca Givner-Forbes, an intelligence analyst at the Terrorism Research Center states that those behind some Websites promoting terrorism "…often use Japanese and Chinese upload Web pages because they don't ask for an e-mail address or any information from the person uploading a file." She says the most common method used by terrorist Websites is password-protected online message boards that only members can use. According to Givner-Forbes, "Most recently they have been leveraging the net more and more to circulate terrorist tactical instructions, training manuals, explosives recipes."

Category 48.2 *Non-US computer-crime laws*

2005-12-02 **EU European anti-terror law e-mail phone call log**

DHS IAIP Daily; http://www.siliconvalley.com/mld/siliconvalley/news/editoria
l/13312628.htm

TELECOM COMPANIES REQUIRED TO SAVE LOGS OF E-MAIL, PHONE CALLS UNDER EUROPEAN UNION ANTI-TERROR PLANS

European Union (EU) justice and interior ministers agreed Friday, December 2, on plans that would require telecommunications companies to retain records of phone calls and e-mails for a minimum of six months for use in investigations of terrorism and other serious crimes. Britain's Home Secretary Charles Clarke, who chaired the meeting, said the deal among the 25 European Union nations allowed governments to decide how long telecom companies in their nations should retain the data, as long as it was between six and 24 months. "We have agreed to a system which gives flexibility to member states who want to go further," Clarke told a news conference. Clarke said terrorist groups, drug dealers and people-trafficking gangs would better be targeted under the new rules. Clarke said he was optimistic the European Parliament would adopt the bill later this month -- meaning it could come into force next year. The data-tracking plan was among 12 priority measures EU governments are pushing through in the wake of July attacks on London's transportation system.

Category 48.2 *Non-US computer-crime laws*

2005-12-14 **EU European Parliament anti-terrorism rules phone Internet logs data storage two years**

DHS IAIP Daily; http://today.reuters.com/business/newsArticle.aspx?type=telecomm&storyID=nL14475452

EUROPEAN UNION PARLIAMENT APPROVES RULES ON ANTI-TERRORISM DATA

The European Parliament on Wednesday, December 14, adopted new rules drawn up by the European Union (EU) to store phone and Internet data for up to two years to fight terrorism and other serious crime. The measure was approved in record time after being proposed by the European Commission in September, and is part of the 25-nation bloc's response to the terrorist attacks in Madrid in 2004 and in London this year. Britain, holder of the rotating EU presidency, hailed the adoption as a step forward in the fight against terrorism and organized crime. Europe's telecoms and Internet industries issued a joint statement, saying the new rules raised major concerns about technical feasibility and proportionality. "This directive will impose a significant burden on the European e-communications industry, impacting on its competitiveness," the statement said. The industry also said only 20 percent of e-mails would be covered since many service providers were based outside the bloc.

Category 48.2 *Non-US computer-crime laws*

2006-03-28 **Australia anti-spam code ISP responsibility compliance Hotmail Yahoo Web mail affected**

DHS IAIP Daily; http://www.electricnews.net/frontpage/news−9676885.html 23

AUSTRALIA TACKLES SPAM WITH NEW CODE.

Australia has cracked down on junk mail with what is believed to be the world's first industry code for tackling spam. Under the new code, Internet service providers (ISPs) will bear some of the responsibility for helping fight spam. Service providers must offer spam-filtering options to their subscribers and advise them on how to best deal with and report the nuisance mail. In addition to Australian ISPs, global e-mail operators like MSN Hotmail and Yahoo will be hit by the legislation.

Category 48.2 *Non-US computer-crime laws*

2006-04-19 **Australia antispam conviction new law world's most prolific spammer**

EDUPAGE; http://www.theregister.co.uk/2006/04/19/oz_spam_conviction/ 23

AUSTRALIA CONVICTS SPAMMER UNDER NEW LAW

Wayne Mansfield, who has been identified by Spamhaus as one of the world's most prolific spammers, has become the first person convicted under a tough antispam law enacted in Australia in April 2004. Mansfield and his company, Clarity1, were accused of sending more than 56 million unsolicited e-mails in violation of the law. In his defense, Mansfield claimed that recipients of his e-mails had agreed to receive them. He also argued that because he harvested the addresses he used in his spamming prior to the antispam law's taking effect, they were exempt from the law. The judge in the case rejected both of those arguments and found Mansfield guilty. Mansfield will be sentenced later.

48.3 Non-US intellectual property laws

Category 48.3 *Non-US intellectual property laws*

2005-05-25 **Sweden MPAA ban illegal downloading intellectual property rights violation copyright infringement**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=8606639

SWEDEN BANS DOWNLOADING COPYRIGHTED MATERIAL

Responding to pressure from entertainment industry groups, including the Motion Picture Association of America (MPAA), Sweden has made it a crime to download copyrighted material from the Internet. Previously, only uploading copyrighted works was illegal. The new law, which goes into effect July 1, allows consumers to make one copy of CDs for personal use and to copy newspapers. Those found guilty of violating the new law can be fined. The MPAA has said that governments in Scandinavian countries have been reluctant to take action against copyright piracy, though Swedish authorities did conduct a raid in March of this year in which several servers suspected of hosting copyrighted content for downloading were seized. Reuters, 25 May 2005

Category 48.3 *Non-US intellectual property laws*

2005-07-11 **intellectual property software patents European law**

RISKS; http://tinyurl.com/7zosm; http://webshop.ffii.org/ 23 94

EUROPEAN PARLIAMENT REJECTS SOFTWARE PATENT DIRECTIVE

Pete Mellor writes, "On 6 July 2005, the European Parliament decisively rejected the directive of the European Commission, which would have brought software into the patent system.

For those like me who have followed the argument about software patents over the last many years, this comes as a relief. I was first alerted to the potential damage of software patents many years ago when I heard Richard Stallman talk. He gave another set of seminars in London around two years ago. I find his arguments against software patents totally convincing."

Category 48.3 *Non-US intellectual property laws*

2006-01-25 **Microsoft license source code European Commission fine monopoly source code sharing anti-trust**

EDUPAGE; http://news.zdnet.com/2100-3513_22-6030879.html 23

MICROSOFT TO LICENSE SOURCE CODE

In an effort to avoid a stiff fine issued by the European Commission, Microsoft has agreed to license some of its source code. European antitrust regulators have found Microsoft guilty of abusing its monopoly power and have insisted on changes to the company's practices to address the violations, including offering a version of its operating system without the Microsoft Media Player and providing access to its source code to rivals so they can develop software that will properly interoperate with Windows computers. Microsoft met the first condition, but commissioners last month said that if the company continued to deny access to competitors, it would face a fine of nearly $2.5 million per day, retroactive to December 15 of last year. Microsoft is appealing the rulings against it but has said that while those appeals are pending, it will license the source code for its Windows Server System. The European Commission will review Microsoft's proposal before deciding whether to fine the company.

Category 48.3 *Non-US intellectual property laws*

2006-01-27 **British Phonographic Industry BPI illegal file sharing UK trial ruling**

EDUPAGE; http://news.bbc.co.uk/2/hi/entertainment/4653662.stm 23

BRITISH COURTS FIND IN FAVOR OF RECORDING INDUSTRY

In the first two cases of illegal file trading that went to trial in the United Kingdom, the High Court has ruled against two men, ordering them to pay damages to the British Phonographic Industry (BPI). The two defendants and three other individuals were accused of illegally sharing nearly 9,000 songs over the Internet. One defendant argued that there was no evidence against him. The court rejected that position and ordered him to make an initial payment of 5,000 pounds; his fine is expected to rise to at least 13,500 pounds. The other defendant said he did not know that what he was doing was illegal and pointed out that he sought no profit. A judge said that "Ignorance is not a defense" and ordered the man to make an initial payment of 1,500 pounds. The other three individuals have refused to settle and are awaiting trial. Officials from the BPI said the rulings were a "massive step forward" in their efforts to curb illegal file trading. Many of the other defendants in BPI lawsuits have settled out of court, but more than 50 cases remain outstanding. The BPI has given those individuals a deadline of January 31 to avoid court action.

Category 48.3 *Non-US intellectual property laws*

2006-03-16 **French legislation penalties copyright violation infringement intellectual property rights**

EDUPAGE; http://news.yahoo.com/s/afp/franceinternet 23

FRENCH OUTLINE PENALTIES FOR COPYRIGHT VIOLATIONS

Legislators in France have passed a law that criminalizes copyright violations stemming from bypassing copy protections. Some in the government had argued that making such copies should be allowed and that a tax added to the cost of CDs and DVDs could be used to compensate artists. Currently, an estimated 8 to 10 million computer users in France regularly download copyrighted songs and movies. That proposal was rejected in favor of a law that mirrors a directive issued in 2001 by the European Union. Under the new law, those found guilty of supplying software that allows users to bypass copy protections will face six months in prison and a fine of about $37,000. Those found guilty of using such software are subject to fines of between about $1,000 and $4,000.

Category 48.3 *Non-US intellectual property laws*

2006-03-21 **Creative Commons license Holland Netherlands court ruling precedent copyright intellectual property rights issues**

EDUPAGE; http://news.com.com/2100-1030_3-6052292.html 23

COURT AFFIRMS CREATIVE COMMONS LICENSE

A Dutch court has ruled that a publisher who used photographs protected by a Creative Commons license is subject to the terms of that license, marking what is likely the first case law pertaining to the Creative Commons. Former MTV VJ Adam Curry had posted photographs of his daughter on Flickr and assigned one of the Creative Commons license levels to those photos. A Dutch gossip magazine published those photos without Curry's permission, in violation of the terms of the license. The magazine argued that the licensing terms were unclear and that information about how to obtain further information about the license was not obvious. The court rejected that argument, saying the onus is on users of copyrighted content to understand the applicable license and obtain necessary permissions. According to Creative Commons Canada, the ruling sets an important precedent in that it affirms the Creative Commons licenses, which are a relatively new program for specifying usage rights, and that it holds users of protected content liable "even without expressly agreeing to, or having knowledge of, the conditions of the license."

Category 48.3 *Non-US intellectual property laws*

2006-03-22 **European Commission EC Microsoft anti-trust ruling source code sharing copyright intellectual property rights issues EU**

EDUPAGE; http://online.wsj.com/article/SB114302628720105056.html 23

MICROSOFT TO SUPPORT COMPETITORS

In its latest effort to comply with a March 2004 ruling by the European Commission (EC), Microsoft announced it would provide free, unlimited technical support to software companies developing products to work with Microsoft's server software. The 2004 antitrust ruling requires Microsoft to make its code available to rivals that want to develop products that run on Windows machines and compete with some of Microsoft's applications. Microsoft had previously offered 500 free hours of technical support and said it has also extensively updated the documentation for its products. In its latest announcement, Microsoft said the improved documentation along with unlimited support should address the EC's concerns. Jonathan Todd, spokesperson for the European Union (EU), said that the technical documentation appears to remain insufficient, noting that it should provide competitors with all the information they need and that they "should not be forced to rely on help from Microsoft staff." The EU, which is expected to issue a ruling some time in the next two weeks about Microsoft's compliance, could impose a fine of nearly $2.5 million per day, retroactive to December 15.

Category 48.3 *Non-US intellectual property laws*

2006-03-22 **French legislation music monopoly Apple iTunes music piracy increase**

EDUPAGE; http://news.com.com/2100-1028_3-6052058.html 23

FRENCH LEGISLATORS TRY TO AVERT MUSIC MONOPOLY

Lawmakers in France's National Assembly, the country's lower house, have passed a bill that would require purveyors of digital music technologies to share access to those technologies, allowing cross-operation among files and players. The most obvious target of the legislation is Apple Computer, whose iPod device and iTunes music format are linked. Under the bill, users would be able to play iTunes songs on non-Apple music players, and iPods could be used to play music files in other formats, such as those from Sony or Microsoft. Apple responded to the move by saying that if passed by France's Senate, the law will only serve to increase music piracy. A spokesperson from Apple said if the law is passed, "music sales will plummet just when legitimate alternatives to piracy are winning over customers." Others noted that the law could slow innovation because it does not offer strong protections for intellectual property. French officials countered by saying the law would in fact increase sales of online music and that they hope other countries pass similar legislation.

Category 48.3 *Non-US intellectual property laws*

2006-03-24 **Russian bill lawmakers anti-piracy intellectual property rights issues**

EDUPAGE; http://www.siliconvalley.com/mld/siliconvalley/14178447.htm 23

RUSSIAN BILL UPSETS ANTIPIRACY GROUPS

A bill being considered by Russian lawmakers has antipiracy groups up in arms, saying it would worsen the country's already terrible record of enforcing intellectual property rights. Russia's current laws include protections for rights holders, but enforcement of those laws is poor. Antipiracy groups say music and software piracy in Russia costs U.S. businesses $1.8 billion annually. The new bill would replace all existing statutes covering intellectual property. Olga Barannikova of the Coalition for Intellectual Property Rights said the bill is rife with problems and will lead to even more piracy rather than aid the country's antipiracy enforcement. "They may seem like small changes," she said, "but they will cause chaos." Barannikova faulted lawmakers for drafting the bill without consulting businesses or groups representing intellectual property rights.

Category 48.3 Non-US intellectual property laws

2006-04-12 **China rule software piracy economic development intellectual property rights**

EDUPAGE; http://news.bbc.co.uk/1/hi/technology/4902976.stm 23

CHINA ADOPTS NEW RULE TO ADDRESS SOFTWARE PIRACY

Following trade talks with the United States, Chinese authorities have issued a new guideline requiring PC manufacturers to load a licensed operating system on all computers before they leave the factory. Although an official from the State Copyright Bureau in China denied that the new regulation is in response to foreign pressure--insisting it was implemented for "the country's economic development"--China has long been seen as a haven for software pirates, with piracy rates as high as 90 percent. Under the new rule, computer makers must install legally licensed operating systems on all systems, and retailers who sell imported computers must do the same. Furthermore, computer manufacturers and vendors of operating systems must report the numbers of computers made and operating systems installed each year to the country's Ministry of Information Industry (MII). The MII also stated that software makers should provide "favorable pricing and qualified service" to computer manufacturers.

49.1 US government surveillance of citizens

Category 49.1 *US government surveillance of citizens*

1999-04-20 **airline passenger screening terrorists**

Wired

The new Federal Aviation Agency supersecret passenger profiling system will watch for patterns of ticket purchase and other travel behavior correlated with terrorism and crime. Declan McCullagh wrote in _Wired_ that terrorist profiles include "a passenger's last name, whether the ticket was purchased with cash, how long before departure it was bought, the type of traveling companions, whether a rental car is waiting, the destination of the flight and passenger, and whether the ticket is one-way or round-trip." Privacy advocates, including the ACLU, argued that the U$2.8B system proposed in 1997 would inevitably infringe on personal freedom and likely begin to use race and ethnicity as factors despite explicit exclusion from the initial algorithms.

Category 49.1 *US government surveillance of citizens*

1999-04-20 **bank secrecy reporting privacy customer data police law**

AP

Congressman Ron Paul, (R-TX) proposed repeal of the 1974 Bank Secrecy Act, which despite its name actually allows Banks to supply law enforcement agencies to access bank records related to suspicious activities in general and any transaction exceeding $10,000. Such information is invaluable to the US Customs Service and the FBI in tracking money-laundering operations that often the involve illegal drug trade. Opponents such as the ACLU argue that such laws violate the Fourth Amendment of the US Constitution banning unreasonable search and seizure.

Category 49.1 *US government surveillance of citizens*

1999-11-19 **privacy communications wiretapping law enforcement interception monitoring**

EPIC

On November 19th, EPIC and the ACLU issued a press release that began as follows:
The Electronic Privacy Information Center (EPIC) and the American Civil Liberties Union (ACLU) today asked a federal appeals court to block new rules that would enable the FBI to dictate the design of the nation's communication infrastructure.

The challenged rules would enable the Bureau to track the physical locations of cellular phone users and monitor Internet traffic. In a petition to the U.S. Court of Appeals for the District of Columbia Circuit, the groups say that the rules — contained in a Federal Communications Commission (FCC) decision issued in August — could result in a significant increase in government interception of digital communications.

The court challenge involves the Communications Assistance for Law Enforcement Act ("CALEA"), a controversial law enacted by Congress in 1994, which requires the telecommunications industry to design its systems in compliance with FBI technical requirements to facilitate electronic surveillance. In negotiations over the last few years, the FBI and industry representatives were unable to agree upon those standards, resulting in the recent FCC ruling. EPIC and the ACLU opposed the enactment of CALEA in 1994 and participated as parties in the FCC proceeding.

Category 49.1 *US government surveillance of citizens*

1999-12-06 **information warfare privacy government international spying NSA**

Newsbytes, Wired, Security Wire

The American Civil Liberties Union (ACLU) announced formation of Echelonwatch.org in cooperation with the Electronic Privacy Information Center (EPIC) and the Omega Foundation to monitor developments in the controversial Echelon spy network. According to the ACLU and others, the Echelon program is an effort to filter out potential national and international security threats from all kinds of global communications, including wire, satellite, microwave, and wireless channels. There are few details available, since the National Security Agency (NSA) refuses to discuss the project in public. It is theorized that the system analyzes voice and data to spot keywords that alert observers to possible threats. On December 3rd, EPIC filed a lawsuit against the NSA demanding access to government documents about Echelon.

Category 49.1 *US government surveillance of citizens*

2000-06-22 **privacy cookies government Web policy politics**

NewsScan, USA Today http://www.usatoday.com/life/cyber/tech/cti139.htm

The Clinton Administration's Office of National Drug Control Policy . . . [was] criticized by Republican lawmakers for using "cookies" (small programs placed surreptitiously on a Web-user's computer) to track the individual's subsequent journey through the Web. House Majority Leader Dick Armey (R., TX) said: ""The government should not be in the business of cybersnooping... It is an outrage when this vital trust is violated by the lack of concern for personal privacy." The drug office says it will stop using cookies. (AP/USA Today 22 Jun 2000)

Category 49.1 *US government surveillance of citizens*

2001-07-12 **surveillance biometric face recognition privacy public anonymity**

NewsScan

ACLU UPSET ABOUT HIGH-TECH SURVEILLANCE AT SUPER BOWL [2 Feb 2001]

The American Civil Liberties Union has written to Tampa, Florida's mayor protesting the surveillance procedures used by Tampa's police department at last week's Super Bowl football game. In attempt to identify any well-known criminals or terrorists in the stadium, the police set up hidden video cameras that took pictures of thousands of fans and transmitted the images to computers at a central command post for comparison with file photographs. In the letter, ACLU executive Howard Simon wrote: "The ACLU believes this activity raises serious concerns about the Fourth Amendment right of all citizens to be free of unreasonable searches and seizures," Simon wrote to Tampa Mayor Dick Greco. "Aside from the constitutional issues raised by the developing use of surveillance technology, we believe the public should be given an opportunity to ask -- and have answered -- the many questions raised by this practice." (USA Today 2 Feb 2001)
http://www.usatoday.com/life/cyber/tech/2001-02-02-super-bowl-surveillance.htm

CONSERVATIVE AND LIBERAL AGREEMENT: NO HIGH-TECH SURVEILLANCE [12 Jul 2001]
Dick Armey, the conservative House Majority Leader, and the left-leaning American Civil Liberties Union (ACLU) have issued a joint statement deploring the growing use by law enforcement agencies of high-tech surveillance tools to monitor ordinary people in public places. Recent news stories have revealed attempts in Tampa and Virginia Beach to use face-recognition software to identify passers-by on city streets. An Armey spokesman calls that trend disturbing, and says that "the American public doesn't want Big Brother looking over its shoulder." (Newsbytes/USA Today 12 Jul 2001)

FACE-OFF: SURVEILLANCE SYSTEMS VS. PRIVACY ADVOCATES [1 Aug 2001]
U.S. federal agencies have committed millions of dollars to the improvement of facial-identification systems that lets cameras scan faces in a crowd and automatically compare them to stored images. An example of this technology is the FaceIt system (developed by Visionics), which has been used in Israel to manage the flow of individuals entering and exiting the Gaza strip and in Tampa, Florida to taking photos of individuals walking in an entertainment district and matching the photos with digital mug shots of known criminals. The Visionics system and systems developed by its competitors have been funded by such agencies as DARPA, NSA, and the U.S. Justice Department. George Washington University law professor Jeffrey Rosen, a privacy advocate who is critical of these developments, warns: "America now faces a choice about how far we want to go down the road to being a surveillance society." (San Jose Mercury News 1 Aug 2001)
http://www.siliconvalley.com/docs/news/svfront/016044.htm

Category 49.1 *US government surveillance of citizens*

2001-12-19 **identification paper tracing audit trail stamps fibers forgery impersonation privacy anonymity**

NewsScan

'SMART' TECHNOLOGY EYED FOR POSTAL SECURITY [19 Dec 2001]

Rep. Henry Waxman (D-Calif.) has proposed a "smart" suggestion for improving the security of the U.S. Postal Service. He's pushing a two-dimensional barcode "stamp" that would contain the sender's ID as well as the date, time and place the postage was paid. Meanwhile, Maynard H. Benjamin, president of the Envelope Manufacturers Association, has suggested that the agency consider "fiber fingerprinting," which identifies correspondence by the unique characteristics possessed by each piece of paper. Privacy experts say that traceable mail would stifle whistle-blowers and government critics, and that the security measures might not be effective anyway. "You'll have the same fraudulent problems that you have with IDs and credit cards now," says Lauren Weinstein, moderator of the Privacy Forum. "The bottom line is that the bad guys are going to find a way around it. What if they steal your stamps, and you get framed for something you didn't send?" (Wired 19 Dec 2001)
http://www.wired.com/news/conflict/0,2100,49186,00.html

Category 49.1 *US government surveillance of citizens*

2002-06-03 **financial institutions banks confidential information monitoring money-laundering alert suspicious activity privacy surveillance**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A49323-2002Jun2.html

U.S.A.P.A.T.R.I.O.T. ACT TESTS PRIVACY BOUNDARIES

The post-September 11th antiterrorism legislation known as the [Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism = U.S.A.P.A.T.R.I.O.T.] Act, which enlists financial institutions in an effort to identify money-laundering and terrorist funding, has caused concern among some civil libertarians because the legislation gives law enforcement and intelligence agencies greater access to confidential information without a subpoena. And last week the Treasury Department's Financial Crimes Enforcement Network (FinCen) began operating a secure online network to make it easier for financial firms to alert the government to suspicious customer activity. FinCen director James F. Sloan says that suspicious-activity reports, complemented by the agency's data warehouses and mining tools, have identified terrorist suspects, and have led to "an opportunity to work with the industry like never before." (Washington Post 3 Jun 2002)

Category 49.1 *US government surveillance of citizens*

2003-01-16 **privacy surveillance law enforcement cameras databases libraries intimidation laws government observation homeland defense terrorism**

NewsScan

ACLU SEES A GROWING 'SURVEILLANCE MONSTER'

In a new report called "Bigger Monster, Weaker Chains," the American Civil Liberties Union says that there is a rapidly growing "American Surveillance Society" brought about by "a combination of lightning-fast technological innovations and the erosion of privacy protections" threatening "to transform Big Brother from an oft-cited but remote threat into a very real part of American life." This "surveillance monster" includes, among other things, cameras monitoring public spaces, proposals for databases filled with personal information on U.S. citizens, and anti-terrorist legislation allowing the government to demand that libraries turn over reading histories of their patrons. Yet the report asserts that these monsters don't even have to be real for them to be terrifying: "It is not just the reality of government surveillance that chills free expression and the freedom that Americans enjoy. The same negative effects come when we are constantly forced to wonder whether we might be under observation." (AP/USA Today 16 Jan 2003)

Category 49.1 *US government surveillance of citizens*

2003-01-24 **TIA Total Information Awareness monitoring surveillance law enforcement government privacy**

NewsScan

O BIG BROTHER, WHERE ART THOU? (EVERYWHERE)

In order to monitor the U.S. civilian population in its effort to detect terrorists, the government's Total Information Awareness program will rely almost completely on data collection systems that are already in place — e-mail, online shopping and travel booking, ATM systems, cell phone networks, electronic toll-collection systems and credit card payment terminals. Technologists say that what the government plans to do in data sifting and pattern matching in order to flag aberrant behavior is not very different from programs already in use by private companies. For instance, credit card companies use such systems to spot unusual spending activities that might signal a stolen card. The early version of Total Information Awareness uses a commercial software collaboration program called Groove, which was developed in 2000 by Ray Ozzie, inventor of Lotus Notes. Groove enables analysts at various government agencies to share intelligence data instantly, and links programs that are designed to detect suspicious patterns of behavior. However, some computer scientists question whether such a system can really work. "This wouldn't have been possible without the modern Internet, and even now it's a daunting task," says cryptology expert Dorothy Denning, a professor in the Department of Defense Analysis at the Naval Postgraduate School. Part of the challenge, she says, is knowing what to look for. "Do we really know enough about the precursors to terrorist activity? I don't think we're there yet." (New York Times 23 Dec 2002)

SENATE DELAYS FUNDING FOR PENTAGON SURVEILLANCE PROGRAM

The U.S. Senate voted yesterday to block funding of the Defense Department's Total Information Awareness (TIA) program, which when developed would use "data mining" techniques to scan for patterns in worldwide communications activity and use those patterns to identify terrorist threats. Calling TIA "the most far-reaching government surveillance program in history," Senator Ron Wyden (D-Ore.) said that by blocking R&D funds the Senate thereby "makes it clear that Congress wants to make sure there is no snooping on law-abiding Americans," even if the purpose of the activity is to prevent terrorist attacks against the United States. (Reuters/San Jose Mercury News 24 Jan 2003)

Category 49.1 *US government surveillance of citizens*

2003-03-31 **PATRIOT II legislation Justice Department encryption punishable**

NewsScan

U.S.A.P.A.T.R.I.O.T. - II ACT WOULD PUNISH CRIMINALS WHO ENCRYPT

Draft legislation circulating in the Justice Department would impose stiffer prison sentences for scrambling data in commission of a crime — something encryption specialists say would have little effect on fighting terrorism and will only hurt legitimate uses of cryptography. "Why should the fact that you use encryption have anything to do with how guilty you are and what the punishment should be?" asks Stanton McCandlish of the CryptoRights Foundation. "Should we have enhanced penalties because someone wore an overcoat?" The measure, which would add up to five years to a sentence for a first offense and 10 years after that, is backed by police and intelligence agents who worry that encryption will hamper their ability to fight crime. "If you went the extra step to keep us from getting evidence, you should pay an extra price," says a former computer crimes investigator with the New York Police Department. But many question whether such a law would have its intended effect: "You have to be intentional about using encryption, and that's a tricky thing to prove. I do see this provision as largely symbolic rather than effective," says a former National Security Agency counsel. The new proposal is part of legislation dubbed [U.S.A.P.A.T.R.I.O.T. II], a sequel to the 2001 [U.S.A.P.A.T.R.I.O.T.] Act. (AP 31 Mar 2003)

Category 49.1 *US government surveillance of citizens*

2003-05-20 **pentagon TIA Terrorist Information Awareness visas driver's license medical records consumer privacy government**

NewsScan

PRIVACY ADVOCATES DOUBT PENTAGON PROMISES ON SPYING

The Pentagon has changed the name of its planned anti-terrorist surveillance systems, but critics say the fundamental program remains the same and would risk violating citizens' privacy if fully implemented. Now renamed the Terrorist Information Awareness program (from Total Information Awareness), the system would broaden government surveillance activities to encompass passport applications, visas, work permits, driver's licenses, car rentals and airline ticket purchases as well as databases including vast amounts of personal information, such as financial, education, medical and housing and identification records. Sen. Ron Wyden (D-Ore.), a major opponent of the TIA, says, "What most Americans don't know is that the laws that protect consumer privacy don't apply when the data gets into government's hands. Lawfully collected information can include anything, medical records, travel, credit card and financial data." Testing of the system is already underway, raising privacy advocates' concerns about "false positives" based on erroneous data. "If TIA is relying on personal information contained in databases to determine whether someone is a suspect, what recourse does that person have whose information has been entered incorrectly?" says a spokeswoman for the Free Congress Foundation, which estimates that an error rate as small as .10% could result in more than 30,000 Americans wrongly being investigated as terrorists. (AP 20 May 2003)

Category 49.1 *US government surveillance of citizens*

2003-06-02 **Lifelog Darpa pentagon pattern life behavior habits**

NewsScan

LOOKING FOR MEANINGFUL PATTERNS IN YOUR LIFE? SEE DARPA!

The Pentagon's Defense Advanced Research Projects Agency (DARPA) is taking bids on a new project called LifeLog, which will help someone capture his or her "experience in and interactions with the world" via cameras, microphones, and sensors; the goal is to created advanced software to assist in the analysis of a person's behavior, habits, and routines. Privacy advocates are expressing concern, but DARPA spokesperson Jan Walker says that the "allegation that this technology would create a machine to spy on others and invade people's privacy is way off the mark." LifeLog's software "will be able to find meaningful patterns in the timetable, to infer the user's routines, habits and relations with other people, organizations, places and objects." (AP/USA Today 2 Jun 2003)

Category 49.1 *US government surveillance of citizens*

2003-07-14 **privacy terrorism awareness TIA pattern recognition searches**

NewsScan

PRIVACY APPLIANCES TO GUIDE TIA PATTERN-RECOGNITION SEARCHES

Data security expert Teresa Lunt, working at PARC (Palo Alto Research Center), has developed a "privacy appliance" intended to help prevent the Pentagon's Terrorism Information Awareness (TIA) project from inadvertently violating individual rights. Privacy appliances (which filter out personal identifying information) include such built-in protections as an unalterable log of what information is returned and to whom — and the software in such devices would be smart enough to adjust results based on what has previously been released and whether individuals can be identified through inference. Lunt says people have the mistaken idea that TIA would remove data sources from private hands and include them in a government database. But that's not the way it works, and in fact there's nothing new about it; the fact is, marketing companies routinely use data mining techniques to look for customer patterns that would support corporate sales programs, and under TIA those existing techniques would merely be applied to the relatively new problem of identifying and monitoring potential terrorist operations. (AP/San Jose Mercury News 14 Jul 2003)

Category 49.1 *US government surveillance of citizens*

2003-07-18 **surveillance microchip personal information Mexico**

NewsScan

IMPLANTABLE MICROCHIP STRIKES A CHORD IN MEXICO

Palm Beach, Fla.-based Applied Digital Solutions, maker of the implantable VeriChip, is targeting consumers south of the border, where people see the tiny devices as a possible new way to thwart crime. The microchips, which are available in the U.S. as well, are implanted under the skin and can be used to link to information on identity, blood type and other information housed on a central computer. In Mexico, citizens hope the tiny devices could prove one more weapon in the arsenal needed to combat a rising wave of kidnappings, robberies and other crimes. The Mexican company in charge of distribution says it hopes to implant 10,000 chips in the first year and ensure that 70% of all hospitals contain the technology necessary to read the chips. Company officials say they are working on developing a similar technology that would use satellites to locate people who've been kidnapped, an application that is popular with Mexicans, but has raised privacy concerns in the U.S. (AP 18 Jul 2003)

Category 49.1 *US government surveillance of citizens*

2003-07-23 **passports 2004 US microchip privacy surveillance**

NewsScan

SMART' PASSPORTS SET FOR 2004 DEBUT

Beginning in October 2004, the U.S. will begin issuing "smart" passports that include an embedded microchip that stores a compressed image of its owner's face. The new digital passports are intended to prevent tampering, but civil liberties groups say such technology could eventually be used to monitor the activities of citizens in unprecedented detail. However, Frank Moss, deputy assistant secretary for Passport Services at the U.S. State Department says such fears are unfounded: "They will include no information other than that on the basic passport information page." Meanwhile, European travelers may also soon be required to carry passports containing both fingerprint and iris scan biometric information, but no date has been set yet for the new passports' introduction. (New Scientist 23 Jul 2003)

Category 49.1 *US government surveillance of citizens*

2004-01-05 **webcam monitoring surviellance school**

NewsBits; http://www.usatoday.com/tech/webguide/internetlife/2004-01-05-class-webcams_x.htm

Webcams keep suspended students on track

Fredreka Schouten, writing in USA TODAY, reported on a Mississippi high school where suspended students watch teachers through Web cameras and microphones. In addition to helping students who are being punished for bad behavior avoid even more damage to their scholastic progress, the system allows classes to be archived for several weeks -- helpful for students who are ill or who want to review. Privacy advocates are concerned about possible harm from the surveillance. "Distance learning is a legitimate use of cameras in the classroom 'as long as the purpose is learning and they are not there as a pretext for another use,' says Barry Steinhardt, director of the American Civil Liberties Union's technology and liberty program. But he says he worries that cameras also could have 'a chilling effect on the speech of students.'" Schouten adds, "'They feel under constant observation,' Steinhardt says. 'And it affects the willingness of teachers to be creative or to introduce unpopular topics.'"

Category 49.1 *US government surveillance of citizens*

2004-01-05 **US immigration tracking system foreigners surveillance**

NewsScan

DIGITAL TRACKING SYSTEM FOR VISITORS

U.S. immigration authorities are now using a digital inventory control system called US-VISIT, designed to keep track of the movements of foreign visitors who enter the country with visas. US-VISIT (an acronym standing for United States Visitor and Immigrant Status Indicator Technology) requires that digital fingerprints and photos be taken of visitors as they arrive in the United States. Homeland Security undersecretary Asa Hutchinson says, "We are looking at two purposes: to increase security and to improve the integrity of immigration control. A key thing is that we will be able to know who is overstaying their visa and violating the terms of their admission to this country." (Los Angeles Times 5 Jan 2004)

Category 49.1 *US government surveillance of citizens*

2004-04-27 **public surveillance privacy Florida town background check law enforcement databases**

NewsScan

WANT ATTENTION? DRIVE THROUGH MANALAPAN, FLORIDA

Manalapan, Florida, where two out of every three homes are worth more than $500,000, will soon be running background checks on every car and driver that passes through town. Cameras will take infrared photos recording a car's tag number, and computer software will automatically run the numbers through law enforcement databases; police will also have a picture of the driver, taken with another set of cameras. A Manalapan police official says, "Courts have ruled that in a public area, you have no expectation of privacy." In any event, the official makes a point of saying that the data collected this way will be destroyed every three months. (AP/USA Today 27 Apr 2004)

Category 49.1 *US government surveillance of citizens*

2004-05-05 **handhelds federal government surveillance**

DHS IAIP Daily; http://www.fcw.com/geb/articles/2004/0503/web−derby−05−05−04 .asp

May 05, Federal Computer Week — Officials take surveillance STEPs.

At this year's Kentucky Derby, local, state and federal law enforcement and emergency management officials were keeping an eye on Churchill Downs using handheld devices, wireless connectivity, and a geospatial application that tapped into surveillance cameras. In the joint operations center, officials could access information and view maps through a geospatial application called Spatial Templates for Emergency Preparedness, or STEPs. The software collects geographic information system (GIS) data from disparate databases and makes it accessible through a Web portal. With STEPs, officials could monitor weather from their computers, access digital map data previously available only in hardcopy form and use 3-D visualization software to see the infield and stage emergency response personnel or vehicles, Langley said. Agencies involved included local police, emergency officials and homeland security personnel; Kentucky state police and the National Guard; and agents from several federal agencies such as the FBI, the Bureau of Alcohol, Firearms, Tobacco and Explosives, the U.S. Marshals Service and the Secret Service. Users as far away as Washington, DC, could also access the portal.

Category 49.1 *US government surveillance of citizens*

2004-05-24 **ID tracking passport foreign visitors**

DHS IAIP Daily; http://news.com.com/2100−7348−5219101.html

May 24, New York Times — U.S. nearing deal on way to track foreign visitors.

The Department of Homeland Security is on the verge of awarding the biggest contract in its young history for an elaborate system that could cost as much as $15 billion and employ a network of databases to track visitors to the United States long before they arrive. The program, known as US-Visit and rooted partly in a Pentagon concept developed after the terrorist attacks of 2001, seeks to supplant the nation's physical borders with what officials call virtual borders. Such borders employ networks of computer databases and biometric sensors for identification at sites abroad where people seek visas to the United States. With a virtual border in place, the actual border guard will become the last point of defense, rather than the first, because each visitor will have already been screened via a global web of databases. Visitors arriving at checkpoints, including those at the Mexican and Canadian borders, will face "real-time identification"--instantaneous authentication to confirm that they are who they say they are. American officials will, at least in theory, be able to track them inside the United States and determine if they leave the country on time.

Category 49.1 *US government surveillance of citizens*

2004-06-23 **wireless WiFi police handheld devices surveillance database anti-terrorism**

NewsScan

WIRELESS COPS AT THE AIRPORT

State troopers patrolling Boston's Logan International Airport will be using Blackberry handheld wireless devices to search the database of a company called LocatePLUS, which holds billions of online public records. The database was developed by aggregating and integrating a number of
databases to create what the company's chief executive calls a "complete dossier" on an estimated 205 million people. State Police Lt. Thomas Coffey calls the system "invaluable" and says "it really provides us with information that we probably could not obtain elsewhere without a lot of legwork." LocatePLUS has more than 15,000 customers, including more than 2,000 law enforcement agencies. (AP/USA Today 23 Jun 2004)

Category 49.1 *US government surveillance of citizens*

2004-09-09 **Chicago surveillance network cameras emergency suspicious behavior**

NewsScan

CHICAGO PLANS NEW SURVEILLANCE NETWORK

Chicago mayor Richard Daley says his city's going to install a network of more than 2,000 surveillance cameras to alert authorities to suspicious behavior or emergency situations. Daley says, "Cameras are the equivalent of hundreds of sets of eyes. They are the next best thing to having police officers stationed at every potential trouble spot." Software would be used to detect unusual activity, such as a bag being abandoned in a stairwell or movement in an off-limits area. Daley dismisses privacy concerns, on the grounds that cameras will be installed only in public places (where a police officer would have a perfect right to check what's going on). (AP/USA Today 9 Sep 2004)

Category 49.1 *US government surveillance of citizens*

2004-10-11 **government chat rooms surveillance statistical profile research grant homeland security Combat Terrorism mathematical model**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A25272-2004Oct11.html

U.S. GOVERNMENT FUNDS CHAT ROOM SURVEILLANCE

The U.S. government is funding a year-long study by a Rensselaer Polytechnic Institute computer science professor aimed at developing mathematical models to identify patterns in the chaotic traffic generated by online public forums that might reveal "hidden communities" of terrorists. RPI professor Bulent Yener will download data from selected chat rooms while tracking the times that messages were sent in order to create a statistical profile of the traffic. For instance, if QTpie and RatBoi consistently send messages within seconds of each other in a crowded chat room, it might be inferred that they are "speaking" to each other, camouflaged by the "noise" of the chat room environment. "For us, the challenge is to be able to determine, without reading the messages, who is talking to whom," says Yener. The $157,673 grant to conduct the study comes from the National Science Foundation's Approaches to Combat Terrorism program, which works in concert with U.S. intelligence agencies to make its selections. However, some scholars doubt the concept has much merit: "In a world in which you can embed your message in a pixel on a picture on a home page about tea cozies, I don't know whether if you're any better if you think chat would be any particular magnet," says Harvard Law School Internet scholar Jonathan Zittrain.

Category 49.1 US government surveillance of citizens

2005-02-14 **Real ID Act privacy homeland security privacy licenses trojan**

NewsScan; http://news.com.com/From+high-tech+drivers+licenses+to+national+ID+cards/2100-1028_3-5573414.html

'SMART' DRIVER'S LICENSES A TROJAN HORSE?

A move by Congress to endorse a Republican-backed measure that would compel states to redesign their driver's licenses by 2008 to comply with standards for making them electronically readable has critics questioning government's motives, saying it gives the Department of Homeland Security carte blanche to do nearly anything "to protect the national security interests of the United States." Rep. Ron Paul (R-Texas) says, "Supporters claim it is not a national ID because it is voluntary. However, any state that opts out will automatically make nonpersons out of its citizens. They will not be able to fly or to take a train." Proponents of the Real ID Act say it reflects the recommendations of the 9/11 Commission and will help in the battle against terrorism and efforts to identify illegal immigrants. But Paul says, "In reality, this bill is a Trojan horse. It pretends to offer desperately needed border control in order to stampede Americans into sacrificing what is uniquely American: our constitutionally protected liberty." (CNet News.com 14 Feb 2005)

Category 49.1 US government surveillance of citizens

2005-04-01 **US government DHS tracking foreign international students visas US-VISIT privacy concerns surveillance**

EDUPAGE; http://www.fcw.com/article88459-04-01-05-Web

FEDS SET TO CHOOSE METHOD FOR TRACKING EXITING STUDENTS

Officials at the Department of Homeland Security are expected to issue a decision soon about the required procedure for foreign students who are leaving the United States. The US-VISIT program, which tracks visiting scholars and is designed to prevent terrorists from entering the country on student visas, lacks a consistent process for keeping tabs on individuals who leave the country. One proposal would require individuals to visit a kiosk at the airport, where they would be fingerprinted and photographed. Under another proposal, screening officers would take fingerprints and photos at airport gates and check them against the US-VISIT database. The third proposal would combine elements of the other two. The department is conducting a study of the three options, and a report is expected in a few weeks identifying which method will provide the greatest level of security without excessively interfering with convenience or impinging on privacy. Federal Computer Week, 1 April 2005

Category 49.1 US government surveillance of citizens

2005-05-06 **unit record database Department of Education personal information disclosure security break civil liberties privacy concerns**

EDUPAGE; http://chronicle.com/prm/weekly/v51/i35/35a03701.htm

PROPOSED DATABASE WORRIES SECURITY EXPERTS

Amid a rash of corporate and institutional data breaches recently, security experts are questioning whether a "unit record" database proposed by the Department of Education could be kept secure. Currently the department collects aggregate data on college students and graduation rates. A unit record database would track individual students through their college careers, presenting what some see as an extremely tempting target for hackers. The current system would force a hacker to "compromise several databases," according to Eugene Spafford, professor of computer sciences and electrical and computer engineering at Purdue University, whereas with a database like the one proposed, "it's possible to attack it from any point in the system." Barbara Simons, former president of the Association for Computing Machinery, was also concerned about a unit record database, suggesting that it might not be the safest way to accomplish the department's goals. Grover Whitehurst, director of the Institute of Education Sciences at the Education Department, said the agency is investigating security options for the proposed database and welcomes suggestions. He noted that the system might not use Social Security numbers as identifiers and said that if the information in the system were limited in scope, it would not be very appealing to hackers. Chronicle of Higher Education, 6 May 2005 (sub. req'd)

Category 49.1 *US government surveillance of citizens*

2005-11-23 **Center Disease Control Prevention US government agency federal regulation passenger tracking proposal surveillance privacy concern**

EDUPAGE; http://govhealthit.com/article91532-11-23-05-Web

CDC PROPOSES TRACKING PASSENGERS TO PREVENT PANDEMICS

The Centers for Disease Control and Prevention (CDC) proposed federal regulations to electronically track more than 600 million U.S. airline passengers a year traveling on more than 7 million flights through 67 hub airports. The proposed regulations are posted on the CDC's Web site and will be available for a 60-day comment period in the Federal Register starting November 30. They would require airlines, travel agents, and global reservation systems to collect personal information beyond that now collected by the Transportation Security Administration or the Homeland Security Department. The same rules would apply to passengers on international cruise lines and ferries that dock at U.S. ports. The CDC said that frustrations with attempts to track the SARS outbreak prompted the proposal, which is intended to allow the CDC to respond quickly to signs of a new pandemic. Federal Computer Week, 23 November 2005

Category 49.1 *US government surveillance of citizens*

2006-01-05 **US government surveillance privacy Web-tracking technologies NSA**

EDUPAGE; http://news.com.com/2100-1028_3-6018702.html 23
http://news.com.com/2100-1028_3-6018702.html
http://news.com.com/2100-1028_3-6018702.html

GOVERNMENT KEEPING TABS WHEN IT SHOULDN'T

Despite a federal directive forbidding the use of Web-tracking technologies for federal agencies, recent reports have shown that the majority of agencies do in fact employ permanent cookies or other tools that track users. The technologies can be used to identify repeat visitors to federal Web sites and sometimes to track users' surfing on nongovernmental sites. Last week, the Associated Press found that the National Security Agency was using permanent cookies (temporary cookies are allowed), a practice it has since discontinued. Separately, reporters at CNET News.com looked at the Web sites of all agencies listed in the U.S. Government Manual and evaluated what tracking tools they were using. Results showed dozens of agencies using tools that appear to contravene the directive, including sites for the military, cabinet departments, and election commissions. When contacted about the tracking tools, officials at many agencies reportedly said they were unaware that their sites used such technologies. Peter Swire, law professor at Ohio State University, who participated in the drafting of an earlier Web-tracking policy for the Clinton administration, said, "It's evidence that privacy is not being taken seriously."

Category 49.1 *US government surveillance of citizens*

2006-01-31 **EFF lawsuit AT&T NSA cooperation wiretap cooperation**

EDUPAGE; 23
http://news.yahoo.com/s/ap/20060201/ap_on_hi_te/domestic_spying_lawsuit

EFF SUES AT&T OVER COOPERATION WITH NSA

The Electronic Frontier Foundation (EFF) has filed suit against AT&T for allegedly cooperating with the National Security Agency (NSA) in eavesdropping on individuals without a warrant. President Bush ordered the wiretaps following the terrorist attacks of 2001 and has vigorously defended them, saying the Constitution and Congressional resolutions allow them. Civil liberties groups and others reject that, saying that the wiretaps violate existing laws on surveillance. The EFF said it identified AT&T as one company involved in the activities and has filed suit "to stop this invasion of privacy, prevent it from occurring again, and make sure AT&T and all the other carriers understand there are going to be legal and economic consequences when they fail to follow the law." The EFF alleges that AT&T provided the NSA with access to its network, which carries both voice and data, and to its vast databases that store information on phone calls and Internet activity. AT&T refused to comment on the litigation.

Category 49.1 US government surveillance of citizens

2006-02-08 **legislation bill forbid unnecessary data storage**

EDUPAGE; http://news.zdnet.com/2100-9595_22-6036951.html 23

BILL WOULD FORBID UNNECESSARY STORING OF DATA

A bill introduced by Rep. Ed Markey (D-Mass.) would require operators of Web sites to delete information about the site's users unless the site had a "legitimate" need to preserve that data. Information covered by the bill includes names, addresses, phone numbers, e-mail addresses, and other data, and all Web sites would be subject to the legislation, including those operated by individuals and nonprofits. According to Markey, the Eliminate Warehousing of Consumer Internet Data Act of 2006 is intended to address two issues: identity theft and government subpoenas of Internet data from Web sites including Google and Yahoo. Markey said personal information about Internet users "should not be needlessly stored to await compromise by data thieves or fraudsters, or disclosure through judicial fishing expeditions."

[MK note: but see later developments which work towards the exact opposite of this initiative.]

Category 49.1 US government surveillance of citizens

2006-03-07 **USA PATRIOT Act national security civil liberties anti-terrorism homeland security DHS legislation**

EDUPAGE; http://www.wired.com/news/wireservice/0,70362-0.html 23

U.S.A.P.A.T.R.I.O.T. ACT GETS NEW LIFE

After a filibuster led to additional measures designed to protect civil liberties, the House and Senate have approved a renewal of the U.S.A.P.A.T.R.I.O.T. Act that President Bush is expected to sign before it expires this Friday. In all, the legislation renews 16 provisions of the bill passed in 2001 to help combat terrorism. Since its original passage, however, civil libertarians have criticized the law for sacrificing individuals' rights in the pursuit of information about terrorists. Supporters of the law argue that no evidence has been brought forth indicating that the powers of the legislation have been misused. The bill that is being sent to the president renews the federal authority to obtain usage records through National Security Letters, but the bill includes language that specifically exempts most libraries from the demands of the letters. Another change to the law allows those under investigation to formally challenge the part of the law that prevents them from revealing that they are under investigation.

Category 49.1 US government surveillance of citizens

2006-03-15 **US Department of Justice Google lawsuit search data disclosure government privacy concerns**

EDUPAGE; http://www.siliconvalley.com/mld/siliconvalley/14104319.htm 23

JUDGE GIVES GOVERNMENT SOME OF WHAT IT SOUGHT

The judge hearing the case between the U.S. Department of Justice and Google has indicated he will require the search company to supply the government with a portion of the data it was seeking. Government officials had subpoenaed one million Web addresses and a week's worth of search queries, alarming Google as well as privacy advocates that the government was exerting too much control over data that most presume to be private. During negotiations, however, the government reduced its request to just 50,000 Web addresses and 5,000 searches, a reduction that went a long way toward defusing the standoff. U.S. District Judge James Ware said that given the changed terms of the government's request, he would likely support the subpoena but would make sure individuals' rights are not compromised by data that must be turned over. Observers said that the changed terms of the subpoena mean the case is unlikely to resolve the issue of government access to search records. Orin Kerr, law professor at George Washington University, said, "It...will have very little legal consequence in the long term." Lauren Gelman, associate director of Stanford's Center for Internet and Society, said, "It's something we're going to see come up again and again."

Category 49.1 *US government surveillance of citizens*

2006-03-30 **US Department of Justice DoJ Freedom of Information Act COPA Internet search records**

EDUPAGE; 23
http://news.yahoo.com/s/ap/20060331/ap_on_hi_te/internet_blocking

JUSTICE DEPARTMENT CASTS A WIDE NET FOR INFORMATION

Subpoenas obtained through the Freedom of Information Act indicate that the U.S. Justice Department is seeking Internet usage data from at least 35 companies in its efforts to defend the 1996 Child Online Protection Act (COPA) against court challenges. One of the subpoenas sparked a legal showdown between the government and Google, which challenged the request for millions of records of Internet searches. In that case, the government significantly scaled back its request, which the judge ruled was allowable. Other companies that received similar subpoenas are Comcast, EarthLink, AT&T, Cox Communications, Verizon Communications, Symantec, and other makers of computer security products. The Supreme Court has ruled twice that COPA is likely unconstitutional, and the government will go to trial in October to defend it. David McGuire, spokesman for the Center for Democracy and Technology, expressed concerns echoed by other critics that the government is seeking large amounts of information to defend a questionable law.

Category 49.1 *US government surveillance of citizens*

2006-04-13 **library wins FBI dispute PATRIOT Act litigation national security letter First Amendment Rights civil liberties homeland security DHS**

EDUPAGE; http://www.nytimes.com/2006/04/13/nyregion/13library.html 23

LIBRARY GROUP WINS DISPUTE WITH FBI

Following a recent change in terms of the U.S.A.P.A.T.R.I.O.T. Act, federal authorities said they will end their efforts to prevent a library organization from identifying itself as a part of an antiterrorism investigation. Last year, the FBI sent a so-called national security letter to the Library Connection, an organization of 26 libraries in Connecticut, seeking patron records and e-mail messages. As it was originally enacted, the U.S.A.P.A.T.R.I.O.T. Act authorized the letters and forbade recipients from disclosing that they had been sent the letter. The group protested, saying the gag order violated their First Amendment rights, and last September a federal judge agreed. Ironically, it was during those proceedings that the government inadvertently identified the group in question as the Library Connection when attorneys for the government filed court documents with the group's name not redacted. Congress has since revised the U.S.A.P.A.T.R.I.O.T. Act, which now grants the government discretion to allow some recipients of national security letters to identify themselves. Kevin O'Connor, the United States attorney in Connecticut, said that in light of the changed legislation, the government would end its appeal of the decision to allow the Library Connection to come forward.

Category 49.1 *US government surveillance of citizens*

2006-04-14 **legislation ISP tracking data retention privacy issues homeland security DHS anti-terrorism**

EDUPAGE; http://news.zdnet.com/2100-9588_22-6061187.html 23

LEGISLATORS GET BEHIND ISP TRACKING

A number of government officials, including state and federal legislators, have endorsed the notion of requiring ISPs to keep detailed records of users' activities online. A data retention would force ISPs to collect and store some data that they currently do not capture and to keep other records far longer than they currently do. Officials including Rep. Ed Whitfield (R-Ky.), head of a Congressional subcommittee on oversight and investigations, have said that such a law would aid law enforcement. Michael Chertoff, secretary of homeland security, has also voiced support for such legislation. Critics of the idea have questioned whether storing such records would genuinely benefit law enforcement; raised concerns about who would have access to such records; and noted that it's not clear who would have to pay for such data warehouses.

Category 49.1 *US government surveillance of citizens*

2006-04-29 **privacy legislation law bill proposal Congress Internet Service Providers ISPs log file records retention browsing consumers confidentiality control**

RISKS; CNET news.com http://tinyurl.com/gb663 24 27

PROPOSAL TO FORCE DATA RETENTION BY ISPs

Rep. Diana DeGette (D-CO) has proposed legislation to force Internet Service Providers to store log files with complete records of all Internet activity by their customers until at least one year after closure of their accounts -- or indefinitely for people who continue their subscriptions. The proposed rationale for this extraordinary burden was that "America is the No. 1 global consumer of child pornography, the No. 2 producer. This is a plague we had nearly wiped out in the seventies, and sadly the Internet, an entity that we practically worship for all the great things it has brought to us, is being used to commit a crime against humanity." Declan McCullag, writing for CNET news.com, said, "For their part, Internet providers say they have a long history of helping law enforcement in child porn cases and point out that two federal laws already require them to cooperate. It's also unclear that investigations are really being hindered, according to Kate Dean, director of the U.S. Internet Service Provider Association."

Lauren Weinstein commented in RISKS,

>It was only a few months ago that people were screaming bloody murder about DoJ demanding Search Engine records -- a demand that apparently only Google had the backbone to appropriately resist, noting the sensitivity of the data involved. This controversy triggered calls (including in some legislative quarters) for a law mandating the destruction of much related data after some reasonable, relatively short interval, with appropriate designated exceptions for R&D, business development, and the like.

Now, by waving the red flag of fighting child pornography, seemingly intelligent and usually well-meaning legislators appear ready to create the mother of all big-brother database laws, a treasure trove of personal data that will ultimately be available for every fishing expedition under the sun.

For those persons who trust the government not to abuse such data, I hasten to note that these kinds of infrastructures, once in place, tend to be self-perpetuating, and will be available to *future* governments as well, including administrations who might not be as "benign" as the current one.<

In a later posting, Weinstein added,

>The irony of the situation relating to proposals for required data retention … is that many incredibly bad and dangerous concepts -- like government-mandated data retention of this sort -- will virtually always be linked to laudable ideas (like fighting child abuse) that we all agree are important goals. A cynical view would be to assume that this is done purposely to push "evil" laws using "noble" hooks. This clearly does happen sometimes.

But I believe that in the majority of these cases we're dealing with legislators and others who genuinely believe in their causes, and either don't have the will or background to recognize or understand the horrible collateral damage that their proposals would do.

Casting such persons as being purposefully evil is probably unproductive and unfair. Instead, we need to help them see the "big picture," rather than just the narrow focus of their good intentions.

For after all, the road to hell still does indeed remain paved with good intentions.<

And in RISKS 24.31, Weinstein wrote:

>If Internet users must live in fear that their actions on the Net are subject to retrospective analysis -- not only based on today's criteria but potentially on tomorrow's as well -- the effects on how we view and use the Net will be drastic, with vast unintended negative consequences that strike to the heart of our democracies.

This issue is ultimately more important than network neutrality, Internet governance, or most (if not all) of the other technically-related concerns that we bandy about here in IP or in most other forums, because it strikes to the very core of basic privacy concerns and personal freedoms.

Government-mandated Internet data retention could be the most potent single technological move in recent history toward enabling future tyranny against both individuals and groups.<

Category 49.1 *US government surveillance of citizens*

2006-05-22 **warrantless wiretapping surveillance NSA FISA Foreign Intelligence Surveillance Act TSP Terrorist Surveillance Program**

Wikipedia http://en.wikipedia.org/wiki/NSA_warrantless_surveillance_controversy

NSA WARRANTLESS SURVEILLANCE CONTROVERSY

The NSA warrantless surveillance controversy is a dispute about an eavesdropping and data mining program carried out by the National Security Agency (NSA) that the administration now refers to as the Terrorist Surveillance Program. Under the program, the NSA conducts surveillance on international and domestic phone calls, without Foreign Intelligence Surveillance Act (FISA) court authorization, which the text of FISA defines as a felony. [1] The Bush administration argues that the program is in fact legal on the grounds that FISA is an unconstitutional violation of the President's "inherent powers" and/or that FISA was implicitly overridden by other acts of Congress. Many legal scholars outside of the administration find these arguments unconvincing. In addition to the legality of the program, the controversy extends to questions of the duties of Congress, the press's role in exposing a classified program and the legality of telecommunications companies cooperating with the program.

The presidential authorization creating the Terrorist Surveillance Program is classified and only select members of the Congressional Intelligence committees and leadership were (partially) briefed. The existence of the program was not known to the American public until December 2005, when the New York Times, after learning about the program more than a year earlier, first reported on it.[2]

[Wikipedia]

References used in this introduction:
1. Article 50 United States Code, Section 1809 (In FISA, subchapter 1)
http://caselaw.lp.findlaw.com/casecode/uscodes/50/chapters/36/subchapters/i/sections/section_1809.html
2. NYT's Risen & Lichtblau's December 16, 2005 "Bush Lets U.S. Spy on Callers Without Courts". Retrieved on February 18, 2006.
http://www.commondreams.org/headlines05/1216-01.htm

49.2 Non-US government surveillance of citizens

Category 49.2 *Non-US government surveillance of citizens*

1998-02-05 **privacy surveillance dataveillance information warfare**

EDUPAGE

IS BIG BROTHER REALLY WATCHING?

A secret hearing of Canda's Immigration and Refugee Board was told the Canadian government paid $31-million during the early 1980s for state-of-the-art software to track Canadian citizens by interfacing with credit card transactions, banking data, driver's license information, pension records, taxation information, criminal records and immigration records, according to transcripts. The U.S.-made Promis system could provide details of a person's health care and even library transactions. Updated versions are reportedly still being used by the RCMP and CSIS, but neither agency could be reached for comment. (Ottawa Sun 2 Feb 98)

Category 49.2 *Non-US government surveillance of citizens*

1999-01-02 **police database personal information privacy Europe**

The Times (London)

The Europol Computer System (TECS) began operations in 1999, causing widespread alarm among privacy advocates (and, one hopes, criminals as well). The database, established to support crime-fighting by the new 15-nation police intelligence agency for the European Economic Union, stores not only information about criminals but also about suspects, victims and even potential victims. By law, the data should be available only to authorized law enforcement officers; however, a recent case in which a Belgian policeman passed data from another police database to the Mafia has caused alarm among civil rights activists.

Category 49.2 *Non-US government surveillance of citizens*

1999-01-07 **espionage privacy international surveillance communications**

Daily Telegraph, Guardian

Privacy advocates blew a gasket when Enfopol 98 was revealed — a Europe-wide system for monitoring telecommunications for police purposes. All European ISPs and telcos would be required to provide real-time, full-time access to all electronic communications regardless of where the calls originate. Even satellite-based systems such as Iridium would have to comply with these requirements. Enfopol would tie in with FBI plans as well for global electronic surveillance. After the revelation by the German Internet magazine _Telepolis_, the fate of the legislative proposals was in doubt. In early April, the Members of the European Parliament decisively rejected the proposal.

Category 49.2 *Non-US government surveillance of citizens*

1999-10-01 **survellance privacy law enforcement wiretaps guards police detection**

WEST AUSTRALIAN

The Research Director of the Australian Institute of Criminology, Peter Grabosky, gave a pessimistic view of the future in his keynote speech at the Annual Conference of the Australia and New Zealand Society of Criminology held at the University of Western Australia in September. Decreasing budgets for police, the increasing use of private security forces and public pressure to find and punish drug-dealers and other malefactors was already contributing to a climate that was more tolerant of surveillance than in the recent past.

Category 49.2 *Non-US government surveillance of citizens*

1999-12-15 **surveillance artificial intelligence pattern recognition speech keywords NSA ECHELON**

Crypto-gram 99 12

The ECHELON system was described in a report by Bruce Schneier in his Crypto-gram newsletter for December 1999 < http://www.counterpane.com/crypto-gram-9912.html >. He wrote, "I've seen estimates that ECHELON intercepts as many as 3 billion communications everyday, including phone calls, e-mail messages, Internet downloads, satellite transmissions, and so on. The system gathers all of these transmissions indiscriminately, then sorts and distills the information through artificial intelligence programs. Some sources have claimed that ECHELON sifts through 90% of the Internet's traffic. " Apparently some recent patents filed by the NSA detail algorithms for rapid recognition of keywords in phone message and Internet traffic.

Category 49.2 *Non-US government surveillance of citizens*

1999-12-21 **Echelon government spying surveillance intelligence exchange law privacy criminals**

http://www.datashopper.dk/~boo/index.html

Investigative reporters Bo Elkjaer and Kenan Seeberg of Denmark published several dozen reports in Danish about the Echelon spy network. They interviewed reclusive communications engineer Margaret Newsham in a Las Vegas suburb, where the ex-Lockheed Martin employee lives alone with an attack-dog and sleeps with a loaded pistol under her pillow — in fear, she says, of retaliation by the US intelligence services for her blowing the whistle on Echelon. Ms Newsham says that she was directly involved in the creation of the worldwide surveillance systems and was fired in 1984 for protesting the direction of the project. She told the reporters that the projects she worked on from 1974 to 1984 involved remote surveillance by the CIA and NSA of US citizens who were on US soil — a clear violation of US law.

Category 49.2 *Non-US government surveillance of citizens*

2000-02-28 **communications intelligence COMINT surveillance interception international cooperation**

Crypto-gram http://www.counterpane.com/crypto-gram-9905.html ; EU Parliament http://www.iptvreports.mcmail.com/ic2kreport.htm 99 05

The European Parliament accepted a report on the ECHELON (and other) spy networks in May 1999. See < http://www.iptvreports.mcmail.com/ic2kreport.htm > for the full report. Key findings concerning the state of the art in Comint include:
* Comprehensive systems exist to access, intercept and process every important modern form of communications, with few exceptions (section 2, technical annexe);
* Contrary to reports in the press, effective "word spotting" search systems automatically to select telephone calls of intelligence interest are not yet available, despite 30 years of research.
* However, speaker recognition systems - in effect, "voiceprints" - have been developed and are deployed to recognise the speech of targeted individuals making international telephone calls;
* Recent diplomatic initiatives by the United States government seeking European agreement to the "key escrow" system of cryptography masked intelligence collection requirements, and formed part of a long-term program which has undermined and continues to undermine the communications privacy of non-US nationals, including European governments, companies and citizens;
* There is wide-ranging evidence indicating that major governments are routinely utilising communications intelligence to provide commercial advantage to companies and trade.

Category 49.2 *Non-US government surveillance of citizens*

2002-09-05 **surveillance civil liberties homeland security Internet monitoring freedom Europe USA international**

NewsScan

BEWARE THE 'PREDATORS OF DIGITAL FREEDOMS'?

Reporters Without Borders, an international media-rights group, has accused several Western democracies of becoming "predators of digital freedoms" in their efforts to increase surveillance on the Internet as part of their fight against terrorism. "A year after the tragic events in New York and Washington, the Internet can be included on the list of 'collateral damage,'" said the group in a report. "Cyber-liberty has been undermined and fundamental digital freedoms have been amputated." The report cites recent moves to weaken individual privacy laws in the U.S., Britain, France, Germany, Spain, Italy and Denmark, as well as the European Parliament, that risk turning ISPs and telecommunications operators in those countries "into potential branches of the police." The report's findings mirror those in another report earlier this week issued by the Electronic Privacy Information Forum and Privacy International, which note that governments worldwide have made it easier for authorities to eavesdrop on telephone and online conversations in order to fight terror. (AP 5 Sep 2002)
http://apnews.excite.com/article/20020905/D7LRJR200.htm

Category 49.2 *Non-US government surveillance of citizens*

2002-10-15 **government wireless cellular phone mobile surveillance tracking identification monitoring**

NewsScan

UK GOVERNMENT PLANS CELL PHONE TOWER TRACKING SYSTEM

The government of the U.K. is funding secret radar technology research that uses mobile phone masts to enable security officials to watch vehicles and people in real time almost anywhere in Britain. The Celldar technology, which works wherever there is cell phone coverage, "sees" the shapes made when radio waves emitted by the towers meet an obstruction. Signals bounced back by immobile objects, such as buildings and trees, are filtered out by the receiver, and what's left on the screen are images of anything that moves. When combined with technology that allows individuals to be identified by their mobile phone handsets, the Celldar system would enable security officials to locate and track a specific person from hundreds of miles away. An individual using one type of receiver, a portable unit a little bigger than a laptop, could even create a "personal radar space" around his or her location for security purposes. Researchers are also working on an "X-ray vision" feature that would enable the devices to "see" through walls and look into people's homes. UK Ministry of Defence officials are hoping to introduce the system as soon as resources allow, but civil liberties advocates have been quick to complain: "It's an appalling idea. The government is just capitalizing on current public fears over security to introduce new systems that are neither desirable nor necessary," says Simon Davies, director of Privacy International. (The Observer 13 Oct 2002)
http://www.observer.co.uk/uk_news/story/0,6903,811027,0

Category 49.2 *Non-US government surveillance of citizens*

2005-02-07 **Poland spies list online data leakage confidentiality spies informers government surveillance**

NewsScan; http://australianit.news.com.au/articles/0

POLAND'S SPIES EXPOSED ONLINE

A leaked list containing the names of about 240,000 people who allegedly spied for Poland's former communist regime has overtaken sex as the hottest search item on the Net in Poland. "This thing is huge. We have recorded around 100,000 Internet searches a day for the list, which is 10 times the number looking for sex," Piotr Tchorzewski, who works at Poland's biggest Internet portal Onet, told Rzeczpospolita Daily. The list, which contains in alphabetical order the names of alleged agents and collaborators of the communist-era secret service, mixed together with the names of those who were allegedly spied on, has also been put up for auction on the Internet, but its bid price late today -- 2.99 zlotys (about $AU1.25) -- was hardly breaking records. (The Australian 7 Feb 2005)

Category 49.2 *Non-US government surveillance of citizens*

2005-02-23 **Australia pedophiles tracking e-tag surveillance**

NewsScan; http://australianit.news.com.au/articles/0

E-TAGS FOR AUSTRALIAN PEDOPHILES

Dangerous pedophiles could be electronically tagged and subjected to strict curfews after their release from jail under new laws before the Victorian parliament. Under the scheme, child sex offenders considered risks can be put under supervision orders administered by the adult parole board. The supervision conditions can include electronic bracelets allowing the offenders to be tracked, restrictions on where they live, curfews, and restrictions on movements to block their access to children. "We take the view that protecting the community, particularly vulnerable children, has to be our highest priority," Police Minister Tim Holding said. "We think these laws are an effective and appropriate way of protecting Victorians from serious child sex offenders who show a real likelihood of re-offending," he said. (The Australian 23 Feb 2005)

Category 49.2 *Non-US government surveillance of citizens*

2005-08-05 **surveillance mobile cellular phone operators civil liberties audio covert**

RISKS; http://cellphones.engadget.com/entry/1234000563053276/ 24 02

UK CELLPHONE OPERATORS CAN INSTALL SURVEILLANCE SOFTWARE ON HANDSETS

We're always a little wary of that very blurry line between protection of the general public and infringements on basic civil liberties, but it would appear that according to the Financial Times by way of the Guardian, at least one UK cellphone carrier not only has the power (and mandate) to remotely install software over the air to users' handsets that would allow for the kind of monitoring we thought only perverts and paranoiacs had access to: picking up audio from the phone's mic when the device isn't on a call. While don't think the backlash on this one has really gotten underway yet, and though we do hate to rock a cliché, we can't help but be reminded of that classic Benjamin Franklin quote, ``They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety.'' What's worse, a cellphone carrier and The Man are gonna take it from us without our permission on the sly?

[Abstract and comments from Dave Farber]

Category 49.2 *Non-US government surveillance of citizens*

2006-02-02 **wiretapping surveillance illegal government ministers espionage**

RISKS; Wikipedia 24 17
http://en.wikipedia.org/wiki/Greek_telephone_tapping_case_2004-2005

GREEK GOVERNMENT PHONES TAPPED ILLEGALLY

More than 100 mobile phone numbers belonging mostly to members of the Greek government and top-ranking civil servants were found to have been illegally tapped for a period of at least one year. The details of the case were presented at a press conference given by three government ministers on Thursday February 2, 2006. The phones tapped included those of the Prime Minister Costas Caramanlis and members of his family, the Mayor of Athens, Dora Bakoyannis, most phones of the top officers at the Ministry of Defense, the Ministry of Foreign Affairs, and the Ministry of Public Order, members of the ruling party, the Hellenic Navy General Staff, the previous Minister of Defense (at the time a member of the opposition party), one phone of the American Embassy. Moreover, the mobile phones of former National Defence Minister Giannos Papantoniou and businessmen of Arab descent were also at the foresight of the wiretapping ring, as well as of former governemnental officials from the Panhellenic Socialist Movement (PASOK).

Prime minister Costas Caramanlis has known of this surveillance since March 11, 2005, lifting concerns about his reasons of not previously revealing it. Greek medias suspected the United States of having organized the wiretaps, as an anonymous important official quoted by the AFP declared that "it is evident that the wiretaps were organized by foreign intelligence agencies, for security reasons related to the 2004 Olympic Games." Leader of the PASOK socialist opposition George Papandreou said that the Greek governement itself had pointed towards the US as responsible of the wiretaps by giving up the zone of listening range, in which the US embassy was included.

[From Wikipedia, the free encyclopedia]

Category 49.2 *Non-US government surveillance of citizens*

2006-02-09 **Yahoo China censorship aid identify prosecute political crimes journalists local law compliance**

EDUPAGE; http://www.internetnews.com/xSP/article.php/3584191 23

GROUP SAYS YAHOO AIDED CHINESE AUTHORITIES

For the second time recently, Yahoo has been accused of helping the Chinese government identify and prosecute individuals accused of political crimes. In 2005, Yahoo was criticized for providing information that helped Chinese authorities prosecute journalist Shi Tao, who was convicted of revealing state secrets. Reporters Without Borders said that another case has surfaced in which the ISP provided information to the Chinese government that led to the conviction of Li Zhi. According to the group, Li was found guilty of "inciting subversion" after he posted comments online critical of local officials and was sentenced to eight years in prison. Mary Osaka, a spokesperson from Yahoo, said that at the time the company was unaware of the nature of the investigation. In addition, she reiterated the company's position that it is better for Yahoo to have a presence in the country, "providing services we know benefit China's citizens," even if that requires compliance with local laws that run counter to U.S. beliefs and values.

4A Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1997-03-06 **infowar propaganda law**

EDUPAGE

The _Dallas Morning News_ posted news of Timothy McVeigh's supposed confession on its Web site in advance of publication in its morning edition; analysts suggest that the reason for this decision was to circumvent legal injunctions against publication by presenting a fait accompli.

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1997-03-25 **liability Web frames copyright**

RISKS; also EDUPAGE 18 94

Several publishers launched a lawsuit against TotalNews, which uses frames to point visitors to different news sources. However, the copyright owners claim that this display of their materials in the context of TotalNews own Web page violates their ownership rights. The problem seems to be exacerbated by the banner advertisements that TotalNews places on its Web page, thus benefiting from revenue while using other people's property without recompense.

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1997-03-27 **e-commerce gambling**

EDUPAGE

An Arizona representative introduced the Internet Gambling Prohibition Act of 1997, which would make all transmission of gambling information through the Net illegal . ISPs would have to cut off service to violators only upon receipt of a legally-valid notice.

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1997-03-28 **elections censorship law Canada**

RISKS 18 95

Elections Canada proposed to ban posting of opinion-polls on the Internet within 48 hours before a federal election. No bureaucrat ventured a public guess as to how such a ban would be enforced.

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1997-04-14 **Web passwords**

RISKS 19 7

Bob Frankston reported that the new public Web-browsing kiosks being installed by a USWest affiliate store the passwords visitors use when accessing closed Web sites. Presumably clicking "back" on the browser allows any subsequent user to branch back to the secured pages. Frankston reminds users to uncheck the "save password" box before leaving the kiosk.

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1997-04-29 **Web law copyright intellectual property trademark**

EDUPAGE

In a startling case of anhistorical cluelessness about the history and even the definition of the World Wide Web, Ticketmaster Group sued Microsoft for including a hot link from Microsoft Web pages to Ticketmaster Web pages without a formal agreement granting permission for such links. The problem apparently stemmed from Ticketmaster's perceptions that Microsoft was deriving benefit from the linkage but bypassing Ticketmaster's advertising. A few weeks later, Ticketmaster programmed its Web pages to lead all Sidewalk users trying to follow unauthorized links to a dead end, where they were confronted with the statement, "This is an unauthorized link and a dead end for Sidewalk. Ticketmaster does not have a business relationship with Sidewalk and you do not need them to visit us. They want to traffic on our good name and your desire for information on live entertainment events to sell advertising for their sole benefit while offering nothing in return."

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1997-05-25 **cookies Web**

EDUPAGE, AP

The IETF proposed to change browser defaults to control the ability of Web sites to store information in users' <cookies.txt> files. Not surprisingly, the online marketing industry, in the form of the Association of Online Professionals and the Internet Advertising Bureau, vigorously opposes such a change in the default. Netscape, Firefly Network Inc. and VeriSign Inc proposed the Open Profiling Standard and were supported by 60 other companies, not including Microsoft. Two weeks later, Microsoft dropped its opposition and agreed to join Netscape and the others in supporting this proposal.

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1997-05-27 **censorship law election Canada**

Wired via PointCast

Electronic Frontier Canada protested a ruling by Elections Canada that forced Ottawa environmental activist Krishna Bera to take down his Web page, "Vote Green." Elections Canada warned that he faced a fine of about U$750 or a year in jail for posting advertising during an election campaign without identifying the sponsor. Defenders of anonymity argued that the public interest is best served by allowing individuals to express possibly unpopular positions without suffering discrimination or persecution; defenders of the law argued that the public interest is best served by ensuring that voters know who is trying to influence their vote. The EFC said it would challenge the ruling in court.

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1997-06-03 **privacy electronic commerce Web**

AP, PR

Microsoft proposed its own alternative to the Open Profiling Standard offered by Netscape and five dozen other companies to protect the privacy of browsers on the World Wide Web. The World Wide Web Consortium's Platform for Privacy Preferences, or P3, backed by Microsoft and by the Center for Democracy and Technology, is an extension of the existing standard for communicating meta-data between Web site and Web browser. P3 would extend the Platform for Internet Content Selection (PICS) to include limitations on what kind of information about the user could be stored by a Web site or passed on to others. A third alternative for protecting privacy is eTrust certification, supported by the Electronic Frontier Foundation; it would certify what kind of privacy safeguards a given site implements and would periodically audit compliance with the stated standards. The term "eTrust" was soon changed to "TRUSTe." See <http://www.truste.org/> for details.

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1997-06-12 **privacy standards Web**

EDUPAGE

In a startling outbreak of common sense, Microsoft announced that it would support industry-wide privacy standards instead of inventing its own and ramming them down the market's throat. The Platform for Privacy Preferences are sponsored by the World Wide Web Consortium and supported by (gasp!) Netscape and many other companies; they would help Web browsers restrict the types of personal information to be captured about users without permission. In a charming bit of self-satire, a Microsoft executive was quoted as saying, "This is unprecedented, but we realized that we need to work together for the common good." Observers are now on the lookout for flying pigs.

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1997-06-12 **censorship Web link law**

RISKS 19 22

In a curious case of extra-territoriality, a British court in Nottinghamshire warned a Canadian in British Columbia that he would be sued in _British_ court if he refused to take down (1) an article called the JET Report (dealing with accusations of satanic child abuse in Nottinghamshire) from his Web site; and (2) remove all links from his Canadian site to mirror sites where the JET Report might be found. The English barrister who wrote to Jeremy Freeman said that he was infringing on their copyright of the Report — and so were links to other sites with unauthorized copies of that report. See <http://www.jeremy.bc.ca/jetrep.htm> for details.

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1997-06-15 **Web language law Canada**

EDUPAGE

In another piece of anti-English government persecution, the Office de la Langue Française (known as the Language Police) of the Province of Québec ordered a computer store to change its Web page to respect laws demanding either unilingual French commercial texts or (in public places) assurance that English shall be no more than half the size of the French lettering on the sign. The store, Micro-Bytes Logiciels of Pointe Claire took its Web site off-line, inconveniencing both anglophone and francophone customers. A week later, the rabidly anti-English Culture and Communications Minister, Louise Beaudoin, declared that the Province would exert control over Web sites in order to protect the French language despite formal federal jurisdiction over telecommunications — constitutional change by fiat.

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1997-06-17 **Web standards P3**

PR Newswire

Jesse Berst, ZDNet AnchorDesk editorial director, launched an e-petition demanding that Microsoft and Netscape agree on a single standard for HTML on the World Wide Web. The text of the Web Interoperability Pledge (WIP), supported by the World Wide Web Consortium (W3C) reads as follows:
Web Vendors: "I pledge to support recommended HTML tags as defined by W3C, and submit all extensions to HTML to W3C before shipping them."
Web Publishers: "I pledge to use only recommended HTML tags as defined by W3C."

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1997-07-03 **Web law copyright intellectual property trademark**

EDUPAGE

Intellectual property attorneys and civil liberties lawyers were puzzling over the implications of legal actions to prevent reference to Web sites — that is, to forbid the unauthorized use of what makes the World Wide Web the World Wide Web. In federal court in Georgia, a judge ruled that the state law forbidding unauthorized linkage to a Web site was open to challenge on First Amendment grounds.

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1997-07-16 **hacking course law enforcement police training**

Providence Journal-Bulletin

Law enforcement officials in the Master's degree in Administration of Justice at Salve Regina University in Providence, RI can take a Hacking-101 course called "Culture, Computers and the Law." Instructor Nicholas Lund-Molfese hopes the officers will be able to apply their new knowledge of the hacking subculture and techniques to preventing crime and catching cyber-criminals.

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1997-07-17 **privacy Web**

EDUPAGE

According to EDUPAGE editors, "The Federal Trade Commission has announced that the managers of Web sites that collect personal information about children must obtain parental consent before releasing it to third parties. Although the FTC does not regulate advertising for children over the Net, it does have general jurisdiction over any deceptive market practices."

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1997-07-24 **Internet state law interstate commerce**

UPI

Missouri Attorney General Jay Nixon accused Hog's Head Beer Cellars of North Carolina of selling beer to an 18-year old without requesting her age before accepting a credit-card number for the sale. Delivery on July 15 took place without a request for proof of age. The suit seeks a court order preventing Hog's Head from marketing and selling alcohol without a Missouri license and engaging in the sale of alcohol to minors or failing to verify the age of a customer.

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1997-09-11 **Web law copyright links**

EDUPAGE

Tim Berners-Lee, one of the founders of the World Wide Web, criticized Ticketmaster for suing Microsoft over "unauthorized" hot links to their Web site. He said that pointing at someone's public Web site was analogous to discussing a topic without asking for anyone's permission to do so.

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1997-10-01 **ISP libel law**

UPI

In San Franscisco at the start of October, Superior Court Judge David Garcia ruled against Michael and Lilith Aquino, founders of a temple allegedly devoted to worshipping Satan. Apparently a pseudonymous person or persons called "Curio" had accused the couple of various Bad Things and they sued "Curio's" ISP, ElectriCiti. The judge stated that federal law protects ISPs against lawsuits for the behavior of users of their services.

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1997-11-03 **cyberspace law Internet publication date**

AP

On March 21, 1996 the Web site for _Business Week_ posted an article entitled, "The Fall of the Wizard of Wall Street." The next day, the magazine published the article in its paper edition. On March 24, 1997, Julian H. Robertston Jr sued the publishers for $1B in damages for libel. The date his suit was filed was a year and a day after the online publication date (excluding a weekend in the way). New York's libel law has a 1 year statute of limitation, so the lawyers for _Business Week_ asked the trial judge to dismiss the suit, claiming that its online posting constituted publication. The plaintiffs argue that the clock was reset by the paper publication.

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1997-11-27 **Copyright Web**

RISKS 18 78 ff

The Shetland Times case continued in 1997, when a British judge ruled in favor of an interim interdiction of the use of direct linkages to the Times' Web page by its competitor, The Shetland News. Lord Hamilton of the Outer House of the Court of Session, agreed that, at least until the case comes to full trial, the fact that users of the News Web site could branch directly to the Times' stories without passing through the Times' home page — and therefore missing Times advertising — constituted prima facie evidence of damage to the plaintiff. Some observers interpreted the interim ruling as applying purely to the use of the headlines, as copyrighted materials, without permission; these observers argue that the judgment does not, in fact, bear on whether the hot links point to the original Times articles or to something else. In November, the feuding editors agreed to an out-of-court settlement. They agreed that the News is entitled to link directly to stories in the Times by means of headlines, provided that each link to any individual story carry the legend, "a Shetland Times story" beneath the headline. Additionally, the agreement requires the News to insert, adjacent to each Times headline, a "button" or icon showing the Shetland Times logo. The button and the legend would be linked to the home page of the Shetland Times. The headlines would be linked directly to a Times article. However, the News editor pouted that he wouldn't link to the Times site at all under those circumstances: Nyah!

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1998-03-13 **pornography spelling URL Net Web law domain name DNS**

RISKS 19 63

Pornographers seem to be on the ball, as it were: they consistently register domain names similar to those of popular sites. For example, writes RISKS correspondent James Willing, leaving out a hyphen in a movie site often leads one to a pornographic site. As late as June 1998, you could misspell <http://www.microsoft.com> by leaving out the r and you would go to a porn site; however, this "micosoft.com" site disappeared sometime in the latter half of 1998.

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1998-03-22 **libel Web criticism ACLU student home page school controls**

EDUPAGE

In Cleveland, a high school student posted insulting remarks about one of his teachers on the student's personal Web page. He was suspended. The ACLU protested on his behalf and in March, a federal judge temporarily reinstated the student pending the court case. The ACLU argued that school has no right to control communications by its students away from school grounds. A similar case started in Miami in May, where the administration objected to his characterization of his own school as ""one of the worst schools within a 10-state radius" and "the melting pot of the world's most disgusting people — from the cafeteria to the principal."

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1998-04-22 **international jurisdiction Internet Web liability law tort**

RISKS 19 69

Recent law-school graduate and experienced programmer Rob Bailey pointed out in RISKS that the way international law is evolving, governments may try to exercise "personal jurisdiction" allowing them to subpoena citizens and residents of other countries for violations of local law due to Web content. Examples include the French position on requirements to make French-language materials to French residents and the Saudi Arabian attitude towards images of women showing anything but clothing, face and hands. For an article by jurist Christopher Meyer exploring the possible consequences of personal jurisdiction, see <http://www.wlu.edu/~lawrev/text/543/Meyer.htm>.

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1998-04-23 **liability ISP common carrier libel publishing Internet**

EDUPAGE

In 1997, White House advisor Sidney Blumenthal was libelled by Matt Drudge and included AOL in his lawsuit. In a ruling in April, U.S. District Judge Paul L.Friedman exculpated the ISP, saying that such services should not be held to the same standard as newspapers, magazines, TV networks or radio stations. This ruling supports the view that ISPs should be treated in law as common carriers, not responsible for content transmitted by their users.

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1998-05-10 **Web law language rights restrictions France advertising**

EDUPAGE

A year and a half after valiant protectors of the French language dragged Georgia Institute of Technology into French courts to protest the use of all-English advertising materials for an all-English university campus located in France, the court decided that it wasn't a violation of French law after all. In any case, Georgia Tech, recognizing the value of multilingual marketing, had already provided Web pages in French and German as well as English.

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1998-06-23 **liability ISP subscriber user common carrier**

EDUPAGE

EDUPAGE authors wrote, "The Supreme Court has let stand a lower court ruling that frees Internet service providers such as America Online from legal liability for information one subscriber circulates to millions of others. The appeals court said that federal law `plainly immunizes computer service providers like AOL from liability for information that originates with third parties.' The case is Zeran vs. America Online, 97-1488. (San Jose Mercury News 22 Jun 98)" In October, a Florida appeals court rejected the culpability of AOL in a case where a convicted sex maniac tried to sell the plaintiff's eleven-year-old son a porn video via an AOL chat room. The plaintiff described AOL as "a home shopping network for pedophiles and child pornographers." That case moved on to the Supreme Court.

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1998-09-27 **link URL Web liability civil law**

EDUPAGE

Hollywood photographer Gary Bernstein sued several Web operators for having links — even indirect links — to a site that contained pirated copies of his works. In other words, his lawyers argued that the contamination spread along Web links: from the bad site to all those that linked to it and then to all the sites that linked to the sites that linked to the copyright infringer. By this reasoning presumably every owner of a Web site on the planet should be liable. Luckily, Los Angeles Federal District Court Judge Manuel A. Real dismissed the indirect linkage and Bernstein withdrew his entire suit pending further planning.

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1999-02-11 **information warfare competition advertisements Web sites intellectual property copyright**

Reuters

In a striking example of information warfare, the Alexa Internet company offers competitors the opportunity to superpose their own ads on top of their competition's Web pages. Subscribers to the Alexa service get "smart links" which provide pop-up information such as a Web site's company address and financial information. In addition, the service allows advertisements to be tailored to a specific target; for example, ads can appear when the user clicks on a competitor's Web site.

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1999-04-19 **law regulation Web site universal readability access**

Freedom Forum
http://www.freedomforum.org/technology/1999/4/30handicapaccess.asp

According to the US Access Board, established to enforce the Disabilities Act of 1990 and other equal-opportunity legislation, all federal government Web sites will have to provide for accessibility to visually-impaired users in compliance with Section 508 of the 1998 Workforce Investment Act. The deadline for government sites was the end of May 1999; by 7 Aug 2000 the requirements will extend to suppliers with federal contracts. According to some members of the federal Electronic and Information Technology Access Advisory Committee, the same rules will eventually apply to all Web sites hosted in the USA. Requirements stipulate that "in addition to conventional html and PDF versions available online, all online information must also be available from the agency via audio text and TTY, as well as through cassette tape, Braille, large print, or computer disk."

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1999-04-28 **e-mail spam mail-bombing civil lawsuit injunction**

AP, Los Angeles Times http://www.latimes.com/home/business/t000038417.html

In 1995, Intel employee Ken Hamidi was fired; he responded by flooding Intel with critical e-mail to 30,000 of his former colleagues at Intel. The company obtained an injunction in April 1999 to stop Hamidi from sending his message to corporate e-mail accounts. Free-speech advocates were shocked at the judge's decision that the company's e-mail system, even though connected to the Internet, was not a public forum and that Hamidi's unauthorized use of the addresses constituted illegal trespass.

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1999-05-11 **e-commerce law legislation regulation Europe international**

E-Commerce Times

The European Commission approved several measures affecting e-commerce: (1) jurisdiction over electronic transactions would reside in the country of the seller; (2) consumers would have a single European opt-out registry to escape spam; (3) ISP liability for copyright violations and libel would increase; (4) ISP liability for third-party storage and transmission of illegal content would be reduced.

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1999-05-13 **Internet Web advertising regulation enforcement policing FTC**

E-Commerce Times

A predictable burst of protest met the modest proposals from the FTC to monitor online advertising to cut down on fraud. Large ISPs such as AOL and the ITAA (Information Technology Association of America) claimed that the move was too regulatory.

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1999-05-17 **Web online publishing annotation comments free speech**

Wall Street Journal

An interesting wrinkle in the on-going fights over second-hand representation of Web-site content erupted when Third Voice announced a new service allowing participants to post and see the electronic equivalent of "Post-It" notes on any Web site — without the involvement or approval of the Web-site owners. The notes look like part of the original site to the uninformed.

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1999-06-09 **jurisdiction Internet Web servers state location physical presence lawsuit**

C|NET

The three judges of the California Court of Appeal for the Second District ruled that the mere physical presence of servers hosting a Web site does not constitute grounds for defining jurisdiction. The case was Rambam vs the Jewish Defense Organization; plaintiff argued that because the JDO used California-based GeoCities and Xoom.com servers to host their Web site, therefore he should be able to sue defendant in California.

Category 4A *Evolution of Net law: framing, pointing, linking, jurisdiction, neutrality*

1999-06-14 **privacy defamation anonymity Internet Web law tort lawsuits**

LA Times

Companies being attacked by anonymous critics online began suing "John Doe" defendants and demanding that the courts force disclosure of the identity of their gadflies. Xircom attacked someone called "A View From Within" for his or her criticism of the company. In the first six months of 1999, AOL alone was served with 110 warrants for disclosure of users' actual identities.

4A2 Pointing, linking, deep linking, metatext

Category 4A2 *Pointing, linking, deep linking, metatext*

2000-03-09 **trademark lawsuit Web banner advertisements focus profile**

NewsScan

Cosmetics giant Estee Lauder has won a lawsuit filed in Germany against Excite Inc. and New York-based iBeauty, with a Hamburg District Court agreeing that Excite's sale to iBeauty of certain Estee Lauder trademarks, such as Estee Lauder, Clinique and Origins, amounted to unfair competition under German law. The trademarks were used by the companies to trigger banner ads for [other] beauty products on Web sites. Similar lawsuits have been filed by Estee Lauder in federal court in New York and in France. A Jupiter Communications analyst says the case "has major implications for many sites across the Web," because keyword-based ads generate hundreds of millions of dollars in revenue. He calls the German decision "at least a first precedent out there in cyberspace related to this type of conflict." (Wall Street Journal 9 Mar 2000)

Category 4A2 *Pointing, linking, deep linking, metatext*

2000-03-29 **Web linking pointing legality lawsuit judgement**

NewsScan, Los Angeles Times
http://www.latimes.com/business/20000329/t000029415.html

A federal judge has ruled that it is not illegal for an online company to provide a link on its Web site to that of a competitor. The ruling came in response to a lawsuit filed by Ticketmaster Online-CitySearch against Tickets.com. In dismissing four counts of Ticketmaster's lawsuit, the judge said that "deep linking by itself... does not necessarily involve unfair competition," as long as it is clear whose site a customer is on when they click through. Ticketmaster says it will file an amended complaint and attempt to reinstate the dismissed charges. "If we spend substantial money to build up a site why should they be able to take that and build their business on the backs of our hard work?" says Ticketmaster attorney Robert Platt. Tickets.com attorney Daniel Harris replies, "They have an open site and are a member of the free Internet community. They have to live by the rules of that community as it has grown up." (Los Angeles Times 29 Mar 2000)

Category 4A2 *Pointing, linking, deep linking, metatext*

2000-04-10 **linking legal judgement lawsuit**

POLITECH

In Osaka, Japan, a court ruled against the creator of the FLMASK utility software that allows users to remove the anti-porn digital masks from films. The judge also ruled that all sites linking to the offending URL were in violation of the law.

Category 4A2 *Pointing, linking, deep linking, metatext*

2000-05-09 **free speech linking legislation proposal**

Wired http://www.wired.com/news/politics/0,1283,36209,00.html

The Methamphetamine Anti-Proliferation Act proposed in Congress would have made it a federal crime to link to any information about illegal drugs or to advertising for illegal drugs. The proposal suffered widespread condemnation for violation of US First Amendment guarantees and vagueness.

Category 4A2 *Pointing, linking, deep linking, metatext*

2000-05-13 **linking free speech lawsuit**

POLITECH

Microsoft sent demands to Slashdot insisting that it not only remove objectionable articles but also links to specific sites containing copies of material claimed to be in violation of Microsoft's copyrights.

Category 4A2 *Pointing, linking, deep linking, metatext*

2000-06-06 **Web pointing lawsuit principle fundamental**

NewsScan

MP3Board Inc. . . . [sued] the Recording Industry Association of America in an effort to avoid having its mp3board.com Web site, which includes a search engine and hyperlinks to other sites, shut down. Since October the RIAA has been writing cease-and-desist letters to MP3Board, claiming "that mere hyperlinks to other works on other sites was a copyright infringement." MP3Board's suit "seeks to declare that hypertext linking, created by automated processes, from one site on the World Wide Web to another does not constitute copyright infringement even if the destination of the hypertext link is to a Web site containing material that infringes upon intellectual property rights." A review of the mp3board.com site by the RIAA found at least 662 links that it believes are infringing on the copyrights of the five major record labels it represents. (Hollywood Reporter 6 Jun 2000)

Category 4A2 *Pointing, linking, deep linking, metatext*

2001-01-12 **trespass linking bots spiders Web lawsuit jurisprudence precedent**

NewsScan

WHAT DOES "TRESPASS" MEAN IN CYBERSPACE?
Recent court cases have used the ancient law of "trespass" to rule against companies that used software robots to search the public Web sites of other companies to capture sales leads for mass marketing purposes. However, the original idea of trespass is that trespasser causes some kind of harm (such as crashing the site being trespassed upon). But what if there is no harm - crash or traffic gridlock or anything else? The recent decisions do not seem to require that a plaintiff allege real harm, and some legal observers are concerned that the decisions will have bad unintended consequences. Dan L. Burk, a University of Minnesota law professor, warns: "If I don't like your linking to my site, or searching my site, even though it is open to the public, and I say, 'Stop,' you have to stop... whether you are actually hurting me or not." (New York Times 12 Jan 2001)
http://partners.nytimes.com/2001/01/12/technology/12CYBERLAW.html

---

Category 4A2 *Pointing, linking, deep linking, metatext*

2001-01-18 **linking URL advertising intellectual property law jurisprudence**

NewsScan

'DEEP LINKING' COMES UNDER FIRE
StepStone, a UK online recruitment company, has obtained an injunction in Germany preventing Danish rival OFiR -- a media firm that owns online recruitment portals in the UK, Germany, Denmark and France -- from linking to StepStone Web pages. The move is one of the few cases to test the law on "deep linking" -- links between sites that bypass home pages and therefore miss the advertising on them. "It is not, of course, every case of hypertext linking which is unlawful -- the Internet would grind to a halt," said Adrian Lifely, an attorney for Osborne Clark, the law firm advising StepStone. "But the courts in Europe do have power to intervene where linking is extensive and prejudicial to the site involved." The law firm said OFiR was using the link to StepStone's database to boost the number of job offerings it claimed to provide. The ruling in favor of the injunction was based on new European laws regulations on database and copyright protection, said Lifely. (Financial Times 18 Jan 2001)
http://news.ft.com/news/industries/internet&e-commerce

Category 4A2 *Pointing, linking, deep linking, metatext*

2001-06-29 **copyright intellectual property Web search engines metatext**

NewsScan

LAWSUIT OVER INVISIBLE REPRODUCTION OF COPYRIGHTED MATERIAL [29 Jun 2001]
The Belgian company Euregio.net is suing the astrology site EasyScopes owned by Women.com (recently acquired by iVillage) for copyright infringement, even though the disputed material was not placed on the EasyScopes to be read (it was in white letters on a white background, and therefore essentially undecipherable). Euregio says the misappropriated material was used by EasyScopes to trick Internet search engines and "try to get the people who would normally be interested in the information on our site, to try to get them on their site." (New York Times 29 Jun 2001)
http://partners.nytimes.com/2001/06/29/technology/29CYBERLAW.html

---

Category 4A2 *Pointing, linking, deep linking, metatext*

2002-05-14 **deep linking copyright intellectual property Web courtesy etiquette consideration politeness**

PoliTech

An increasing number of firms have been suing Web site owners for daring to post the URLs of material in the originating Web sites that allow advertisement-laden pages to be bypassed. Known as deep-linking, this practice is seen by many ad-supported sites as a form of appropriation of content. Robin Miller, Editor in Chief of OSDN (Linux.com, Newsforge.com, freshmeat.net, Slashdot.org, DaveCentral.com, and other popular tech Web sites), pointed out on PoliTech that it should be a matter of simple courtesy to respect the owners' preferences by avoiding deep linking.

[MK comment: Be particularly careful not to circumvent Web publisher's wishes when they require registration to access materials such as White Papers. It's usually trivially easy to obtain the actual URL of the paper, but it would be discourteous to the people who are offering the material to distribute that URL, thus allowing their registration to be bypassed.]

Category 4A2 *Pointing, linking, deep linking, metatext*

2002-06-10 **deep linking copyright intellectual property lawsuit Web**

NewsScan

DANISH PUBLISHERS PROTEST DEEP LINKING
The Danish Newspaper Publishers' Association is suing a news Web site that provides links directly to news stories, without going through the site's home page. Newsbooster editor-in-chief Nicolai Lassen says linking directly to the story saves the reader time: "From the home page down to the actual story you want to read can be a very, very long way. By using a technology such as Newsbooster, you save a lot of time." Newsbooster charges users a subscription fee to send links to news items containing user-designated keywords, and the Danish Newspaper Publishers' Association believes that it should either shut down or negotiate to share those fees. "We consider it unfair to base your business upon the works of others," says the group's managing director. But to Internet purists, the whole point of Web is to create linkages between relevant pages. If the Web's creators hadn't wanted linking, "they would have called it the World Wide Straight Line," says one Web site operator. In the U.S., early court decisions have sided with deep-linking, except in cases of framing, where a site tries to make information created by other sites appear to be its own. "It was one of those issues that people thought was more or less settled. For whatever reason, these last couple of months, a spate of new disputes have come up," says an Internet legal expert. (AP 10 Jun 2002)
http://apnews.excite.com/article/20020610/D7K28Q3G0.html

Category 4A2 *Pointing, linking, deep linking, metatext*

2002-06-21 **deep linking Web permission copyright intellectual property**

EDUPAGE

NPR'S LINK POLICY PROTESTED
National Public Radio has roused public protest in response to its policy on Web linking, which requires prior written consent to link to, or frame, any material on the NPR Web site. A form on the site requests the linker's name, e-mail address, physical address, phone number, information about the linking site, how long the link will remain on the site, the proposed wording, the U.S. state in which the linking site is incorporated, and whether the site is commercial. Although the permission form was updated in March 2002, the policy began to attract attention on Web logs June 19 after a blog owner posted a link to the form. NPR established the policy to support its noncommercial, journalistic nature, according to an NPR spokesman, and to track use.
Wired News, 20 June 2002
http://www.wired.com/news/business/0,1367,53355,00.html

4A3 Jurisdiction

Category 4A3 *Jurisdiction*

1997-01-05 **Internet Web language law France**

Reuters, EDUPAGE, AP

Georgia Tech Lorraine, a French campus of the Georgia Institute of Technology, was in hot water in January when French courts opened hearings on whether the French government has any right to force Web sites physically resident in France to publish their materials in French. All of the students at the campus are required to be fluent in English and all the courses are in English. In June, the case was dismissed on a technicality by French courts, leaving unresolved the question of whether the government of France is legally entitled to order the language of expression of Web sites pertaining to French affairs. According to an AP report by Nicolas Marmie, "Georgia Tech had faced possible fines of up to $4,300 each time the untranslated Internet site was visited."

Category 4A3 *Jurisdiction*

1997-01-07 **internet gambling**

EDUPAGE

EDUPAGE reported on a case of international gambling: >Minnesota law enforcement officials have targeted an Internet-based bookmaking operation being run from a Native reserve in New Brunswick. Representatives of the Tobique Band say they are not violating any laws because the toll-free number is not accessible by Canadians and Americans must call a foreign country to place bets on sporting events because telephone wagering is also illegal there. Minnesota investigators point to a recent victory over a band in Idaho that thought it was immune from laws in other states. (Toronto Globe & Mail 6 Jan 97 A8)<

Category 4A3 *Jurisdiction*

2000-02-22 **jurisdiction online gambling fraud**

NewsScan

In a New York trial that's testing whether this country's. criminal laws apply to Web sites beyond U.S. borders, 21 defendants are charged with using the Internet to violate a law that provides for sentences of up to five years in prison and $250,000 in fines for placing or taking bets over phone lines. The gambling site (based in Antigua, where Internet gambling is legal) accepted bets placed through the Web by U.S. citizens. One of the defendants insists: "As far as we're concerned, all bets are placed here on our server here in Antigua, which is a sovereign state and we're fully licensed"; however, Washington lawyer Jim Halpert comments: "It may not make a difference whether the server was located in Antigua, because the federal anti-gambling law in question applies broadly. Typically, the fact that a site is doing business with consumers in a jurisdiction is sufficient to establish jurisdiction in the state where the consumer is located." (USA Today 22 Feb 2000)

Category 4A3 *Jurisdiction*

2000-06-04 **criminal hacking privacy data haven monitoring government sovereignty jurisdiction**

NewsScan, New York Times
http://partners.nytimes.com/library/tech/00/06/biztech/articles/04have.htm

A company called Havenco has built what it calls a "data haven" on an abandoned military platform in the sea, six miles off Britain's coast, in order to offer communications services to clients who want to avoid monitoring by governmental authorities. Declaring his small fortress a sovereign country beyond the reach of British law, Havenco co-founder and chief executive Sean Hastings, a 32-year-old U.S. citizen, says, "Technology has made it easier to move information and hide information. Soon it will be impossible to trace where money is and who has money, and that will eventually force governments to move away from income taxes and toward consumption taxes." (New York Times 4 Jun 2000)

Category 4A3 *Jurisdiction*

2000-10-11 **extortion theft fencing law enforcement police international jurisdiction**

NewsScan, MSNBC http://www.msnbc.com/news/475316.asp

A Web site devoted to the sale of stolen goods has raised the ire of British lawmakers, who point out that it is illegal to sell stolen property back to its owner. TheBurglar.com is accused of violating the Theft Act by charging people "reward" money for the return of their possessions. Victims of burglaries can post the details of their losses on the site, and burglars are then invited to anonymously contact their victims by e-mail to negotiate the return of the stolen property. The site collects the agreed-upon cash, and keeps it until the victim has verified receipt of the goods. TheBurglar.com then sends the payment to the address or account of the thief's choice. And despite outrage among law enforcement officials, TheBurglar.com likely will escape prosecution. A note on its site reads: " TheBurglar.com Headquarter is placed in Copenhagen, but due to spite we have moved the office to a secret location." (ZDNet UK 11 Oct 2000)

Category 4A3 *Jurisdiction*

2001-01-11 **taxation Web jurisdiction international agreement OECD**

NewsScan

OECD REACHES CONSENSUS ON WEB TAXES
The Organization for Economic Cooperation and Development, which represents 30 leading industrialized nations, says its members have reached a landmark agreement that defines how countries should tax business conducted over the Internet. Tax experts say the deal marks an important milestone, but that wealthy nations need to hold further talks to develop a comprehensive approach to e-commerce taxation. The OECD's committee on fiscal affairs ruled that doing business through a Web site would not leave a company liable to taxation in the country from which the Web site had been accessed. The exemption from liability applies even if the company's Web site is hosted by a third party, such as an ISP. But the committee ruled that a company should generally pay tax in countries hosting servers through which the business was conducted. A company would be liable for paying tax if the server were performing functions that formed a core part of the business activity, such as downloading software. Jacques Sasseville, head of the OECD's tax treaty unit, said the consensus marked an interim solution and that more clarification would be necessary. (Financial Times 11 Jan 2000)
http://news.ft.com/news/industries/internet&e-commerce

Category 4A3 *Jurisdiction*

2001-06-27 **international jurisdiction Web content national law regulations international agreement**

NewsScan

EUROPEAN E-COMMERCE: WHOSE LAW IS IT ANYWAY? [27 Jun 2001]
The European Commission is rethinking a policy that currently applies the law of the country in which the consumer resides to trans-border e-commerce disputes. The reason for the reconsideration is that publishers and others have been complaining that it is impossible to do business internationally if a single country can force its rules on the whole world. Case in point: the dispute between a French court and the U.S. portal Yahoo.com, where the court is insisting that Yahoo must abide by French laws that prohibit displays or sales of Nazi memorabilia on Web sites. If the French prevail, they will have made their laws apply to citizens of all other countries that have no such laws. (New York Times 27 Jun 2001)
http://partners.nytimes.com/2001/06/27/technology/27CROS.html

---

Category 4A3 *Jurisdiction*

2001-09-03 **cybersquatting DNS domain name system trademark extortion international regulation agreement policy proposal intellectual property**

NewsScan

U.N. WANTS STRONGER PROTECTIONS AGAINST CYBERSQUATTING
The World Intellectual Property Organization (WIPO), an agency of the United Nations, wants to protect high-profile individuals and organizations from having their names misappropriated by "cybersquatters" who register domain names of well-known people or companies without their permission. Recent examples have included celebrities such as Julia Roberts and Mick Jagger and soccer clubs like Real Madrid. A WIPO official said: "There is evidence of widespread registration of Internet domains by people who have no connection whatsoever with the names they give their sites. We are recommending that governments look at how the legal basis for dealing with this can be extended." (Reuters/New York Times 3 Sep 2001)
http://partners.nytimes.com/reuters/technology/tech-tech-internet.html

---

Category 4A3 *Jurisdiction*

2002-02-27 **hate speech auction censorship filtering court ruling judgement appeal international conflict jurisdiction**

NewsScan

NAZI MEMORABILIA CASE GETS SECOND LOOK IN U.S. COURTS [11 Feb 2002]
About a year ago a French court decided that Yahoo had violated French law by allowing French citizens to view auction sites displaying Nazi memorabilia and ruled that Yahoo pay $13,000 a day in fines; however, in the U.S. (where the auction sites are located), a federal judge ruled that the French judgment can not be enforced in this country. That ruling is now being appealed by the two original plaintiff groups, The International League Against Racism and Anti-Semitism and the Union of French Jewish students. Alan Davidson, an attorney for the Washington, D.C.-based Internet civil liberties group Center for Democracy and Technology, warns that the French ruling "really puts free expression and communication in jeopardy on the Net," by reducing online speech to the lowest-common denominator of what is permissible as dictated by the most repressive nations. Taking a contrary point of view, University of Chicago law school professor Jack Goldsmith says that countries have the right to choose for themselves what is lawful within their own borders: "That is the essence of territorial sovereignty." (New York Times 11 Feb 2002)
http://partners.nytimes.com/2002/02/11/technology/11NECO.html?pagewanted=print

YAHOO FACES CRIMINAL CHARGES IN FRANCE[27 Feb 2002]
A French criminal court says it plans to prosecute Yahoo and its former president Timothy Koogle for allegedly condoning war crimes by selling Nazi memorabilia. Koogle faces a maximum sentence of five years and an approximately $40,000 fine if found guilty -- a verdict that could have profound implications for free speech on the Net. France had ordered Yahoo in November 2000 to block French citizens from access the sites, but a U.S. federal judge ruled last fall that Yahoo, as a U.S.-based site, was not bound by French laws governing content. (Financial Times 27 Feb 2002)
http://news.ft.com/news/industries/internet&e-commerce

Category 4A3 *Jurisdiction*

2002-11-26 **jurisdiction location intellectual property copyright international**

NewsScan

HOW DO YOU SUE A COMPANY YOU CAN'T FIND?
The Internet music-swapping firm KaZaA, which has assumed the successor role to now-defunct Napster, is being sued in a federal court in Los Angeles by the Recording Industry Association of America for copyright violations, but the RIAA has several problems to overcome. First, there is a question of geography, since KaZaA is everywhere and nowhere: its distributor, Sharman Networks, is incorporated in the South Pacific island nation of Vanuatu, it is managed from Australia, its computer servers are in Denmark, and its developers can't be found. Second, there is an issue of jurisdiction: Sharman's lawyer says, "What they're asking is for a court to export the strictures of U.S. copyright law worldwide. That's not permitted. These are questions of sovereignty that legislatures and diplomats need to decide." And third, there is the question of whether giving people the tools (KaZaA's service) to break the copyright law is itself a copyright violation, even if KaZaA itself did not misappropriate copyrighted music. (New York Times 7 Oct 2002)

KAZAA CASE TO DECIDE REACH OF U.S. COPYRIGHT LAW
A federal judge in Los Angeles has agreed to rule on the question whether American media companies can hold a non-U.S. Internet music file-swapping service liable for breaches of U.S. copyright law as long as a very large number of the file-swapping service's customers are in the U.S. The service in question is Kazaa, which is owned by the Austrian company Sharman Networks, and which has 21 million users. Judge Stephen Wilson has not yet decided the issue, but says he is "inclined" find that his court has jurisdiction: "I find the argument about providing the service to so many California residents compelling." An attorney for the media companies says: "This is important because it shows that you cannot escape U.S. justice by setting up shop outside the United States" — whereas an attorney for Sharman argues that a decision to make companies liable to courts in other countries could lead to a judge "in communist China" to rule against U.S. companies that operate online. (AP 24 Nov 2002)
http://shorl.com/fahadesostigy

Category 4A3 *Jurisdiction*

2002-12-10 **libel Internet international jurisiction lawsuit**

NewsScan

WHERE IS THE INTERNET?
If a citizen of Country X believes he's been libeled by a magazine published in Country Y, does he sue in Country X or Country Y? Australian mining magnate Joseph Gutnick chose Australia to file his lawsuit against Dow Jones, publisher of Barron's magazine, which he alleges defamed him. Australia's highest court has just ruled that it has jurisdiction over the case, and Gutnick says that publishers will now "have to be very careful what they put on the Net. The Net is no different from a regular newspaper. You have to be careful what you write."(Reuters/San Jose Mercury News 10 Dec 2002)

Category 4A3 *Jurisdiction*

2002-12-16 **interstate jurisdiction libel court judgement**

NewsScan

VA. COURT THROWS OUT INTERNET LIBEL SUIT
Three days after Australia's highest court ruled that an Australian businessman may sue Dow Jones & Co. for an article posted in New Jersey but accessible in Australia, a federal appeals court threw out a Virginia prison warden's lawsuit against two Connecticut newspapers, saying the articles posted on their Web sites were not aimed at a Virginia audience. The latest ruling reversed a lower court's decision that found prison warden Stanley Young could sue The Hartford Courant and The New Haven Advocate on the grounds that they falsely depicted him as racist in articles about alleged mistreatment of Connecticut inmates sent to Virginia to alleviate overcrowding. "The facts in this case establish that the newspapers' Web sites, as well as the articles in question, were aimed at a Connecticut audience," wrote Judge M. Blane Michael in the unanimous opinion. "The newspapers did not post materials on the Internet with the manifest intent of targeting Virginia readers." Both courts based their decisions on targeting, but differed in how they defined it, said Michael Geist, a professor at the University of Ottawa who tracks such rulings worldwide. "We have U.S. courts that looked largely at a commercial presence and the intended presence, while you got the Australian court more concerned about where the harm was felt." (AP 13 Dec 2002)
http://apnews.excite.com/article/20021213/D7NT6UEG0.htm

Category 4A3 *Jurisdiction*

2003-02-12 **Internet jurisdiction online auctions**

NewsScan

YAHOO EXONERATED IN NAZI MEMORABILIA CASE
A Paris court has thrown out a case brought against Yahoo by French human rights activists who maintained that Yahoo should be held legally responsible for allowing online auctions of Nazi collectibles. French law forbids the display or sale of racist material. The case led to a landmark ruling in France, with a court ordering Yahoo to block Web surfers in France from accessing auctions selling Nazi memorabilia. Yahoo eventually banned sales of Nazi collectibles when it began charging users for auction listings, saying it did not want to profit from such items, but insisted it had nothing to do with the ongoing litigation. Tuesday's decision ends the three-year legal struggle, with the Paris court's decision that Yahoo did not meet the criteria of "justifying war crimes" because its auction listing did not result in "glorifying, praising or at least presenting the crimes in question favorably." (AP 12 Feb 2003)
http://apnews.excite.com/article/20030212/D7P520LO0.htm

Category 4A3 *Jurisdiction*

2003-04-28 **Internet jurisdiction US supreme court**

NewsScan

SUPREME COURT DODGES QUESTION OF INTERNET JURISDICTION
The U.S. Supreme Court has refused to review a case that might have decided what courts have jurisdiction over cases involving the Internet. The case it rejected was an appeal brought by Healthgrades.com, which rates health care providers, after it had lost a lawsuit to home health care provider Northwest Healthcare Alliance. When Northwest received a poorer rating than it thought it deserved, it sued Healthgrades for defamation, and won. (AP/San Jose Mercury News 28 Apr 2003)

Category 4A3 *Jurisdiction*

2005-01-26 **BlackBerry patent Supreme Court US Canada law legal jurisdiction**

NewsScan; http://apnews.excite.com/article/20050126/D87RP7R00.html

WHERE IN THE WORLD IS BLACKBERRY?

The Canadian government has joined the battle of Ontario-based Research in Motion Ltd. (RIM), creators of the BlackBerry, in that firm's decision to defend itself all the way to the U.S. Supreme Court against a patent infringement case brought against it by an Arlington, Virginia, company. RIM claims that since its BlackBerry relay server is based in Canada, U.S. patent laws have no jurisdiction. The Arlington company argues that RIM is using its technology to reap profits in the U.S. and so U.S. patent laws rule. The Court is expected to hear arguments from the two sides in February. (AP 26 Jan 2005)

Category 4A3 *Jurisdiction*

2005-02-11 **Yahoo France Nazi lawsuit court**

NewsScan; http://www.usatoday.com/tech/news/techpolicy/2005-02-11-yahoo-nazi-stuff_x.htm

NAZI MEMORABILIA DECISION SEEN AS VICTORY FOR FREE SPEECH

The 9th U.S. Circuit Court of Appeals announced it will rehear some arguments in a 5-year-old lawsuit against Yahoo by two French human rights groups that want to ban the sale of Nazi-related items on any Internet site viewable in France. Since French law bars the display or sale of racist material, the groups had won a French court order requiring the company to block Internet surfers in France from auctions selling Nazi memorabilia there, but Yahoo kept such memorabilia on its popular U.S.-based site, yahoo.com. The two-sentence ruling Thursday does not explain how the judges came to their decision but compels both sides to argue their cases again in front of an 11- judge panel. Yahoo attorney Mary Catherine Wirth says, "If American companies have to worry that foreign judgments entered against them might be enforceable, it could end up with companies censoring their Web sites, but Richard Jones, who represented the French organizations, called the decision "meaningless."(AP/USA Today 11 Fe 2005)

4A4 Blocking

Category 4A4 *Blocking*

2000-05-25 **autonomous agents crawlers bots contract law commerce restrictions property auction**

NewsScan, WSJ http://interactive.wsj.com/articles/SB955937300461505269.htm,
San Jose Mercury News
http://www.sjmercury.com/svtech/news/breaking/ap/docs/36278l.htm

The Justice Department is investigating whether eBay's block on "shopping bots" and "crawlers" constitutes anticompetitive behavior. At issue are software programs used by two aggregator sites that compile lists of thousands of sales across a number of auction sites. Bidder's Edge and AuctionWatch have been meeting with Justice officials to discuss the filtering actions taken by eBay that block their ability to search its site. EBay does allow shopping bots from other sites to search its database, but only after they sign a licensing agreement to do so. It has called unauthorized listings of its wares "trespassing and stealing," but Bidder's Edge CEO James Carney says, "What's at stake here is the architecture of commerce on the Internet, whether you can freely search others' sites or whether you have to have their permission. (EBay's tactics) threaten to break down the openness that made the Internet great." (Wall Street Journal 4 Feb 2000)

[In April,] A federal judge . . . [said he was] planning to issue an injunction against Bidder's Edge, one of several so-called aggregators of online auction listings that compile and compare information on eBay, Yahoo, Amazon and other auction operators. The ruling comes in response to a lawsuit filed by eBay, which charges that Bidder's Edge violated the federal Computer Fraud and Abuse Act by using information gleaned from eBay's site. Legal scholars say such a ruling could set new standards in a debate over what is considered copyrightable intellectual property. "Decisions like this are disturbing because if extracting information off a site like eBay's is trespass, then it's going to be difficult for consumers to have the benefit of services that do price comparisons," says a University of California, Berkeley law professor. (Wall Street Journal 17 Apr 2000)

[In May,] Saying that the law recognizes no right to use another's personal property, U.S. District Judge Ronald Whyte . . . ruled that the Internet firm Bidder's Edge trespassed against auction firm eBay when it used "spider" software to crawl through eBay's Web site acquiring information that had been amassed by eBay. Bidder's Edge . . . [claimed] that the issue is "about the openness of information on the Internet," but eBay argues that the judge's ruling was "important for all Internet entrepreneurs who hope to create businesses based on databases without fear that trespasses will come in and steal the fruits of their labor." (AP/San Jose Mercury News 25 May 2000)

Category 4A4 *Blocking*

2001-12-12 **e-mail property rights free speech criticism lawsuit ruling court judgement**

NewsScan

FLOODING A COMPANY'S MAIL SYSTEM: FREE SPEECH ISSUE OR PROPERTY ISSUE? [12 Dec 2001]
An appellate court in California has ruled that an ex-Intel employee had no right to send e-mail messages criticizing the company to 30,000 Intel employees. The ex-employee argued that the company's e-mail system is entitled to the First Amendment protections of a public forum; a divided court disagreed, with the majority saying that "Intel is as much entitled to control its e-mail system as it is to guard its factories and hallways." An appeal is expected. (San Jose Mercury News 12 Dec 2001)
http://www.siliconvalley.com/docs/news/svfront/email121201.htm

---

Category 4A4 *Blocking*

2003-03-12 **pop-up advertising blocking software ISP Internet service provider**

NewsScan

EARTHLINK MOVES TO BLOCK POP-UP ADS
EarthLink, in a move to differentiate itself from rival ISPs, says it will offer subscribers free software to block those annoying pop-up ads that clutter the screen. The Pop-Up Blocker software uses technology from FailSafe Technology in Salt Lake City, and by taking the initiative to offer it EarthLink hopes to reinforce its image as an ISP that's more receptive to user needs than many of its competitors. Meanwhile, advertisers are already hard at work on new formats and strategies to outsmart the ad-blockers. And the race continues? (Wall Street Journal 19 Aug 2002)

AOL SMACKS DOWN POP-UP ADS
In an effort to revitalize its online service, AOL is pulling the plug on those annoying pop-up ads that clutter users' screens. Although the company officially stopped selling pop-ups on Tuesday, the ads will continue to appear on the site for several more months, because it must still honor existing advertising contracts, says CEO Jonathan Miller. Also, AOL is reserving the right to run pop-ups on behalf of AOL and other AOL Time Warner divisions. Consumers generally don't like pop-up ads, according to a November 2001 study by Dynamic Logic. In fact, only telemarketing was considered more annoying than pop-ups in that study, which looked at consumer responses to TV commercials, direct mail, and print ads in newspapers and magazines. According to a Nielsen/NetRatings report issued last month, fewer than one in 10 of all companies advertising online use pop-up ads. Meanwhile, Microsoft's MSN service says it will continue to run pop-ups, although with a low frequency, and Yahoo plans to continue using pop-ups on a limited basis, mostly for surveys after a consumer completes a shopping purchase or related to movie ads. (Wall Street Journal 16 Oct 2002)

EARTHLINK DERIDES AOL'S POP-UP ADS
Earthlink has launched a two-week ad campaign in the New York Times and USA Today to try to woo current AOL subscribers who are unhappy with AOL's practice of using pop-ads. One ad asks mockingly, "What can you expect now that AOL only allows pop-up ads from AOL Time Warner businesses?" Another sneers: "It took AOL 8.0 tries to figure out people don't like pop-up ads?" AOL seems to be trying to shrug its rival off, and a spokesman for that company said condescendingly: "It must be frustrating for competitors in the online industry who have lost this wedge issue with customers." (Atlanta Journal-Constitution 1 Nov 2002)

AOL DELIVERS USERS FROM 'POP-UP PURGATORY'
America Online is giving its subscribers some relief from the annoying pop-up ads that seem to be proliferating at an alarming pace across the Web. In response to complaints from users, AOL will automatically install its Web Pop-Up Controls onto the desktops of its 33 million subscribers during the next two weeks. Many AOL users had listed pop-up advertising as one the most annoying features of surfing the Web. "AOL's new Pop-Up Controls will allow our members to explore the Web without being trapped in pop-up purgatory," says an AOL spokesman. The latest move mirrors one made by rival Earthlink several months ago, and comes as the world's largest Internet provider is struggling with stagnant subscriber growth over the past year. (CNet News.com 11 Mar 2003)
http://news.com.com/2100-1024-992142.html

Category 4A4 *Blocking*

2005-06-15 **censorship China content filtering Web blog**

RISKS 23 90

MICROSOFT CENSORING BLOGS IN CHINA

Peter G. Neumann contributed this acerbic little note:

Microsoft is cooperating with China's government to censor MSN's Spaces Chinese-language Web portal. Bloggers are prevented from posting words such words as *democracy*, *human rights*, and *Taiwan independence*. 5 million blogs have been created since the service started on 26 May 2005. China reportedly has 87 million online users.

[Source: AP item by Curt Woodward, 14 Jun 2005, seen in the *San Francisco Chronicle*.]

[I wonder whether this issue of RISKS will be blocked because of those OFFENSIVE words? (And I thought *democracy* and *human rights* were DEFENSIVE words?) PGN]

4A5 Archives

Category 4A5 Archives

2001-05-07 **copyright intellectual property privacy archives USENET persistence**

NewsScan

NET CONVERSATION: OPEN, CASUAL... AND ETERNAL
Privacy advocates haven't been expressing much concern about the creation by the Internet search Google of its "archive of human conversation," which allows the searching of archived postings of the Usenet bulletin boards (http://groups.google.com). Devorah Pierce, a lawyer for the Electronic Frontier Foundation, a noted advocacy group for privacy on the Internet, says that contributors to Usenet discussions shouldn't expect too much privacy because "if that's not a public forum I don't know what is." But she and others worry that people don't expect their casual conversations to follow them forever. Another privacy advocate, Bruce Koball, says: "People can be rightfully mortified when the come back five years from now and see a post that they made. And now it's enshrined in magnetic media for time immemorial." (New York Times 7 May 2001)
http://www.nytimes.com/2001/05/07/technology/07NECO.html

Category 4A5 Archives

2001-08-15 **copyright intellectual property archive Web broadcast permission**

NewsScan

THIRD-PARTY ARCHIVING COMES UNDER FIRE [15 Aug 2001]
Public companies have embraced Internet technology to offer investors access to live webcasts of once-private meetings, where company officials discuss quarterly results and business outlooks. But in some cases, creating a historical record can become a headache when that record is archived on other companies' Web sites. In one of the highest-profile disputes, R.J. Reynolds has demanded that financial news provider Bloomberg stop archiving the tobacco firm's conference calls, saying that the information exchanged in those calls belongs to the company. Bloomberg has responded that it's not violating any copyright restrictions because it records the calls itself, rather than using recordings produced by another company. Reynolds' policy is to make each call available on its Web site for just seven days, saying that investors could be confused if information exchanged in the call is taken out of context, but Bloomberg has refused to take the calls off its own site, saying it is valuable for shareholders to be able to go back and listen to officials' reasoning for making a business decision. One copyright expert says it would be difficult for a company to sue for unauthorized use of a conference call unless it is registered with the copyright office, especially when the call includes outside analysts as interviewers. Bloomberg records and archives between 500 and 1,000 conference calls each quarter, and customers pay $1,285 a month for the company's flagship Bloomberg Professional service. (Wall Street Journal 15 Aug 2001)
http://interactive.wsj.com/archive/retrieve.cgi?id=SB997196102924013249.djm

---

Category 4A5 Archives

2001-11-28 **Web sensitive data archiving duplication control copyright intellectual property distribution removal impossible change**

RISKS 21 80

David Colker of the Los Angeles Times wrote, "Government agencies have tried to remove sensitive information, only to discover that copies have proliferated and they're virtually impossible to eradicate. Within days of the 11 Sep attacks, the federal Agency for Toxic Substances and Disease Registry rushed to pull a suddenly sensitive report from its Web site titled "Industrial Chemicals and Terrorism." The agency eliminated all traces of the document and its description of sources for home-brew nerve gases and improvised explosives. But on the World Wide Web, almost nothing truly dies. . . ."
http://www.latimes.com/news/printedition/la-000094419nov27.story

---

Category 4A5 Archives

2001-12-20 **Web copyright intellectual property archives long-term retention**

NewsScan

LONG-TERM RETENTION OF DIGITAL RESEARCH MATERIALS [5 Sep 2001]
RLG has released the second report developed in collaboration with OCLC Online Computer Library Center to advance long-term retention of digital research materials. In a joint announcement of the report, RLG president James Michalko said he hopes the study will spark a debate that ultimately will result in "some small number of trusted, reliable service providers, whether they are research institutions themselves or third parties." OCLC president and chief executive officer Jay Gordon explained that OCLC's digital archiving initiatives "are guided by active participation in this working group and other key projects." The paper is freely available as a PDF document from the RLG web site at www.rlg.org/longterm/attributes01.pdf and is linked to from www.oclc.org/digitalpreservation and www.oclc.org/presres.

PRIVACY, SECRECY AND RESPONSIBILITY [20 Dec 2001]
[Another in a series]. . . of two reports collaboratively prepared by RLG and OCLC Online Computer Library Center to advance long-term retention of research materials held in digital form is now available from RLG and OCLC. Dialogue on the standards, criteria, and mechanisms for certifying digital information repositories will encourage an international consensus. "Ultimately," says RLG president James Michalko, "I'd like to see the debate result in some small number of trusted, reliable service providers, whether they are research institutions themselves or third parties." (RLG News Issue 53)
http://www.rlg.org/longterm/attributes01.pdf

Category 4A5 Archives

2002-01-22 **Internet Web archives legal implications lawsuit trial judgement ruling**

RISKS 21 88

Roger Needham wrote in RISKS that a judge thinks that archiving news stories may violate the integrity of a criminal prosecution. "It is a principle in many jurisdictions that a jury should not know about prior charges or convictions of the accused. In a Scottish court a man was accused of a particularly revolting crime, he having been acquitted of a similar offence on a technicality a number of years ago. The judge ruled that the editor of a newspaper was in contempt of court by leaving reports of the earlier trial on line in his archive, because he had made it too easy for jurors to find out what they were not meant to know. The judge apparently believed that the greater ease of access of the on line archive as compared to a paper archive was a difference not of degree but of kind."

Category 4A5 Archives

2002-03-04 **archive data loss compatibilitie media retention archives readability accessibility expiration degradation**

RISKS 21 91

Chris Leeson summarized another case of technological obsolescence and data loss in archives: "The BBC's 1986 Domesday Project (a time capsule containing sound, images, video and data defining life in Britain) is now unreadable. The data was stored on 12-inch video discs that were only readable by the BBC Micro, of which only a handful still exist. The time capsule contains "250,000 place names, 25,000 maps, 50,000 pictures, 3,000 data sets and 60 minutes of moving pictures.". The article notes that the original Domesday Book (compiled in 1086 for tax purposes) is still in "mint condition."

Category 4A5 Archives

2005-03-03 **online archive New York Public Library Digital Gallery**

EDUPAGE; http://chronicle.com/prm/daily/2005/03/2005030307n.htm

NEW YORK PUBLIC LIBRARY UNVEILS ONLINE ARCHIVE

The New York Public Library this week unveiled an online archive of 275,000 images, available to the public for free. The project, called the NYPL Digital Gallery, is supported by a $7 million grant from The Atlantic Philanthropies and includes Civil War photographs, illuminated manuscripts, Japanese prints, early American maps, and photographs of New York City buildings and streetscapes. Paul LeClerc, president and chief executive officer of the library, noted that while other libraries are digitizing texts, few are putting materials such as photographs and maps online. Images in the collection are either in the public domain or are owned by the library and can be downloaded and used for noncommercial purposes. The NYPL Digital Gallery project, which is unrelated to the library's arrangement with Google to digitize content, is expected to add another 225,000 images to its database in the coming months. Chronicle of Higher Education, 3 March 2005 (sub. req'd)

4A6 Libel

Category 4A6 *Libel*

1997-06-01 **law harassment anonymity Internet privacy**

EDUPAGE

ANONYMOUS HARASSMENT ON NET ELUDES FLORIDA LAW
Two Florida men who had been arrested for anonymous harassment on the Internet have now been released. A chief assistant state attorney in Florida explains: "It's simply not criminal under statute in the state of Florida. I'm not condoning this activity. All I'm saying is that I'm left powerless to do anything about it." The two men are 19-year-old former high school students who had used a Web site to allege that a teacher and student at their school were engaging in homosexual relations. The statute cited in the men's arrest prohibits anonymous publication of material that holds a person up to ridicule or contempt; however, the Florida state attorney's office concluded that the statute is an unconstitutional infringement of the right to free speech. (St. Petersburg Times 31 May 97)

Category 4A6 *Libel*

1997-08-31 **journalism libel hoax**

EDUPAGE, AP, ZDNN

DRUDGING UP CRITICISM
Gossip columnist Matt Drudge, whose newsletter is distributed via America Online and the World Wide Web, has been taking a drubbing for two recent stories he — one about President Clinton and another about White House adviser Sidney Blumenthal. Blumenthal is considering a libel suit and the New York Times has lamented editorially that Drudge's work is an example of the kind of shoddy journalism encouraged by what it called "www.anarchy.net." And Newsweek investigative reporter Michael Isikoff says that Drudge is "a menace to honest, responsible journalism. He's clearly willing to go with anything, whether he's got any legitimate sourcing, anything approaching legitimate verification. He doesn't conform to any journalistic standard or convention that I'm aware of. And to the extent that he's read and people believe what they read, he's dangerous." (New York Times 15 & 17 Aug 97)

DRUDGE'S APOLOGY DOESN'T STOP BLUMENTHAL'S LIBEL SUIT
A White House spokesman has acknowledged that President Clinton and Vice President Gore approved of Presidential aide Sidney Blumenthal's decision to file a $30 million libel suit against online gossip columnist Matt Drudge. Drudge had reported that Blumenthal "has a spousal abuse past that has been effectively covered up," but when Blumenthal vehemently denied the allegation, Drudge quickly issued a retraction. But Blumenthal wasn't mollified, and proceeded with his lawsuit. In his August 29th "Drudge Report," Drudge says he is "disappointed that this lawsuit was filed even after I retracted my original report and publicly apologized for it. The fact that Mr. Blumenthal's 137-page complaint seeks to recover $30 million from me has no relation to anything that I have done — unless the White House views me as a reporter who should not be in business. The extraordinary admission at the August 28 White House press briefing that both the President and Vice President told Mr. Blumenthal they would support him in this action suggests this White House simply lacks respect for basic principles of free speech and the First Amendment guarantee of a free press. What the White House is doing in supporting this lawsuit should arouse grave concern among all those who cherish our Constitution." Drudge has been widely criticized by mainstream journalists, who have accused him of practicing shoddy journalism. (Edupage 17 Aug 97, Reuter 28 Aug 97, Drudge Report 29 Aug 97)

Category 4A6 *Libel*

2001-08-09 **libel Internet republishing culpability liability ISP news group**

NewsScan

LIBEL IN CYBERSPACE [9 Aug 2001]
A trial court judge in California has interpreted federal law to mean that a person who re-posts libelous information on the Internet is protected against libel suits. The ruling stands a dramatic contrast to traditional libel law, which holds that someone who carelessly or recklessly circulates a defamation may be just as guilty as the originator of the libel. The judge in this case gave a broad interpretation to a federal law passed to protect Internet service providers and news group operators from being held responsible for postings made by third-party individuals. The plaintiffs, who will appeal the judge's decision, charge that "what this ruling does is open the door for any number of wrongdoers to just basically take something that's libelous, republish it and claim immunity." (New York Times 9 Aug 2001)
http://partners.nytimes.com/2001/08/09/technology/10CYBERLAW.html

---

Category 4A6 *Libel*

2001-12-11 **online journalists print libel protection lawsuit court ruling judgement**

NewsScan

ONLINE JOURNALISTS HAVE SAME PROTECTIONS AS PRINT [11 Dec 2001]
Online journalists enjoy the same free-press protections against libel charges as those accorded to print, radio and TV reporters, according to a recent ruling in the New York State Supreme Court. The case, National Bank of Mexico v. Narconews.com, was initiated when the Bank of Mexico -- now part of Citigroup -- sued the drug-war investigative reporting Web site, charging that reports linking the Bank's then-president with narcotics trafficking were false and libelous. A 1964 U.S. Supreme Court decision -- New York Times v. Sullivan -- had established that defamation cases brought against journalists must meet a "higher standard," and that journalists can only be found guilty of libel if their actions are deemed malicious. "This court finds that Narconews is a media defendant and is entitled to a heightened protection under the First Amendment," wrote New York Supreme Court Justice Paula Omansky, citing the NYT v. Sullivan precedent. Al Giordano, editor and publisher of Narconews, said the decision should encourage online journalists to take on more hard-hitting news assignments. "The case law that comes out of Judge Omansky's decision is a miracle for online news sites like my own and online journalists like myself. It establishes that an online news provider now has the same rights as The New York Times or any other newspaper or magazine in the eyes of the law." (Wired.com 11 Dec 2001)
http://www.wired.com/news/politics/0,1283,48996,00.html

Category 4A6 *Libel*

2002-06-21 **defamation First Amendment free speech Web site contempt of court injunction lawsuit**

NewsScan

TO AVOID MORE JAIL TIME, ANGRY MAN SHUTS DOWN WEB SITE
After spending 111 days in jail for contempt of court, a 68-year-old Seattle man has won his release by shutting down a Web site he'd created to attack the retirement home in which he lived -- charging it violated federal housing laws, allowed neighbors to keep him up at night, and employed a manager who had a sexual dysfunction. The judge called him "a mean old man who becomes angry and vicious when he doesn't get his own way," while his lawyer was more supportive: "He had a choice between being pulling it and being put in jail by a judge who doesn't understand some of the fundamental precepts of constitutional law. He's an elderly man who doesn't need to risk his life. He can't tolerate being in solitary confinement." The man said he will continue to fight for his First Amendment rights in court. (AP/USA Today 21 Jun 2002)
http://www.usatoday.com/life/cyber/tech/2002/06/21/web-jailing.htm

[Another report on this case at
< http://news.findlaw.com/ap/ht/1700/6-17-2002/20020617124501_04.html >]

Category 4A6 *Libel*

2005-05-13 **blogging blog entry libel defamation lawsuit St. Lawrence University anonymous attack**

EDUPAGE; http://www.insidehighered.com/news/2005/05/13/lawrence

UNIVERSITY SEEKS NAMES OF BLOGGERS

Officials at St. Lawrence University are trying to obtain the names of individuals responsible for a blog that includes content the university finds inappropriate. Included in the blog, whose stated goal is to fight a "right-wing assault" on the university, are pictures of and harshly derogatory comments about students and faculty whom the blog's contributors see as conservative. Other blog posts criticize university policies and administrators, but Macreena Doyle, a spokesperson for St. Lawrence, said the institution is most concerned about the anonymous attacks on students. "If these were posters attacking students on campus," said Doyle, "we would take action." The university has filed "John Doe" court actions with Time Warner Cable, whose service was used to make postings to the blog, demanding information that would identify the blog's contributors. Google disclosed IP addresses from which blog postings came after being ordered to do so by the courts, but it is not clear whether Time Warner will do the same. Inside Higher Ed, 13 May 2005

4A7 Spam

Category 4A7 *Spam*

1997-05-22 **spam law US**

RISKS 19 18 ff

Two proposals were introduced in the US Congress. The House bill from Chris Smith (R-NJ) was called the "Netizens Protection Act of 1997." The Senate bill was the "Unsolicited Commercial Electronic Mail Choice Act of 1997" from Sen. Murkowski (R-AK). The House bill would extend legislation restricting junk fax; the Senate bill would require junk e-mail to include "ADVERTISEMENT" as the first word of the subject line. ISPs would be required to move toward providing filtering software to bar such tagged e-mail. Critics pointed out that the Senate bill had serious flaws, including no provision for interdicting non-commercial spam. In addition, the proposal for allowing filtering does not deal with the underlying problem: the floods of junk would still enter the Internet and travel to their unwilling recipients before being discarded.

Category 4A7 *Spam*

1997-06-29 **junk spam unsolicited commercial e-mail law legislation**

AP

Donna Murphy Weston, writing for AP at the end of June, summarized several bills in the U.S. federal legislatures in June. "Sen. Robert Torricelli, D-N.J., has proposed a bill that would prohibit junk e-mailers from disguising their identity, continuing to send messages to those who ask to be taken off their list, and using automated programs to cull e-mail addresses from news groups and chat forums." Another proposal, by Sen. Frank Murkowski (R-Alaska), would require labelling of unsolicited commercial e-mail to allow victims to filter the junk out manually or electronically. In the House, Rep. Chris Smith (R-Robbinsville, NJ) wants to ban junk e-mail outright by extending existing telecommunications law (in particular The 1991 Telephone Consumer Protection Act, which protected consumers against abuse of their fax machines) to include computers explicitly "in a ban on transmission of unsolicited ads through telephone lines." Some free-speech advocates object to any government regulation of e-mail at all. Chet Dalzell, speaking for the Direct Marketing Association, claimed, "When you have any new technology, you'll find there are people who'll push the parameters. . . .[b]ut all indications are that marketplace forces will drive development of technology to protect consumers without government regulation."

Category 4A7 *Spam*

1999-10-13 **spam junk unsolicited commercial e-mail criminal law legislation bill proposal**

Newsbytes

The Unsolicited Electronic Mail Act was introduced to the House of Representatives by Heather Wilson (R-NM) and Gene Green (D-TX). This act would
* punish spammers with fines of $500 per message and $25,000 per day;
* define no-spam zones ("virtual gated communities") on the Net;
* allow individuals to post electronic "no trespassing / no spam" signs on their PCs and have mandated legal penalties for violation of those restrictions.

Category 4A7 *Spam*

2000-03-24 **spam unsolicited commercial e-mail law court judgement ruling decision first amendment**

NewsScan

For the fourth time in three years, a federal or state judge has ruled against a state-level attempt to legislate Internet spamming, on the grounds that is in violation of the Constitution's commerce clause, which specifies that a state cannot pass a law concerning activity within its borders if the law's local benefits are outweighed by the burden it imposes on the interstate flow of goods, services, or information. The most recent decision comes from a Washington state Superior Court in Seattle. Professor Jack Goldsmith of the University of Chicago Law School predicts that the issue will ultimately be decided by the U.S. Supreme Court: "It's going to be fascinating," he predicted. "The current justices tend to be pro-states' rights, and they're going to be sympathetic to some of these state regulations. On the other hand, many people think state regulations of the Internet are a drag on the development of the Net, and the Court has shown a broad sympathy to that point of view, too." (New York Times 24 Mar 2000)

Category 4A7 *Spam*

2000-07-19 **spam unsolicited commercial e-mail junk criminals fraud forgery e-mail return address penalties**

NewsScan

The U.S. House of Representatives passed 427-1 a bill that would require senders of unsolicited commercial e-mail messages to provide a valid return e-mail address that recipients of the messages could use to take them off the mailing list. Under the law, the Federal Trade Commission could bring legal actions again spammers who willfully ignore it. Violators could also be sued by Internet service providers. (AP/USA Today 19 Jul 2000)

Category 4A7 *Spam*

2001-02-12 **anti-spam legislation**

NewsScan

CONGRESS EYES ANTI-SPAM MEASURE
Legislation designed to block spam has been reintroduced in the U.S. House of Representatives by the same representatives who sponsored the legislation in the last Congress. Representatives Heather Wilson (R-NM) and Gene Green (D-Texas) resubmitted the Unsolicited Commercial E-Mail Act, which had passed the House last year by a vote of 427-1. The bill stalled in the Senate last year after being introduced late in the session, but "we are optimistic that we will have success this year," says a spokesman for Wilson. The legislation would give consumers the power to block unwanted e-mail and provide ISPs with the legal right to block those who dump unwanted messages onto their networks. It would require e-mail marketers to provide accurate return addresses on unsolicited commercial e-mail; make it illegal to continue sending e-mail after someone has requested to be removed from a distribution list; require unsolicited commercial e-mail to be labeled; and require ISPs to allow their customers to opt out of receiving junk e-mail if the ISP profits from allowing it on their system. ISPs would be allowed to sue spammers for $500 per message if they violate their anti-spam policy. (InfoWorld.com 14 Feb 2001)
http://www.infoworld.com/

Category 4A7 *Spam*

2001-05-10 **unsolicited bulk commercial e-mail spam junk anti-spam legislation**

NewsScan

ANTI-SPAM LEGISLATION [BLOCKED] IN U.S. HOUSE [10 May 2001]
The House Judiciary Committee is blocking an anti-spam bill that previously passed the House Energy and Commerce Commission. The bill would impose a $500 penalty for each piece of unsolicited e-mail a company distributes. Judiciary Committee member Bob Goodlatte (R., VA) said: "Legislation should be narrowly targeted to provide law enforcement with the tools they need to combat abuses without opening the floodgates to frivolous litigation or interfering with legitimate uses of e-mail for marketing purposes." The Committee favors an alternative bill, sponsored by Goodlatte, that penalize senders of unsolicited commercial messages only if the they used a bogus return address. (AP/USA Today 10 May 2001)
http://www.usatoday.com/life/cyber/tech/2001-05-10-anti-spam-opposition.htm

---

Category 4A7 *Spam*

2002-05-29 **anti-spam legislation Europe cookies privacy surveillance controls legislation proposals law**

NewsScan

EUROPEAN PARLIAMENT CLOSE TO SPAM BAN
A bill that would outlaw unsolicited commercial e-mail and prohibit the unauthorized placement of files (such as cookies) on people's computers is close to passage in the European Parliament. In a nod to heightened concerns over cybercrime and terrorist activities, the bill would also give European law enforcement officials greater access to electronic records of people's phone calls and Web visits by allowing the retention of such records "for a limited period" to safeguard national security and aid the "prevention, investigation, detection and prosecution of criminal offenses." The proposed legislation is the result of two years of intense lobbying by consumer groups, e-commerce firms, law-enforcement officials and privacy advocates. "We'll get a good and delicate balance between the needs of law-enforcement agencies and the respect of human rights," says a spokesman for the European Commission. (Wall Street Journal 29 May 2002)
http://online.wsj.com/article/0,,SB1022615363371120040.djm,00.html (sub req'd)

Category 4A7 *Spam*

2002-09-24 **spam text messaging cell phones legislation law bill**

NewsScan

BAN ON CALIFORNIA SPAMMIN'
A new California law that will take effect in January bans the unsolicited sending of text messages to cell phones. The bill's author, Assemblyman Tim Leslie (R, Tahoe City), says the bill is intended to stop spam text messages from getting as out of control as spam e-mail messages. The bill is part of a package (called "leave-us-alone-legislation), which also bans unsolicited fax ads and which makes changes to California's "do-not-call" list for telemarketers. (AP/USA Today 23 Sep 2002)

Category 4A7 *Spam*

2002-09-27 **spam buld e-mail junk lawsuit government law**

NewsScan

CALIFORNIA SUES BULK MAILER
Under a four-year-old anti-spam law that has had little success in controlling unsolicited bulk commercial mail ("spam") over the Internet, California's attorney general has filed a $2 million lawsuit against the PW Marketing Group for sending millions of spam messages, and for failing to include in their messages a valid return address, as required by the law. Calls to PW Marketing have not been returned. To explain the failure to produce more successes over the four years in which the law has been in effect, a spokesperson for Bill Lockyer, the California attorney general, says that anti-spam lawsuits are "difficult, complex cases, and time-consuming." (San Jose Mercury News 26 Sep 2002)

Category 4A7 *Spam*

2002-10-30 **spammer court legal action settlement ban bulk junk e-mail**

NewsScan

VERIZON SILENCES SUPER-SPAMMER
Verizon has reached a legal settlement that bans Alan Ralsky, whose company Additional Benefits LLC is considered to be one of the world's largest sources of bulk e-mail, from sending messages to its 1.64 million Internet access customers. Verizon had filed its lawsuit against Ralsky in March 2001 after several incidents in which Verizon customers were inundated with millions of e-mail solicitations for online casinos, diet pills, credit repair services, etc. The complaint said Ralsky broke federal and Virginia laws by, among other things, clogging its network with illegitimate e-mails. Ralsky must also pay an undisclosed fine, but apparently remains unfazed the recent action, stating that he has lists of 150 million e-mail addresses, so the Verizon case will eliminate only a small portion of those. (AP 30 Oct 2002)
http://apnews.excite.com/article/20021030/D7MVTD300.htm

Category 4A7 *Spam*

2003-02-19 **spam dictionary attack lawsuit ISP Internet service provider**

NewsScan

MICROSOFT STEAMED OVER HOTMAIL SPAM
Microsoft has filed a lawsuit against unnamed bulk mailers who harvested the e-mail addresses of Hotmail users in order to bombard them with junk messages. The spammers allegedly used tools to randomly generate e-mail addresses and then tested them to see which accounts were active. Microsoft argues that this form of dictionary attack violates federal laws, including the Computer Fraud and Abuse Act. (The Register 19 Feb 2003)
http://www.theregister.co.uk/content/6/29382.html

Category 4A7 *Spam*

2003-02-20 **spam laws content filtering**

NewsScan

ANOTHER ANTI-SPAM LAW PROPOSED
At least 26 states already have anti-spam laws on the books, without much to show for them, but California state senator Debra Bowen is trying again, this time by proposing a bill making it a crime to send unsolicited commercial e-mail to accounts in California. Bowen says that spam "is really turning the Internet into a tool of questionable value. I had someone write to me say, 'Spam is turning the Internet into an open sewer, and as the Romans discovered, open sewers are a bad thing.'" However, Jupiter Research analyst Jared Blank says it will take technology rather than legislation to get spam under control. But filtering technology can also be a problem, and the E-mail Service Providers Coalition hopes people will report missing and legitimate e-mail caught in "spam traps." [Good idea. Be sure to do that if you find some befuddled programmer is depriving you of your NewsScan Daily for one silly reason or another, hurting our feelings by confusing us with Spam. Can you BELIEVE that?] (Reuters/USA Today 19 Feb 2003)

Category 4A7 *Spam*

2003-02-21 **spam legislation laws task force ISP Internet service providers**

NewsScan

AOL PREPARES FOR NEW BATTLE AGAINST SPAM
America Online has told its 27 million U.S. customers that it is forming an anti-spam task force and will seek tougher legislation to stop unsolicited junk e-mail. . . . (San Jose Mercury News 21 Feb 2003)

THE AOL APPROACH TO SPAM
America Online, which says it blocks an average of 28 junk e-mail messages per account per day, trashed a billion (presumably unsolicited) messages in a two-day period this week, without letting them arrive at customers' in-boxes. AOL spokesman Nicholas Graham asserts that only "an extremely small fraction" of the messages trapped in AOL's spam filters are legitimate communications. . . . (AP/San Jose Mercury News 6 Mar 2003)

Category 4A7 *Spam*

2003-02-25 **spam marketing proposed legislation penalties**

NewsScan

DIRECT MARKETERS JOIN FIGHT AGAINST SPAM
An unlikely ally has joined the battle against unsolicited commercial e-mail — the Direct Marketing Association announced it is now backing the push for federal legislation to restrict spam. The DMA previously had urged self-regulation, but now says the spam problem has gotten totally out of hand: "The volume is so great that we have to have some sort of government intervention," says DMA senior VP Jerry Cerasale. The group says that legitimate marketers should still be allowed to use e-mail, but plans to suggest that marketers who violate consumers' requests to be removed from mailing lists should pay stiff penalties of $11,000 per incident (per unsolicited message). Spam now comprises 41% of all e-mail, according to Brightmail, and accounts for $4 billion a year in lost productivity, according to a Ferris Research study. (Wall Street Journal 25 Feb 2003)

Category 4A7 *Spam*

2003-03-30 **e-mail bomb Intel free speech private poperty lawsuit**

NewsScan

INTEL VS. HAMIDI: FREE SPEECH CASE OR PRIVATE PROPERTY CASE?
The California Supreme Court will soon be reviewing a lawsuit first brought five years by chipmaker Intel against a terminated employee whom it charges violated its private property rights by bombarding its e-mail system with messages to Intel employees. The ex-employee, Ken Hamidi, has portrayed the dispute as a freedom of speech case, whereas Intel says the issue is not about the content of Hamidi's messages but about the fact that he used Intel's own systems without its permission. Intel says, "For us, it's not a First Amendment issue and never has been. Ken has been very persistent and creative in exercising his right to speak out. But our view is that, in exercising his rights to free speech, he needs to protect the property fights of Intel, including our e-mail system." On the other hand, Stanford law professor Jennifer Granick argues that there was no violation of Intel's property rights because there was no actual damage to Intel property: "There is no harm to Intel's servers — it's the communication of the message that Intel considers the harm. That's not the kind of harm the courts should be in the business of protecting people from. It undermines the nature of the Internet as a place to exercise free speech rights."(San Jose Mercury News 30 Mar 2003)

Category 4A7 *Spam*

2003-04-15 **spam lawsuits AOL America Online**

NewsScan

AOL SUES SPAMMERS
AOL has filed five federal lawsuits against alleged distributors of mass junk-mail, seeking damages of more than $10 million plus an end to the messages. The case comes in response to about 8 million individual spam complaints registered by AOL subscribers, most of whom used a "Spam Report" feature introduced on the Web site last fall. Most of the defendants are referred to as "John Doe," meaning that AOL could not determine their true identities, but the suits also name Michael Levesque of Issaquah, Wash., and George A. Moore Jr. of Linthicum, Md., both of whom had listed false phone numbers in their domain name registrations. By filing the lawsuits, AOL gains additional authority to subpoena Internet service providers and others trying to track down the other spammers. Meanwhile, AOL has also begun targeting spammers who use residential broadband services such as Comcast and RoadRunner, which is owned by AOL Time Warner. (AP 15 Apr 2003)

Category 4A7 *Spam*

2003-04-17 **spam Australia Internet harm**

NewsScan

SPAM WARS: THE BATTLE FOR AUSTRALIA
Another spam story. Richard Alston, Australia's minister for communications and information technology, says that Internet spam "is now completely out of hand" — "no longer a nuisance but costly, disruptive and a threat to IT systems." He therefore will propose to that country's federal parliament legislation that would ban unsolicited commercial Internet messages and impose substantial fines on Australian spammers. Estimates of lost time and productivity are $960 per employee bombarded with e-mail messages offering black market drugs, pornography, Nigerian money laundering schemes, and other such unwelcome material. (The Age, Australia, 17 Apr 2003)

Category 4A7 *Spam*

2003-04-18 **spam pornography lawsuit FTC**

NewsScan

FTC ACCUSES MAN OF PORNOGRAPHIC SPAMMING
There is no federal law banning governing spam, so the Federal Trade Communications is invoking laws against business fraud to file a lawsuit against Brian Westby of Missouri, whom it charges with netting $1 million from his Internet pornographic e-mail campaigns using fake subjects such as "What is wrong?" and "Fwd: You may want to reboot your computer." The FTC says that more than a third of the 120,000 pieces of pornographic spam it receives each day from displeased spam recipients is accounted for Westby's activities. (Washington Post 18 Apr 2003)

Category 4A7 *Spam*

2003-04-26 **spam fight against bounty legislation**

NewsScan

A BOUNTY ON THE HEADS OF SPAMMERS
Congresswoman Zoe Lofgren plans to introduce legislation drafted by Stanford law professor Larry Lessig that would require unsolicited commercial e-mails ("spam") to be identified as advertising and would put a bounty on anyone who breaks that law, by offering rewards of thousands of dollars or more to the person who is first to provide the government with proof and the identity of offending spammers. Lessig is so confident his war on spam will be effective that he's promising to quit his Stanford job if the bill becomes law and "does not substantially reduce the level of spam." (San Jose Mercury News 26 Apr 2003)

Category 4A7 *Spam*

2003-04-30 **spam anti-spam law Virginia jail term e-mail**

NewsScan

VIRGINIA'S NEW LAW THREATENS SPAMMERS WITH JAIL TERMS

Under a new law enacted in Virginia, individuals who use deception to send high-volumes of unsolicited commercial e-mail will be declared felons and liable to one- to five-year prison terms. Virginia Governor Mark R. Warner says, "Many spammers see the current system that imposes civil fines as just a cost of doing business. We hope we will see some high-profile prosecutions. If someone faces a jail sentence and a major forfeiture of assets, it will serve as a deterrent." The new law, which outlaws practices such as forging the return address line of an e-mail message or sending spam surreptitiously, would apply to anyone who sent high volumes of spam to or from anyone in Virginia. (New York Times 30 Apr 2003)

Category 4A7 *Spam*

2003-05-03 **spam out of control law unsolicited e-mail FTC Orson Swindle**

NewsScan

SPAM OUT OF CONTROL — BUT LAW IS NOT THE ANSWER
Eileen Harrington, the director of the Federal Trade Commission's marketing practices, that the problem of spam (bulk unsolicited e-mail) is "worse than we imagined. There is consensus that the problem has reached a tipping point. If there are not immediate improvements implemented across the board by technologists, service providers and perhaps lawmakers, e-mail is at risk of being run into the ground." Legislators at both federal and state levels have been busy enacting or proposing new laws, but FTC Commissioner Orson Swindle remains skeptical: "New laws that are unenforceable for myriad reasons or that are overtaken by the advances of technology have the potential to do more harm than good. No single law, no single new technology, no new initiative, no new meetings are going to solve this problem alone." And John Patrick, chairman of the industry-supported Global Internet Project, agrees, saying that the only solution to spam is to block it with new technology. (AP/Atlanta Journal-Constitution 3 May 2003)

Category 4A7 Spam

2003-05-07 **earthlink buffalo NY spammer spamage accounts 825 million messages award**

NewsScan

EARTHLINK AWARDED $16M IN SPAMAGES
A federal judge awarded Earthlink $16.4 million in damages and instituted a permanent injunction against a Buffalo, NY, man identified as the ringleader of a group that used Earthlink's network to send 825 million spam messages over the past year. Earthlink said Howard Carmack and his cronies used Internet accounts opened with stolen identities and credit cards to send junk e-mail. The ruling is the latest in a series of legal actions taken by ISPs against bulk spammers. Last year Earthlink won $25 million in damages in a suit against another bulk e-mailer, Kahn C. Smith of Tennessee, but it hasn't collected the award. The company also has several other lawsuits pending. Meanwhile, last December, America Online won a $6.9 million judgment against a now-defunct Illinois company that specialized in p*rnographic spam. Over the last few years, AOL has won 25 spam-related lawsuits against more than 100 companies and individuals, says a company spokesman. (AP 7 May 2003)

Category 4A7 Spam

2003-05-13 **spam legislation law proposal farce opt-out lobbyists industry ISPs direct mail retailers divisions subsidiaries**

WP http://www.washingtonpost.com/ac2/wp-dyn/A47350-2003May12?language=printer

W.J. "Billy" Tauzin (R-LA), head of the House Energy and Commerce Committee, and F. James Sensenbrenner Jr. (R-WI), chairman of the Judiciary Committee sponsored an effort to define federal legislation to protect spammers in response to heavy lobbying by the direct mail industry, ISPs, and retailers. Writing in the Washington Post, Jonathan Krim reported, "According to participants in at least three meetings in recent weeks, e-mail marketers prevailed in adding provisions that would supersede tougher state anti-spam laws, would prohibit consumers from suing spammers and would give companies the right to send e-mail to anyone who has done business with them in the past three years." The bill would support opt-out provisions to allow one-time spamming. In addition, every "line of business" or subsidiary could send junk e-mail and require a separate opt-out instruction from recipients.

Category 4A7 Spam

2003-05-14 **buffalo spammer identity theft forgery criminal possession howard cormack earthlink accounts**

NewsScan

'BUFFALO SPAMMER' COULD GET UP TO SEVEN YEARS
Howard Carmack, the so-called "Buffalo Spammer," has become the first person in New York state to be charged under the state's identity theft laws. If convicted, he could be sentenced to 2-1/2 to 7 years in prison for identity theft, forgery, criminal possession of forgery devices (in the form of software used to create phony return addresses), and falsifying business records. According to the indictment, Carmack "stole the identities of innocent New Yorkers to spam millions of consumers throughout New York and the nation." He is charged with using 343 stolen identities to send his unsolicited bulk mailings through Earthlink accounts. An Earthlink executive said the main impact of the arrest would be to demonstrate to others the "very high cost of doing business" in spam. (New York Newsday 14 May 2003)

Category 4A7 Spam

2003-05-23 **spam fraudulent e-mail headers spoofing lawsuits racketeering RICO law legislation**

Macworld http://maccentral.macworld.com/news/2003/05/23/antispam/

Sen. Bill Nelson (D-FL) introduced an antispam bill that would apply the Federal Racketeer Influenced and Corrupt Organizations Act (RICO) to spammers using fraudulent e-mail headers as well as allowing civil lawsuits for damages against spammers.

Category 4A7 Spam

2003-05-27 **federal law legislation private lawsuits opt-out industry lobbyists direct marketing**

PCWorld http://www.pcworld.com/resource/printable/article/0,aid,110881,00.asp

By the end of May 2003, there was a great deal of activity in the US Congress concerning Federal legislation to control spam. Antispam activists severely criticized the majority of the measures and even the concept of using laws as a defense against spam on the following grounds:

* The very definition of spam remains ambiguous;
* Most bills would explicitly supersede more severe state antispam laws, reducing pressure on spammers;
* Many of the laws preclude civil litigation for damages against spammers;
* Most of the laws are based on opting out of spam, allowing potentially huge numbers of unwanted e-mail messages to be sent to victims;
* The laws would essentially legalize spam and place the burden of stopping it on the recipients;
* Offshore spammers would be unaffected by any legislation;
* Litigation against criminal spammers using false identification would remain difficult.

Category 4A7 Spam

2003-06-11 **FTC fight spam Federal Trade Commission ICPEA FBI criminal databases foreign servers overseas**

NewsScan

June 11, CNET News.com — FTC seeks broad powers to fight spam. The Federal Trade Commission (FTC) Wednesday asked Congress for sweeping new powers that would let it cooperate closely with governments abroad and prosecute domestic and overseas spammers more readily. The International Consumer Protection Enforcement Act (ICPEA), a 13-page proposal drafted by the FTC, would turn the agency's investigators into virtual spam cops, granting them the power to serve secret requests for subscriber information on Internet service providers, peruse FBI criminal databases and swap sensitive information with foreign law enforcement agencies. "A recent study by the commission found that 66 percent of spam contained obvious indicia of falsity," the FTC's five commissioners said in a joint statement to Congress released Wednesday. "Moreover, a significant portion of spam is likely to be routed through foreign servers."

Category 4A7 Spam

2003-06-11 **FTC Spam fight new powers U.S. Federal Trade Commision**

NewsScan

FTC ASKS FOR NEW POWERS TO FIGHT SPAM
U.S. Federal Trade Commission Chairman Timothy Muris is asking Congress to broaden the FTC's authority to investigate and prosecute spammers. The request follows congressional hearings on the subject and an FTC study concluding that two-thirds of spam is fraudulent or misleading. Meanwhile, several bills to fight spam have been introduced in Congress, the frontrunner of which is sponsored by Rep. W.J. Tauzin (R-La.), chairman of the House Energy and Commerce Committee. Tauzin's proposed legislation would require e-mail marketers to reveal their true e-mail addresses, honor consumer requests to be removed from mailing lists, and require that p*ornographic spam be labeled as such. The bill would authorize ISPs, state attorneys general and federal law-enforcement officials to track down suspected spammers and would allow fines up to $1.5 million and jail time up to two years for guilty parties. Consumer groups have criticized the Tauzin bill, saying it would override tougher state laws and is full of loopholes. (Wall Street Journal 11 Jun 2003)

Category 4A7 Spam

2003-06-17 **spam civil lawsuit litigation harvesting addresses deceptive subject lines pornography children**

http://www.microsoft.com/presspass/features/2003/jun03/06-17SpamEnforcement.asp

In May and June of 2003, Microsoft launched an assault again spammers by filing 13 civil suits in US and two in the UK. The lawsuits included complaints about deceptive subject lines and harvesting e-mail addresses. Tim Cranton, a senior attorney at Microsoft, said in an interview, "We're focusing our efforts on the type of spam that troubles our customers the most: consumer deception and unsolicited pornography. Deceptive spam includes e-mail that uses misleading information — either about who sent the e-mail or what the e-mail is regarding — to trick the recipient into opening the mail because they think it's something that it isn't. These often come in the form of get-rich-quick schemes, adult services or purported health offerings. An FTC study found that an estimated 66 percent of spam has some type of false information, so this is a huge problem that must be addressed. Another significant customer concern is unwanted, sexually explicit material that may reach children or that is otherwise offensive to recipients who did not request to receive such material."

Category 4A7 *Spam*

2003-06-18 **microsoft sues spammers msn hotmail**

NewsScan

MICROSOFT SUES 15 SPAMMERS
Estimating that more than 80% of the 2.5 billion e-mail messages sent each day to customers of its free Hotmail service are the work of spammers, Microsoft has filed lawsuits against 15 groups of individuals and corporations it claims are major spammers. Like many Internet companies, Microsoft is also looking for technological solutions to the problem of spam. It has already introduced anti-spam software filters on its MSN Internet access service, and plans to include similar software at the next release of its Outlook e-mail software. (New York Times 18 Jun 2003)

Category 4A7 *Spam*

2003-06-20 **against spammers legislate bill law false e-mail headers subject lines**

NewsScan

SENATE TRIES AGAIN TO LEGISLATE AGAINST SPAMMERS
The Senate Commerce Committee has unanimously approved a bill that would make it illegal for any person or company to use fraudulent or deceptive return e-mail address, false e-mail headers, or false and misleading subject lines. The bill, if passed into law, will also require that all e-mail marketing messages label those messages as advertisements, provide the sender's physical address, and offer a way for recipients to decline to receive any further messages from the marketer who sent them. (New York Times 20 Jun 2003)

Category 4A7 *Spam*

2003-07-01 **anti-spam bill law legislations Consumer Union**

NewsScan

FEDERAL ANTI-SPAM BILLS WON'T DO THE TRICK
The legal counsel of the Consumers Union, which publishes Consumer Reports, has told a U.S. House subcommittee that the anti-spam legislation Congress is considering is insufficient, because it places too much burden on consumers: "Thus far, the bills proposed, including H.R. 2214, have an 'opt-out' as part of their core solution. In other words, an Internet service provider must first pass on the spam to consumers, consumers must then read the spam, and then they can exercise their right to stop receiving messages from that particular sender... This puts too much burden on consumers to block spam and makes it too difficult to hold spammers legally accountable for their inappropriate interference with consumers' e-mail." (TechWeb 9 Jul 2003)

Category 4A7 *Spam*

2003-07-18 **spam legislaltion anti-spam laws Congress e-mail**

NewsScan

WHY ARE SPAMMERS BACKING SPAM-CONTROL LAWS?
Bigtime spam-mongers and junk-mail proponents like the Direct Marketing Association are backing proposed antispam legislation, while consumer and public-interest groups, almost without exception, oppose the bills. What's going on? "It's a sign of who benefits from these bills and who doesn't," says a spokesman for the Coalition Against Unsolicited Commercial Email. "When you see some of the biggest spammers in the country backing legislation that is allegedly antispam, you really need to wonder about what these bills actually do." The answer is that rather than banning all unsolicited e-mail outright, as many consumer groups wish, they legitimize spam, as long as the perpetrators adhere to certain rules, such as using accurate subject lines and valid return addresses, and allowing recipients to opt out of future mailings. Two bills are currently making their way through Congress and a variant of thereof is expected to pass overwhelmingly and be signed into law later this year. (Wall Street Journal 18 Jul 2003)

Category 4A7 *Spam*

2003-07-23 **anit-spam legislation Australia new law**

NewsScan

GOOD LUCK: AUSTRALIA CONSIDERS NEW LAW TO BAN SPAM
Australia's federal government plans to introduce legislation to end unsolicited commercial email by banning the "sending of commercial electronic messages without the prior consent of end-users unless there is an existing customer-business relationship"; imposing a range of penalties for breaking this law including fines, infringement notices and the ability to seek injunctions; requiring all commercial electronic messages to include a working opt-out mechanism and the sender's accurate contact details; banning the use of e-mail address harvesting software; and cooperating with overseas organizations to develop international guidelines and mechanisms to battle spam. The legislation would be enforced by the Australian Communications Authority (ACA). Jodie Sangster of the Australian Direct Marketing Association (ADMA) urges caution: "This is an issue where if they get it wrong could have a huge impact on business, particularly small businesses. For that reason, it's in the government's interest to make sure they fully consult and take into account the businesses it's going to impact on." (ZDNet 23 Jul 2003)

Category 4A7 *Spam*

2003-07-23 **anit-spam legislation support lawsuits FTC**

NewsScan

CONSUMERS SUPPORT LEGISLATION ANTI-SPAM LEGISLATION
A recent poll conducted by ePrivacy Group confirms a tidal wave of consumer sentiment against spam: 74% of respondents said they support a "do not e-mail" list and 59% said spammers should be punished. Of those who supported punishment, 80% said they favored consumer lawsuits against spammers. The news comes as no big surprise, but bolsters current efforts in Congress to pass legislation restricting unsolicited commercial e-mail. There are two bills currently moving through the legislative process: one introduced by Sen. Charles Schumer (D-N.Y.), which advocates creating a "do not e-mail" list and allows consumer lawsuits, and another sponsored by Sens. Conrad Burns (R-Mont.) and Ron Wyden (D-Ore.), which would direct the Federal Trade Commission to investigate the feasibility of a "do not e-mail" list. (Wall Street Journal 23 Jul 2003)

Category 4A7 *Spam*

2003-07-23 **spam law legislation opt-in do-not-spam list FTC**

NWF http://www.nwfusion.com/cgi-bin/mailto/x.cgi

Sen. Charles Schumer (D-NY) supported his introduction of the Stop Pornography and Abusive Marketing (SPAM) Act by releasing results of a survey of 1,093 U.S. Internet users polled by the ePrivacy Group. Respondents

* supported a national do-not-spam list (74%),

* agreed that unwanted e-mail should be banned or limited by law (79%), and

* said spammers should be punished (59%).

Critics of the do-not-spam list, including FTC staffers, worried that the list would simply become a source of e-mail addresses for spammers to abuse. Many doubted that spammers would pay any attention to such restrictions.

Category 4A7 *Spam*

2003-08-26 **spam Amazon lawsuit sue e-mail unsolicited**

NewsScan

AMAZON SUES SPAMMERS
Amazon.com has filed federal lawsuits against 11 e-mail marketers it accuses of faking their e-mail addresses to appear as though the messages were sent by Amazon (a practice that is known as "spoofing" and is linked with spam abuses). The research firm IDC predicts that half of all external corporate e-mail — more than 2 trillion messages this year — will be spam. (USA Today 26 Aug 2003)

Category 4A7 *Spam*

2003-08-27 **spam Earthlink lawsuit sue e-mail unsolicited**

NewsScan

EARTHLINK SUES SPAMMERS
EarthLink, the third largest U.S. Internet service provider, has sued 100 spammers located mostly in Alabama and Canada, alleging they used stolen credit cards, identity theft and banking fraud to pay for Internet accounts used to send out more than 250 million junk e-mails. The spammers eluded detection for about six months by creating bogus accounts and leasing phone lines that would automatically connect to EarthLink, even if the bogus users were kicked off. "Our investigation has been ongoing for a number of months, and this is a very tech-savvy spam ring which has made this a particularly challenging investigation," says Karen Cashion, lead counsel for EarthLink's lawsuit. The spam messages included ads for herbal impotence treatments, mortgage loans and fake company Web sites used for "phishing" personal and financial information from unsuspecting victims. EarthLink says it is still working to identify each spammer (the lawsuit lists the Alabama culprits as John Does 1-25), but plans to contact law enforcement officials once it can finger individuals. (AP 27 Aug 2003)

Category 4A7 *Spam*

2003-09-18 **spam UK criminal offense stephen timms law EU legislation unsolicited junk e-mail**

NewsScan

UK MAKES SPAM A CRIMINAL OFFENSE
A new law introduced by U.K. Communications Minister Stephen Timms means spammers could face fines of £5,000 in a magistrates court or an unlimited penalty from a jury. "These regulations will help combat the global nuisance of unsolicited e-mails and texts by enshrining in law rights that give consumers more say over who can use their personal details," says Timms. The law, which takes effect December 11, follows similar steps taken by the Italian government, which recently imposed fines of up to 90,000 euros and a maximum sentence of three years in prison for sending spam. Meanwhile, EU legislation banning unsolicited junk e-mail will be enforced beginning on October 31, but officials say it may have little effect because most spam originates in the U.S. and Asia, and thus will be out of its reach. (BBC News 18 Sep 2003)

Category 4A7 *Spam*

2003-09-24 **spamming california anti-spam law marketing companies**

NewsScan

CALIFORNIA SPAMMIN'
California's new anti-spam law may face the same fate as a similar law in Utah earlier this year. Kevin Johnson of the e-mail marketing company Digital Impact warns: "Hard-core spam will still come through, but legitimate companies will be more hesitant to send e-mail"; he also warns that when companies try to determine whether e-mail recipients live in California, spammers and advertisers may be forced to learn more about consumers, thereby reducing privacy. E-mail marketer Trevor Hughes suggests that the only answer is national legislation to harmonize spam laws in more than 30 states. (USA Today 24 Sep 2003)

Category 4A7 *Spam*

2003-10-04 **anti spam legislation e-mail**

NewsScan

SENATORS INTRODUCE ANTI-SPAM BILL
Senators Conrad Burns (R-Mont.) and Ron Wyden (D-Ore.) have introduced legislation that seeks to cut down on junk e-mail by requiring Internet marketers to provide legitimate return addresses on their e-mail and to honor consumers' requests to be taken off e-mail distribution lists. "This bill will help to keep legitimate Internet traffic and e-commerce flowing by going after those unscrupulous individuals who use e-mail in annoying and misleading ways," said Wyden in a statement. The bill would not allow individuals to sue spammers directly, but would require that state attorneys general sue on their behalf. The Federal Trade Commission could also fine violators, and ISPs could block spammers from their networks. The average U.S. Internet user received more than 2,200 spam messages last year, according to Jupiter Research, and the UK government said last month that spam now accounts for 40% of global e-mail traffic. A similar bill sponsored by Burns and Wyden cleared the Commerce Committee last year, but was not taken up for a vote in the Senate. "Now it's time to move forward. This legislation has been on hold for too long," says Burns. (Reuters 10 Apr 2003)

Category 4A7 *Spam*

2003-10-23 **spam OK Senate litigation laws**

NewsScan

SENATE VOTES TO CAN SPAM
The U.S. Senate has unanimously approved the "Can Spam" bill, sponsored by Sens. Conrad Burns (R-Mont.) and Ron Wyden (D-Ore.), which would ban the sleaziest techniques used by spammers to spew out millions of junk e-mail messages each day. Under the provisions of the bill, senders of unsolicited e-mail would be prohibited from disguising their purpose by using a fake return address or misleading subject line, and would no longer be allowed to harvest e-mail addresses off the Web to bulk up their lists. In addition, junk e-mail would be required to include a legitimate "opt out" function that recipients could use to get off lists. A provision proposed by Sen. Charles Schumer (D-N.Y.) authorizes the Federal Trade Commission to establish a "do-not-spam" list, similar to the recently implemented "do-not-call" list that blocks telemarketing calls. "Kingpin spammers who send out e-mail by the millions are threatening to drown the Internet in a sea of trash, and the American people want it stopped," said Wyden, who urged foreign countries to adopt similar measures. (AP 23 Oct 2003)

Category 4A7 *Spam*

2003-10-28 **spam privacy opt-out Web**

NYT http://www.nytimes.com/2003/10/28/technology/28SPAM.html?th

The CAN-SPAM antispam bill passed by the Senate may do little to stop legitimate companies from sending so-called white-collar spam.

Category 4A7 *Spam*

2003-11-26 **Can Spam Act Anti-Spam Bill House Senate President Bush filters**

NewsScan

ANTI-SPAM BILL PASSES IN HOUSE, SENATE
The Senate passed a bill to curb junk commercial e-mail by voice vote on Tuesday, and the House passed a similar measure on Saturday by a vote of 392 to 5. President Bush is expected to sign the legislation (known as the "Can Spam" Act) once the two bills are reconciled. Many are skeptical. California state Democrat senator Debra Bowen says, "The bill doesn't can spam, it legalizes it. It's full of loopholes. It's difficult to enforce. It's weaker than many state laws." And telecom attorney Charlie Kennedy advised: "The best line of defense for consumers are the antispam filters which are available commercially." (New York Times 26 Nov 2003)

Category 4A7 *Spam*

2003-12-09 **congress anti-spam bill five years prison commercial e-mail identity**

NewsScan

CONGRESS PASSES ANTI-SPAM BILL
Congress has passed anti-spam legislation that would supplant tougher anti-spam laws already passed in some states. The bill encourages the Federal Trade Commission to create a do-not-spam list of e-mail addresses and includes penalties for spammers of up to five years in prison. The legislation would prohibit senders of unsolicited commercial e-mail from disguising their identities by using a false return address or misleading subject line, and would require them to let recipients say they do not want future mass mailings. (Los Angeles Times 9 Dec 2003)

Category 4A7 *Spam*

2003-12-10 **anit-spam legislation reply-to FTC**

NewsScan

December 09, Associated Press — New anti-spam legislation compels consumers to hit 'reply' to e-mails. As the deluge of unsolicited pitches worsened during the Internet's growth, experts have cautioned computer users against doing what comes naturally: Reply to unwanted e-mails to demand an end to them. The reason? Unscrupulous spammers deem each such demand a verification that someone actually received their e-mails—and promptly sent dozens more to the same address. But the "can spam" legislation that Congress approved Monday requires unsolicited e-mails to include a mechanism so recipients could indicate they did not want future mass mailings. The legislation also will prohibit senders of unsolicited commercial e-mail from disguising their identity by using a false return address or misleading subject line, and it will prohibit senders from harvesting addresses off Websites. President Bush has indicated he intends to sign the measure into law. Indeed, the White House revamped its own e-mail system this summer over a flood of so-called spam. The anti-spam bill encourages the Federal Trade Commission to create a do-not-spam list of e-mail addresses and includes penalties for spammers of up to five years in prison in rare circumstances.

Category 4A7 *Spam*

2003-12-12 **anti-spam law virginia unsolicited mass e-mailing Internet History Eraser Pornographic Sites**

NewsScan

FIRST INDICTMENTS UNDER VIRGINIA ANTI-SPAM LAW
The state of Virginia has lodged criminal indictments against two people charged with making unsolicited mass e-mailings; it's the first case to be brought under a new antispam law in that state. Prosecutors say that in a one-month period last summer more than 100,000 AOL subscribers clicked a "report spam" button to complain about messages sent by the two defendants. The e-mail messages, sent with fake return addresses, contained information about stock-picking methods, mortgages and "Internet history eraser" software for deleting evidence that a user had visited pornographic sites. (New York Times 12 Dec 2003)

Category 4A7 *Spam*

2003-12-16 **anti-spam law George W. Bush e-mail marketing CAN-SPAM bill**

NewsScan

BUSH SIGNS NATIONAL ANTI-SPAM LAW
A new law signed by President Bush will attempt to rid the Internet of unsolicited commercial e-mail ("spam") — though many technology experts believe it will not be impossible for legislation passed by a single country to eliminate spam, because it is a global problem. However, supporters of the legislation say it gives state and federal law authorities the tools needed to track down and prosecute the largest and best-organized spammers. Democrat Senator Ron Wyden of Oregon, a coauthor of the CAN-SPAM bill, explains: "Our message is the fight has just begun and enforcement has got to be tough, tough, tough." (Washington Post 16 Dec 2003)

Category 4A7 *Spam*

2003-12-18 **spammers civil suits Scott Richter's OptInRealBig e-mail marketing**

NewsScan

CIVIL SUITS AGAINST SPAMMERS
New York State and Microsoft are filing civil lawsuits suits against prominent e-mail marketing operations, including Scott Richter's OptInRealBig. The lawsuits will attempt to hold responsible not just those accused of actually sending spam but also those who financially benefit from it. Richter, who has stoutly and publicly defended his marketing practices, says he's unconcerned about the lawsuits: "Messing with us is a big mistake. The more press I get, even bad press, the bigger we get." (New York Times 18 Dec 2003)

Category 4A7 *Spam*

2003-12-19 **spammers new york Eliot Spitzer bankruptcy Synergy6 Delta Seven OptInRealBig**

NewsScan

NEW YORK, MICROSOFT TARGET SPAMMERS
New York Attorney General Eliot Spitzer has filed a civil lawsuit against three top spam firms, threatening to seek penalties so large it would drive the companies out of business: "We will drive them into bankruptcy. Therefore, others will not come into the marketplace because they will see there is no viable business model here." The companies under fire are OptInRealBig, of Westminster, Co.; Synergy6, a New York marketing firm; and Delta Seven, a Dallas mailing company whose co-owner has already filed for bankruptcy protection. In addition to spewing spam, prosecutors have accused Delta Seven of obscuring the messages' origin by breaking into computers owned by others — including an elementary school in Korea and the Kuwaiti ministry of finance — to send the mail. Meanwhile, Microsoft has jumped on the anti-spam bandwagon with its own suit filed in Washington State seeking $18.8 million in damages caused by overloading its Hotmail service with junk e-mail. "Any money that is left over after the attorney general's suit, we will happily go after," says Microsoft general counsel Bradford L. Smith. (New York Times 19 Dec 2003)

Category 4A7 *Spam*

2003-12-28 **spam politicians legislators unsolicited non-commercial e-mail exemption CAN-SPAM**

http://www.nytimes.com/2003/12/28/politics/28EMAI.html?th=&pagewanted=print&position=

While they were passing the CAN-SPAM Act, members of Congress sent out hundreds of thousands of junk e-mail messages to constituents, buying e-mail addresses from spam-suppliers, and exempted their own junk e-mail from coverage by the CAN-SPAM Act, which applies to commercial junk but not to political junk.

Category 4A7 *Spam*

2004-01-11 **anti spam law ineffective guidelines junk e-mail**

NewsScan

ANTI-SPAM LAW ENACTED — SO WHAT'S ALL THIS JUNK IN MY IN-BOX?

The new federal anti-spam law went into effect Jan. 1, but consumers report their inboxes are more cluttered than ever — what's going on? Critics say the new law doesn't actually ban spam but rather provides guidelines for sending junk e-mail legally. "Now we have a green light for what would come to be called 'legal spam,'" says ePrivacy Group CEO Vincent Schiavone. John Levine, a board member of the Coalition Against Unsolicited Commercial E-Mail, concurs: "Basically, it's a bill of rights for companies that want to send junk e-mail." In addition, the federal law supercedes stricter laws recently passed in several states, such as California. "Everyone was planning for this California law, which was so draconian," says a California lawyer who defends accused spammers. "Once the federal government passed the federal law, everyone was kind of relieved." And while technology firms are eagerly pursuing new ways of blocking spam, skeptics say the ultimate solution won't be technological or legal, but will depend on developing more savvy users. Mary Youngblood, abuse team manager at EarthLink, suggests putting numbers in the middle of your e-mail address to make it more difficult to guess and using a separate address for online shopping and newsgroup postings. (AP Jan 11 2004)

Category 4A7 *Spam*

2004-01-20 **anti spam CAN act ineffective**

NewsScan

ANTI-SPAM LAW LARGELY IGNORED

The new federal anti-spam law ("Can Spam") doesn't seem to being changing the practices of the largest spammers: most of the largest bulk e-mailers are continuing to send illegal mass mailings for porn, get-rich-quick schemes and miracle drugs. The spam-filtering company Brightmail says that about 58% of e-mail monitored in January has been spam, in defiance of the new law, which took effect at the beginning of this month. The only real impact of the law seems to have been felt by small businesses, many of which have decided to discontinue e-mail marketing. One business, calculating that it would cost $100,000 a year in personnel and technology to make its e-mail system comply with the law, decided to switch its advertising campaigns to Microsoft MSN and Yahoo. (USA Today 20 Jan 2004)

Category 4A7 *Spam*

2004-01-29 **FTC spam relay user responsible secure servers software**

NewsScan

FTC WARNING PUTS ONUS ON COMPUTER USERS

The Federal Trade Commission and regulatory agencies in 26 countries have sent out letters to hundreds of thousands of computer users, warning them that spammers are lurking in cyberspace, waiting for the opportunity to hijack their servers and route junk e-mail through them. Spammers often use unsecured computers to disguise the origin of their messages. "Recipients may think the spam comes from your system," said the FTC's e-mail message. "Securing your server will help you protect your system from being misused." Don Blumenthal, coordinator for the FTC's Internet lab, admitted the agency did not attempt to verify that each computer targeted by the warnings was actually vulnerable to hacking, but said the message urged recipients to visit the FTC Web site for more information on properly configuring their software. (AP 29 Jan 2004)

Category 4A7 Spam

2004-02-03 **antispam law legislation bill CAN-SPAM**

NWF http://www.nwfusion.com/newsletters/sec/2004/0202sec1.html

Can CAN-SPAM Can Spam?

By M. E. Kabay, PhD, CISSP

On January 1, 2004, The CAN-SPAM Act of 2003 took effect in the United States. The Act is formally entitled, "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003" and was introduced as S. 877 (passed Nov 25, 2003) and accepted by the House on Dec 8, 2003 [1].

Critics have consistently attacked the law as inadequate to control spam on the following grounds [2]:

1. The Act is based on an opt-out philosophy. Anyone can send one junk e-mail message legally as long as they offer an opt-out procedures. However, it is widely believed that many or most of the people who send spam value opt-out replies because they validate addresses. They then sell those addresses to other spammers. As a result, many people will be reluctant to use opt-out mechanisms. In any case, there are more than 20 million businesses in the USA today [3], so if every one of them chose to send a user exactly one message per year at random, a user could expect an average of over 54,000 messages requiring an opt-out response per day. If only 1% of these businesses chose to send out junk e-mail, the daily average would be 500 or more new junk messages requiring an opt-out.

Section 5(a)(3)(A) requires spammers to provide an opt-out mechanism, but describes these mechanisms broadly as including "a manner specified in the message, a reply electronic mail message or other form of Internet-based communication. . . ."

As pointed out by blogger Ed Foster, this section means that a spammer could create an opt-out mechanism requiring an unwilling recipient to log on to a Web site and search for opt-out instructions, possibly while being bombarded by pop-up ads [4]. Can you imagine having to log on to Web site after Web site to unsubscribe from drivel you never asked for and detest on sight? Think of the time involved. Furthermore, Web-based opt-out instructions permitted under this law will make it difficult for automated systems to unsubscribe victims of spam using such mechanisms. [Note from MK: I remember one spammer who demanded that his victims _solve a puzzle_ in order to be freed from his waves of, ah, e-xcrement.]

2. Section 9 of the Act mandates a Do-Not-E-Mail Registry for no later than July 2004 but provides no details on how such a registry would be created and updated, how it would be protected against abuse by spammers, which government agency would control it or how it would be used to limit spam.

3. The Act defines "commercial electronic mail message" as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose)." This definition thus permits spam from politicians, political groups, religious organizations, charities, hate groups, hobbyists, cranks, and anyone else so long as the content cannot be construed as "commercial" (which is itself not defined in the Act).

4. CAN-SPAM overrides more restrictive state laws, weakening the range of legal countermeasures against spammers in the USA.

5. Nothing in the Act resolves the problem of spam directed against US residents but originating outside the boundaries of the USA.

By mid-January, anti-spam campaigners were confirming their pessimistic impression of the law's effectiveness. According to Jan Libbenga of _The Register_, "The NANAS sightings newsgroup (a large collection of spam, updated continuously) doesn't contain one spam message that is CAN SPAM compliant." [5]

Let's hope for some successful prosecutions of spamming soon with some stiff penalties. Until then, I'm sorry to say that I doubt that this law will have any helpful effect on spam.

* * *

Category 4A7 Spam

2004-02-17 **spam laws strategy analysis**

Network World Fusion
http://www.nwfusion.com/newsletters/sec/2004/0223sec1.html

Can Laws Block Spam?

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

I just read a new White Paper from Montreal-based Vircom, developer of Modus secure messaging solutions, on recent international anti-spam legislation efforts. Entitled, "Can Laws Block Spam?" the paper uses interviews with five experts on spam:
* Lindsay Barton, Manager, Online Policy at the National Office for the Information Economy of Australia;
* Anne P. Mitchell, Esq., President/CEO, Institute for SPAM and Internet Public Policy and Professor of Law, Lincoln Law School of San Jose, California;
* Michael D. Osterman. President and Founder, Osterman Research
* Troy Rollo, Chairman of the Coalition Against Unsolicited Bulk Email in Australia and Executive Director of the International Coalition Against Unsolicited Commercial Email
* Neil Schwartzman, Editor & Publisher spamNEWS, Chair, Canadian Coalition Against Unsolicited Commercial Email

The paper analyzes the CAN-SPAM act in reasonable detail, but this column has already pointed readers to that legislation and analyses of its weaknesses. More interesting here is the analysis of the European Community Directive on Privacy and Electronic Communication Regulation 2003. This legislation provides for opt-in (not opt-out) restrictions on sending junk e-mail. Much as with fax messaging, no one may initiate e-mail marketing without prior permission or prior business relationship – and there must be an easy way to refuse future junk e-mail at the time of initial data collection about an individual. In addition to enforcement actions initiated by the Information Commissioner in law courts, victims of spam may also sue for damages of up to £5,000 in cases heard before a judge (unlimited if heard before a jury). However, critics point out that the law does not regulate business-to-business spam, including spam sent to employees via their business e-mail addresses.

Another section covers the Australian Spam Act of 2003, which includes not only e-mail spam but also SMS (Simple Message System) junk messages. This law also uses an opt-in strategy, in contrast with the US approaches that depend on opt-out methods. There are also clauses dealing with proper (accurate) origination addresses and restrictions on harvesting e-mail addresses automatically. Penalties are potentially much higher than in the US or in Europe: "Civil penalties under the Act will be assessed according to a sliding scale for repeat offenders. An individual could be liable for up to a total of A$44,000 … for contravention on a single day, while an organization could be fined up to $220,000 AUD in a day. Offenders with a prior record will be penalized up to a maximum of A$220,000 … for each day of spamming by an individual, and A$1.1million … per day for organizations."

Although the Australian law has many admirable features, it founders on the reef of international spam. As commentators note in the White Paper, national laws will inevitably fail to control spam sent from outside their borders. According to a UNCTAD (United Nations Conference on Trade and Development) report on the origins of spam in 2003, the sources were
58.4% USA
5.6% China
5.2% UK
4.9% Brazil
4.1% Canada
21.8% Other

[On a side note, I have been receiving the most amazing junk e-mail from China lately – ads in comically bad English for everything from inflatable dolls the size of buildings to industrial flooring components and chemicals. Given that China has one quarter of the world's population and an economy that is growing at 9-11% per year, this trickle bodes very badly for the future of our inboxes.]

I think Michael Osterman summed up the situation well in his commentary: "Spam legislation, while well intended, will not control spam alone. The only answer is to fight spammers with the same weapon they use: technology. The problem with spam will be better faced by IT staff then by legislators. To control spam, it must be rendered economically non-viable. Now that is difficult to achieve because it costs virtually nothing to send; however, if we can increase the cost of sending a spam message, we can make it nonviable and the only way we can do that is through the increased use of anti-spam tools. . . . When anti-spam filters are effective they can eliminate 95% or more of the incoming spam, "...If an anti-spam filter can stop 95% of the spam that reaches an end user, the cost to the spammer of reaching that potential customer has risen by 20 times. Increasing the effectiveness of these filters to 97% increases the cost to the spammer by 33 times. The hope is that the potential revenue available to spammers drops by a corresponding amount, and equilibrium is reached."

Category 4A7 Spam

2004-02-18 **spam AOL Earthlink Thailand route e-mail conspiracy theory**

NewsScan

CONSPIRACY THEORY

Lawsuits filed yesterday by AOL and Earthlink accuse individuals and companies of running spam networks. The AOL suit alleges a conspiracy between three Floridians and two Americans living in Thailand to route mortgage-scam solicitations to AOL customers and to defeat AOL's spam filters through a company called Connor-Miller Software Inc. Earthlink is accusing 16 individuals and companies in Florida, California, Tennessee and Michigan of operating a multi-state spam operation that has sent more than a quarter of a billion e-mail messages promoting herbal supplements, Viagra and adult dating services and of using stolen identity documents to open Earthlink Internet accounts that were used to transmit the spam. The attorney who represents the Florida defendants in the AOL lawsuit argues that his clients are innocent of spamming: "They set up a network, just like AOL is a network." (Washington Post 18 Feb 2004)

Category 4A7 Spam

2004-02-23 **anti-spam act Australia April 2004**

NewsScan

AUSTRALIAN SPAM ACT STARTS IN APRIL

The Australian Spam Act 2003 comes into force in April. The National Office for the Information Economy (NOIE) has produced helpful guidelines for business on how they should approach the sending of commercial electronic messages. The guidelines focus on compliance with the new legislation. (Spam Act 2003: Guides and Information Sheets Feb 2004)

Category 4A7 Spam

2004-03-10 **CAN-SPAM lawsuit spammers e-mail caller-ID address authentication spoofing**

http://www.nwfusion.com/news/2004/0310microtoan.html

In March 2004, Microsoft, Yahoo and AOL announced lawsuits against spammers under the CAN-SPAM Act. In addition, they proposed technical measures to interfere with spoofing of e-mail addresses — what they termed Caller ID e-mail specification.

Category 4A7 Spam

2004-03-10 **anti-spam lawsuit ISPs legislation Microsoft Earthlink Yahoo**

NewsScan

ISPs SUE SPAMMERS UNDER CAN SPAM LEGISLATION

Teaming up in an unusual joint effort, Microsoft, MSN, EarthLink and Yahoo have filed six lawsuits against hundreds of people who allegedly have sent millions of spam e-mail messages through the plaintiffs' e-mail networks. The lawsuits mark the first legal action taken under the Can Spam legislation, which took effect on Jan. 1. "Congress gave us the necessary tools to pursue spammers with stiff penalties, and we in the industry didn't waste a moment moving with speed and resolve to take advantage of the new law," says AOL executive VP Randall Boe. Among the named defendants are Davis Wolfgang Hawke and Braden Bournival, both of whom are accused of sending millions of e-mails touting weight loss supplements, personal "lie detectors" and other products. Dozens of others are identified only as "John Doe" defendants. (AP/Wall Street Journal 10 Mar 2004)

Category 4A7 Spam

2004-04-29 **CAN-SPAM law legislation prosecution**

http://www.nwfusion.com/news/2004/0429canspam.html

In April 2004, two large spammers, Phoenix Avatar of Detroit MI and Global Web Promotions operating in Australia and New Zealand, were charged with violations of the CAN-SPAM Act. Phoenix Avatar officials were arrested for failing to include an opt-out address or a valid postal address in their junk and for using fraudulent FROM addresses. In addition, the accused mail fraud charges in federal court. The southern-hemisphere spammers were traced to buy cooperation with Australian and New Zealand authorities. All of the cases involved buying the bogus products and tracing money transfers to catch the crooks. Howard Beales, director of the FTC's Bureau of Consumer Protection, explained, "Rather than try to trace the e-mail, we tried to trace the money. It's virtually impossible to trace the spam itself."

Category 4A7 *Spam*

2004-05-01 **Australian spammer FTC pornographic marketing CAN-SPAM Act**

NewsScan

U.S. TAPS AUSSIE SPAMMER

The U.S. government has launched its first criminal case against spammers, and taken civil action against an Australian spammer with the help of local authorities. The U.S. Federal Trade Commission says that the first charges have been brought against several U.S. companies under Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act, which took effect in January. It also has served legal notices on Australian company Global Web Promotions Pty Ltd, which investigators said pitched fraudulent weight-loss and growth-hormone products. The FTC says it brought its case with help by the Australian Competition and Consumer Commission and the New Zealand Commerce Commission. ACCC spokeswoman Lin Enright confirmed the ACCC assisted the FTC in tracking down Global Web Promotions, but would not say whether it would have a continuing role in the matter. (The Australian 30 Apr 2004, rec'd from John Lamp, Deakin University)

Category 4A7 *Spam*

2004-05-19 **FTC explicit labels e-mail pornographic adult content subject line graphc bars**

NewsScan

FTC DEMANDS "EXPLICIT" LABEL FOR "EXPLICIT" MATERIAL

A new Federal Trade Commission rule requires that unsolicited commercial e-mail containing adult-oriented material include a special label in the subject line; it also bars graphic images from appearing in the opening body of the message (to force a recipient to take at least some positive action to see the material he or she has been warned about in the subject line). FTC attorney Jonathan Kraden says the label should help the computers to filter if a computer user decides to set their filtering system up to recognize the label, but First Amendment lawyer Jonathan L. Katz warns: "This is a back-door effort to violate people's First Amendment rights, whether well-intentioned or not." Spammers who violate the rule face possible imprisonment and criminal fines of up to $250,000 for individuals and $500,000 for an organization. (AP/San Jose Mercury News 19 May 2004)

Category 4A7 *Spam*

2004-05-20 **CAN-SPAM law legislation volume statistics research**

NWF http://www.nwfusion.com/news/2004/0520canslaw.html

CAN-SPAM CANNED?

By May 2004, it was clear that despite the CAN-SPAM Act, the volume of spam increased in the US in the first quarter of 2004. Spammers protested that when they tried to comply with the terms of the law, ISPs like AOL blocked their unwanted e-mail even more effectively. According to a report by Grant Gross in the IDG News Service, "Spammer Ronald Scelson, president of MicroEvolutions.com, told the committee he could go back to using forged headers and defeat most spam filters. 'Does the government want us to mail legal or not?' Scelson asked. 'As long as we're doing it the right way and we're going to get blocked, interfered with and shut down, people are going to go around it.' "

Category 4A7 *Spam*

2004-05-26 **ban spam false subject lines e-mail Florida state message idea**

NewsScan

FLORIDA LAW BANS DECEPTIVE SUBJECT LINES IN E-MAIL

Legislation signed by Florida Governor Jeb Bush will allow the state's attorney general to bring civil action against anyone in Florida who sends spam e-mail with a subject line intended to give the message recipient a false idea of what the message is about. (AP/USA Today 26 May 2004

Category 4A7 Spam

2004-05-31 **spam lawsuits investigations tracing money fraud law enforcement industry cooperation**

http://www.nytimes.com/2004/05/31/technology/31spam.html?th=&pagewanted=print&position=

The fight again spam is increasingly involving traditional law enforcement investigation techniques. Because technological solutions have not yet stemmed the fetid tide of electronic slime, private investigators and police officers have been responding to spam advertisements and then tracking the money to arrest the perpetrators of scams and spam. According to Saul Hansell, writing in the New York Times, "…[T]he Direct Marketing Association has paid $500,000 to hire 15 investigators who work alongside agents from the F.B.I. and other government agencies in a program known as Project Slam-Spam…. The project has built cases against 50 spammers, which it has started to refer to federal and state prosecutors. It hopes to orchestrate a coordinated sweep of spam prosecutions and civil cases later this year to highlight the seriousness of its antispam efforts."

Category 4A7 Spam

2004-11-05 **spam guilty Virginia sentencing AOL prosecution trial Jaynes DeGroot fraud**

NewsScan; http://apnews.excite.com/article/20041105/D865NE501.html

SPAMMERS FACE CRIMINAL PENALTIES IN VIRGINIA TRIAL

Virginia prosecutors have brought to trial three North Carolina defendants in what's being billed as the nation's first felony anti-spam case. The Virginia law toughening penalties for sending junk e-mail took effect last year; if convicted, each defendant could face up to 15 years in prison and $2,500 in fines. The prosecutors allege the defendants used falsified or forged return Internet addresses to send bulk e-mail hawking penny stocks and work-at-home schemes through a server in Loudon County, Virginia, where America Online is headquartered. The defense attorneys have argued their clients were simply "marketing via the Internet," which "may be annoying to you. It is not a crime." However, anti-spam activists say the prosecution is a step in the right direction. Spammers "are folks who are fairly comfortable with playing … on the fringes of legitimacy and reality," says the general counsel for the Coalition Against Unsolicited Commercial E-mail. "But if you can attach serious jail time, they would think twice." (Washington Post 27 Oct 2004)
http://www.washingtonpost.com/wp-dyn/articles/A611-2004Oct26.html

* * *

SPAMMERS GUILTY, MAY DRAW JAIL TIME

A brother-sister duo accused in Virginia of sending junk e-mail to millions of AOL customers were convicted yesterday in the first felony prosecution of Internet spam in the U.S. Jurors recommended that Jeremy Jaynes, 30, be sentenced to nine years in prison and his sister, Jessica DeGroot, 28, be fined $7,500 after convicting them of three counts each of sending e-mail with fraudulent and untraceable routing information. A third defendant, Richard Rutkowski, 30, was acquitted. The case was the first to be brought under a tough Virginia anti-spam law that took effect last year. (AP 5 Nov 2004)

Category 4A7 Spam

2005-01-03 **spam CAN-SPAM review law failure useless legislation authentication**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A44124-2005Jan3.html

CAN-SPAM LAW GETS MIXED REVIEWS

The Can-Spam Act, signed into law on Dec. 16, 2003, was touted as a major weapon in the arsenal aimed against spam-mongers, but after a year the law has been used against only a few spammers and recent surveys show that Internet users face more spam than ever. In November, a Virginia jury recommended a nine-year jail term for a North Carolina man who earned the dubious distinction of being the first person convicted of felony spamming. (The case had been brought under Virginia's spam law, which is similar to Can-Spam but allows stiffer penalties.) However, despite this minor victory, experts agree that during the past year spam e-mails represent an everincreasing portion of users' e-mail -- up to 75% to 80% now, according to anti-spam firm Postini. The trend has resulted in most major ISPs turning to technology rather than litigation to stem the flow, and each of the four major U.S. e-mail providers is involved in a nationwide effort to develop e-mail "authentication" technology that would make it more difficult for spammers to disguise their messages. "You've got to stop [spam] from getting to the customers' machines," says Dave Baker, VP of law and public policy at Earthlink. "If you're suing a spammer, you're going after them for damage that's already been done. The biggest single element remains technology solutions. None of these companies are relying solely on litigation." (Washington Post 3 Jan 2005)

Category 4A7 *Spam*

2005-01-20 **state Georgia Slam Spam E-mail Act felony law legislation proposal**

NewsScan;
http://www.ajc.com/hp/content/auto/epaper/editions/thursday/metro_14fea5c30
687223300a9.html

GEORGIA LEGISLATION WOULD MAKE SPAM A FELONY

Georgia Governor Sonny Perdue has proposed a Slam Spam E-mail Act that would make it a felony to send more than 10,000 misleading e-mails during a 24-hour period, make large sums of money off unsolicited e-mail, or involve juveniles in sending it. Speaking at Earthlink's Atlanta headquarters, Perdue promised, "We're going to clean up spam in Georgia and put our citizens back in control of their online lives." EarthLink chief executive Garry Betty, who hosted Perdue's news conference, said that up to 80 percent of all e-mail is spam. (Atlanta Journal Constitution 20 Jan 2005)

Category 4A7 *Spam*

2005-02-01 **CAN-SPAM law ineffective e-mail statistics failure spam**

NewsScan;
http://www.nytimes.com/2005/02/01/technology/01spam.html?hp&ex=11073204
00&en=f7486f68b21cb2cc&ei=5094&partner=homepage

OOPS: 'CAN SPAM ACT' SEEMS TO BE NO-CAN-DO

The Can Spam Act went into effect in January of last year, yet unsolicited commercial e-mail on the Internet is now estimated to account for at least 80% of all e-mail sent -- a figure up from 50-60% percent of all e-mail before the law went into effect. A number of critics of the law had argued that it would make the spam problem worse by effectively giving bulk advertisers permission to send junk e-mail as long as they followed certain rules. Steve Linford, the founder of the UK-based Spamhaus Project, says the law "legalized spamming itself." The law's chief sponsor, Senator Conrad Burns (R- Montana) says the problem isn' t the law but the ineffective enforcement of the law: "As we progress into the next legislative session, I'll be working to make sure the FTC utilizes the tools now in place to enforce the act and effectively stem the tide of this burden." Anne Mitchell of the Institute for Spam and Internet Public Policy comments: "Most people say it's a miserable failure, but I see it as a lawyer would see it. To think that law enforcement agencies can make spam stop right away is silly. There's no such thing as an instant fix in the law." (New York Times 1 Feb 2005)

Category 4A7 *Spam*

2005-04-04 **Florida state spam lawsuits litigation multimillion dollars Tampa spammers Electronic Mail Communications Act CAN-SPAM**

DHS IAIP Daily; http://news.com.com/Florida+files+multimillion−
dollar+spam+s uits/2100−1030_3−5653662.html

FLORIDA FILES MULTIMILLION-DOLLAR SPAM SUITS

The Florida Attorney General's office has filed its first claims under the state's antispam law, charging two men with masterminding a scheme that marketed fraudulent online businesses via e-mail. Florida Attorney General Charlie Crist charged two Tampa residents accused of running an operation that generated over 65,000 deceptive e-mails since 2003, including 48,000 messages sent after the Florida Electronic Mail Communications Act took effect on July 1, 2004. The defendants face up to $24 million in fines. Like the federal Can-Spam Act, the Florida law prohibits the distribution of unsolicited commercial e-mail that contains false or deceptive subject information, or that is sent from invalid e-mail addresses. Under the law, violators face a penalty of up to $500 for every illegal e-mail message they send to Florida residents. "Spam is a pervasive and growing threat to unsuspecting computer users everywhere," Crist said in a statement. "The spam itself is illegal, but it is made even worse when it seeks to rip off Florida consumers. Florida's antispam law was adopted precisely to stop operations such as this one."

Category 4A7 *Spam*

2005-04-13 **Florida state victory vs. spammers lawsuit injunction Attorney General Charlie Crist antispam law**

DHS IAIP Daily;
http://www.computerworld.com/governmenttopics/government/legalissues/story/0,10801,101051,00.html?source=NLT_PM&nid=1010 51

FLORIDA WINS INJUNCTION AGAINST SPAMMERS

The state of Florida won its first victory against spam e-mail when a judge granted an injunction against two men accused of running mass e-mailing operations, the state prosecutor said Tuesday, April 12. Florida Attorney General Charlie Crist said the injunction preventing the men from sending any more deceptive e-mails was part of his department's first prosecution under an antispam law passed by the state legislature last year. The e-mails took recipients to Websites that Crist said were engaged in fraudulent or illegal activities, such as selling pharmaceuticals and cigarettes online or providing a platform for the illegal downloading of copyrighted movies. A national antispam law took effect at the start of 2004 but has done little to curb the flood of spam clogging e-mail in-boxes. Spam is estimated to account for more than 80% of all e-mail traffic, costing businesses billions a year in lost productivity and bandwidth.

Category 4A7 *Spam*

2006-01-05 **phone records sale Internet pretexting privacy law enforcement criminals**

DHS IAIP Daily; http://www.suntimes.com/output/news/cst−nws−privacy05.html 23

PHONE RECORDS ARE FOR SALE VIA ONLINE DATA BROKERS

The Chicago Police Department is warning officers their cell phone records are available to anyone -- for a price. Dozens of online services are selling lists of cell phone calls, raising security concerns among law enforcement and privacy experts. Criminals can use such records to expose a government informant who regularly calls a law enforcement official. Some online services might be skirting the law to obtain these phone lists, according to Sen. Charles Schumer (D-NY), who has called for legislation to criminalize phone record theft and use. In some cases, telephone company insiders secretly sell customers' phone-call lists to online brokers, despite strict telephone company rules against such deals, according to Schumer. And some online brokers have used deception to get the lists from the phone companies, he said. According to Schumer, a common method for obtaining cell phone records is "pretexting," involving a data broker pretending to be a phone's owner and duping the phone company into providing the information. "Pretexting for financial data is illegal, but it does not include phone records," Schumer said.

Category 4A7 *Spam*

2006-01-05 **spammer fine Florida $11.2 billion anti-spam**

EDUPAGE; http://www.wired.com/news/politics/0,69966-0.html 23

SPAMMER HIT WITH $11.2 BILLION FINE

A court has slapped a Florida spammer with an $11.2 billion fine, setting a new precedent for fines against spammers, though the ruling is unlikely to have much effect on the volume of spam. Internet service provider CIS Internet Services, which provides Internet service to parts of Iowa and Illinois, had sued James McCalla for sending more than 28 million e-mail solicitations that fraudulently used the CIS domain as the return address. In addition to the fine, McCalla is forbidden from accessing the Internet for three years. Robert Kramer III, owner of CIS, welcomed the ruling, calling it the "economic death penalty," though he acknowledged that he does not expect to receive any of the money awarded. John Mozena, co-founder and vice president of the Coalition Against Unsolicited Commercial E-mail, said this and other rulings against spammers have not had a significant effect on the total volume of spam, which he estimated continues to be about two-thirds of all e-mail traffic. What is needed, he argued, rather than current laws, which only forbid deceptive or fraudulent spam, is a prohibition against all spam.

Category 4A7 *Spam*

2006-01-09 **University of Texas UT White Buffalo Ventures dating Website spam e-mail CAN-SPAM 5th US Circuit Court of Appeals**

EDUPAGE; http://www.wired.com/news/politics/0,69981-0.html 23

HIGH COURT PASSES ON UT E-MAIL CASE

The U.S. Supreme Court has refused to hear a case involving the University of Texas (UT) and White Buffalo Ventures, which operates a dating Web site focused on UT students. In 2003, UT officials blocked 59,000 e-mails from LonghornSingles.com, saying that they violated the university's antispam policy. According to officials at the school, the overall volume of spam messages was crippling the institution's servers, and the administration had also received complaints specifically about the LonghornSingles.com e-mails. White Buffalo Ventures had ignored a cease-and-desist letter, prompting the university to block all of its messages. White Buffalo took UT to court, said that its messages complied with all provisions of the CAN-SPAM Act, and argued that the federal law should take precedence over any UT policy. In August, the 5th U.S. Circuit Court of Appeals rejected that argument, saying that the university was within its rights to block the e-mails.

Category 4A7 *Spam*

2006-01-12 **Michigan man guilty plea spamming CAN-SPAM Act Ford Unisys US Army**

EDUPAGE; http://news.com.com/2100-7350_3-6026708.html 23

GUILTY PLEA EXPECTED FROM MICHIGAN MAN FOR SPAMMING

A Detroit-area man is expected to plead guilty to violations of the CAN-SPAM Act for his part in a spam racket that prosecutors say sent millions of illegal messages over computer systems belonging to Ford, Unisys, the U.S. Army Information Center, and others. Daniel Lin plead guilty to fraud and other charges in the deal and will face up to two years in prison. Prior to the deal, Lin could have been sentenced to 10 years for his part in the spam scheme. Three other men were also charged in the original complaint in April 2004, which were the first such charges under the federal law to limit spam. The men reportedly earned about $100,000 from their spam-related activities.

Category 4A7 *Spam*

2006-01-18 **spam case judgment guilty anti-spam law**

DHS IAIP Daily; 23
http://www.cnn.com/2006/TECH/internet/01/18/internet.spam.ap/index.html

SUSPECT IN FEDERAL SPAM CASE PLEADS GUILTY

The main defendant in America's first prosecution under a 2004 federal anti-spam law pleaded guilty Tuesday, January 17, to three felony charges, federal prosecutors said. Daniel J. Lin of West Bloomfield Township, MI, faces nearly five years in prison and a fine of up to $250,000, the U.S. Attorney's Office in Detroit said. Two of the counts are fraud charges involving millions of unsolicited spam e-mails sent to computer users. The other is possession of a firearm by a felon, for guns discovered when authorities raided Lin's suburban Detroit home. He is scheduled to be sentenced May 16 in U.S. District Court in Ann Arbor, MI. Lin and three other West Bloomfield Township men were identified in court documents as being part of the massive illegal spam scheme. Court papers described a complex web of corporate identities, bank accounts and electronic storefronts used to send hundreds of thousands of e-mail sales pitches for fraudulent products. The Federal Trade Commission said angry consumers forwarded to authorities more than 490,000 e-mails from the operation from January 2004 to April 2004 -- more than from any other spam outfit worldwide during the same period.

Category 4A7 *Spam*

2006-01-24 **CAN-SPAM violator 25 years sentence California man anti-spam litigation**

EDUPAGE; http://www.internetnews.com/security/article.php/3579591 23

LATEST CAN-SPAM VIOLATOR FACES 25 YEARS

A California man has pleaded guilty to using computer "bots" to surreptitiously take control of 400,000 computers, which were used to distribute adware, spyware, and other unwanted computer code. Jeanson James Ancheta, 20, admitted to earning more than $60,000 from using the illicit system of computers and renting the system to others who used them to launch their own malicious attacks. Ancheta's actions were in violation of the federal CAN-SPAM Act, and they also caused damage to computers at the U.S. Naval Air Warfare Center and the Defense Information Systems Agency. As part of his plea agreement, Ancheta will forfeit $60,000 in cash, a BMW, and computer equipment. He will also pay $15,000 toward damages to federal computers and face a sentence of up to 25 years in prison for his actions.

Category 4A7 Spam

2006-01-26 **spam legal penalties accrue AOL lawsuit CAN-SPAM Act**

EDUPAGE; http://www.wired.com/news/technology/0,70098-0.html 23

SPAM PENALTIES ACCRUE

A federal judge has issued a summary judgment in favor of AOL in its lawsuit against a man AOL describes as "the poster child for the CAN-SPAM Act." Christopher William Smith was accused of sending billions of e-mail messages in violation of the federal statute. Smith's attorneys withdrew from the case several months after it was filed, and U.S. District Judge Claude Hilton said that Smith "refused to participate in this case, willfully disregarding...discovery obligations and failing to comply with multiple court orders." In light of Smith's behavior, Hilton issued a $5.3 million judgment against Smith, to be paid to AOL, as well as ordering him to pay $287,000 in legal fees for the ISP. Smith is currently in custody in Minnesota, waiting to be tried for criminal drug charges stemming from his operating an online pharmacy.

Category 4A7 Spam

2006-01-27 **Maryland spam law New York e-mail marketer ruling**

DHS IAIP Daily; http://www.siliconvalley.com/mld/siliconvalley/news/editorial/13728469.htm 23

MARYLAND SPAM LAW CAN BE ENFORCED, JUDGE RULES.

Spam e-mails offering home financing deals or other offers can violate Maryland law, even if they're sent from another state, a state appeals court has ruled. Court of Special Appeals Judge Sally D. Adkins sided with a law student who argued that he could sue a New York e-mail marketer who had sent him advertising messages. The decision, issued Thursday, January 26, overturns a lower court ruling that Maryland's 2002 Commercial Electronic Mail Act was unconstitutional because it sought to regulate commerce outside state borders. Adkins, in a 60-page decision, blasted the marketer's claims that he should not be punished for violating Maryland law because he had no way of knowing whether his e-mails would be opened in Maryland. "This allegation has little more validity than one who contends he is not guilty of homicide when he shoots a rifle into a crowd of people without picking a specific target, and someone dies," the judge wrote. Maryland was one of the first states to try to control junk e-mail through legislation, and its 2002 law predates the 2004 federal CAN-SPAM Act. The federal law superseded most state laws unless they specifically addressed deceptive or fraudulent e-mail, which Maryland's does.

Category 4A7 Spam

2006-04-18 **FTC spam settlements CAN-SPAM Act violations antispam**

EDUPAGE; http://www.internetnews.com/xSP/article.php/3599796 23

FTC WINS TWO MORE SPAM SETTLEMENTS

The Federal Trade Commission (FTC) has gotten two new settlements in antispam cases. Matthew Olson and Jennifer LeRoy were accused of violating several provisions of the CAN-SPAM Act, including using others' computers to send spam, inserting bogus "From" information and misleading subject lines in e-mails, and failing to provide recipients with an opt-out provision. Olson and LeRoy were charged in connection with an FTC operation targeting spammers who hijack computers to send their spam. Both defendants settled with the FTC and agreed not to send any more spam. As part of their settlement a judgment of $45,000 against the two has been suspended, based on their inability to pay it. The FTC said that if Olson and LeRoy are found to have misrepresented their financial situation, they will be forced to pay the fine.

4A8 Liability

Category 4A8 *Liability*

2003-02-06 **legal liability worm damage operating system vulnerability class-action lawsuit**

NewsScan

KOREAN GROUP SAYS MICROSOFT LIABLE FOR SLAMMER DAMAGE
With support from more than 3,000 broadband subscribers, a South Korean group called the PSPD (People's Solidarity for Participatory Democracy) may file a product-liability class-action suit against Microsoft, alleging the company didn't "perform its duty to the fullest" to prevent the extensive damage caused in South Korea by the Slammer worm that exploited known vulnerabilities in Microsoft SQL 2000 servers. Slammer is also known as the Sapphire worm and SQLExp.(Cnet News.com 6 Feb 2003)
http://news.com.com/2100-1001-983578.html

Category 4A8 *Liability*

2003-08-29 **liability due diligence worm Slammer telco lawsuit**

Maine Today; http://business.mainetoday.com/yourbusiness/030829yourbiz.shtml

When the SQL Slammer worm hit the Verizon ISP in Maine in January 2003, the company shut down access to some of its Internet services as part of its emergency response. Unfortunately, the shut down also triggered penalties for violating its performance standards as regulated by the
Maine Public Utilities Commission (PUC). The judgment hinged on Verizon's failure to apply critical patches that would have prevented the infection

In August, the PUC rejected horizons request for a waiver of penalties for its failure to meet its contractual performance standards and put the company at risk of paying more than $40,000 in rebates to its customers in Maine. Frank Jaffe and Jon Stanley, writing in _Maine Today_, commented, "This decision is one of the first anywhere in the world to define a legal duty requiring the prevention of damage and losses from new types of 'foreseeable' computer security incidents. This same logic could be applied to preventing losses from viruses, or most configuration or programming errors that lead to Web site or system security problems."

In a similar case, the Guess company was fined $11,000 in federal proceedings because the Slammer infection reduced security measures on its web site and compromised customer data.

In both cases, concluded the writers, much of the damage resulted from inadequate preparation for computer incident response.

Category 4A8 *Liability*

2003-10-07 **Microsoft lawsuit security flaws software criminal network vandal**

NewsScan

MICROSOFT SUED FOR DAMAGES CAUSED BY SECURITY FLAWS
Film producer Marcy Levitas Hamilton, whose Social Security number was stolen by network vandals, has filed a lawsuit aimed at holding Microsoft responsible for damage stemming from security flaws in its software. The suit is designed to form the basis of a class action, and alleges that the majority of cyberattacks trace back to vulnerabilities in Microsoft software. Internet security and privacy consultant Richard M. Smith sasy: "This is the first time Microsoft has had its feet held to the fire on security issues." Hamilton's lawsuit notes that after the vandals stole her Social Security number, her bank accounts were accessed and frozen, and her attorney says: "They completely cannibalized her life." Microsoft executive Sean Sundwall responds: "This complaint misses the point. The problems caused by viruses and other security attacks are the result of criminal acts." (USA Today 7 Oct 2003)

Category 4A8 Liability

2004-03-04 **hacking liability companies protect consumer data security privacy e-commerce**

NewsScan

SHIELDING AGAINST LIABILITY FOR HACKED DATA

Companies that handle consumer transactions typically require customers to agree to lengthy "terms-of-use" agreements in they waive any right to sue the company if its computers have been broken into by vandals. Consumer advocates say companies should be held accountable, and Chris Jay Hoofnagle of the Electronic Privacy Information Center argues that if companies are willing to derive the benefit of information collection they should accept the responsibility to secure it. But Verizon Wireless general counsel offers the corporate view that terms-of-use clauses are nothing more than good business practice and are not attempts to avoid corporate responsibility: "Verizon Wireless is very concerned with customer security and privacy. But we are trying to be fiscally responsible to protect the company from lawsuits." (Washington Post 4 Mar 2004)

Category 4A8 Liability

2005-02-24 **liability software GM General Motors responsibility cost repairs patches tort lawasuit**

NewsScan; http://online.wsj.com/article/0

THREAT OF THE 'L' WORD MAKES SOFTWARE MAKERS SHUDDER

Major technology customers are fed up with spending millions to fix shoddy software and are starting to challenge software makers to assume at least some responsibility for costly repairs. So far, it's just a low rumble, but even the thought of the dreaded "L" word -- liability -- sends shivers through the software industry. One leading proponent is GM, whose chief information-security officer says: "Can you imagine if GM produced a vehicle and said, 'We did a pretty good job of engineering this. It worked in the laboratory. Here it is, consumer, you go crash-test it.'" GM is pushing for penalty provisions in new contracts that could hold vendors liable if they fail to meet security requirements. Other customers are seeking to add liability clauses to their "service level agreements" with outsourced technology providers that would limit the number of times their systems can go down. Meanwhile, some companies are taking matters into their own hands: BJ's Wholesale Club last year filed suit against IBM for providing software that allegedly allowed thousands of BJ's customers' credit-card information to be stolen by an organized crime ring. And even the Business Roundtable, a Washington association of CEOs, last year issued a call for "shared responsibility" between technology users and suppliers. (Wall Street Journal 24 Feb 2005)

4A9 Net neutrality

Category 4A9 *Net neutrality*

2006-03-15 **Internet Net neutrality tiered Google Yahoo big bandwidth opposition**

DHS IAIP Daily; http://news.com.com/Debate+heats+up+over+Net+neutrality/2100 −1037_3−6049863.html?tag=nl 23

DEBATE HEATS UP OVER NET NEUTRALITY.

Speculation that the two biggest phone companies in the country, AT&T and Verizon Communications, are planning to create a tiered Internet system that would require big bandwidth users like Google or Yahoo to pay more for their access has become a hot-button issue in the tech industry. Increasingly, it's also an issue on Capitol Hill, where some lawmakers are developing rules to maintain so-called Net neutrality and prevent the emergence of a tiered system. At the Voice over the Net conference at the San Jose Convention Center on Tuesday, March 14, companies on both sides of the bandwidth aisle debated how much Internet regulation is needed. CEOs from network owners AT&T and Verizon Communications have made comments suggesting they plan to create a system where some companies would have to pay more for their data-intensive use of the Net, which, they argue, slows access for regular customers. On the other side of the debate are companies such as Google, eBay and Yahoo, which are against any companies taking on the role of "IP traffic gatekeeper." They support the idea of federal rules that would further restrict network owners from blocking or restricting traffic.

Category 4A9 *Net neutrality*

2006-04-26 **net neutrality amendment bill killed House Energy Commerce Committee**

EDUPAGE; http://news.zdnet.com/2100-9595_22-6065465.html 23

COMMITTEE KILLS NET NEUTRALITY BILL

The House Energy and Commerce Committee has killed an amendment designed to guarantee net neutrality. The amendment would have prevented Internet service providers from delivering different content at different speeds based on content providers' having paid extra fees. Supporters of the amendment, including Microsoft, Amazon, and Google, argued that the Internet was built on ideas antithetical to the notion of paying fees to have content available to consumers. They called on Congress not to drop the issue but to "enact legislation preventing discrimination" against certain content providers. Opponents of the amendment, including cable and phone companies, suggested that the landscape of online content, including such material as movie-quality video, could be available to consumers if content providers paid a surcharge for it. Joe Barton (R-Tex.), chairman of the committee, commented that net neutrality is "still not clearly defined" and that he doubts the dire predictions of the amendment's supporters.

Category 4A9 *Net neutrality*

2006-05-20 **net neutrality Internet Service Providers ISP tiered pricing differential bandwidth allocation speed preferential treatment contracts consumers customers availability accessibility visibility usability**

RISKS; NYT http://www.freepress.net/news/15726 24 30

NET NEUTRALITY DEBATE HEATS UP

Sir Tim Berner-Lee, inventor of the World Wide Web, publicly critized proposals to move to a multi-tiered Internet in which high-paying corporate clients could receive preferential allocations of bandwidth while non-profits and individuals might stagnate in a mire of slow -- or no -- access. Writer Adam Cohen presented a summary of the issues in a New York Times article on May 29, 2006. Key points:

* ISPs and large corporations are pushing for permission to discriminate among content providers by charging for bandwidth. More fees, more speed.

* A growing movement is organizing to push the US Congress to block such attacks on "net neutrality."

* Breaking down net neutrality could permit open censorship of content providers -- for example, blocking or interfering with access based on political preferences.

* Fees for higher bandwidth could curtail new developments such as shared images from cellphones that could generate three-dimensional images of news events.

* Tiered pricing may harm even the ISPs because users may reject paying for services that they expect to be free (once their ISP subscriptions are paid).

4B Intellectual property: patents, copyrights (law)

Category 4B *Intellectual property: patents, copyrights (law)*

1997-01-28 **software theft**

UPI, AP

The FBI launched a nationwide investigation of the software piracy problem in the US. The FBI said that some BBS operators have graduated from exchanging stolen software on into other kinds of criminal activity.

Category 4B *Intellectual property: patents, copyrights (law)*

1997-01-30 **software theft China**

Reuters

The Chinese government announced strict penalties for illegal reproduction of copyrighted materials.

Category 4B *Intellectual property: patents, copyrights (law)*

1997-02-02 **intellectual property copyright**

EDUPAGE

The battle between the NBA and pager companies to stop them from sending basketball scores to subscribers flipped again to the defendants' side. The Second U.S. Circuit Court of Appeals in New York ruled that such transmission is not theft of property. The NBA was expected to appeal.

Category 4B *Intellectual property: patents, copyrights (law)*

1997-02-04 **internet copyright plagiarism**

AAP

Australian Helen Darville claims she did not realize that including large chunks of material taken verbatim from Internet postings and failing to attribute them was a problem. She was fired for her article, "When I am an Evil Overlord." Darville said she thought anything posted on the Net is in the public domain. Media commentators responded that plagiarism is a widespread and under-monitored practice in the news media. Darville was in the news in 1995 when she invented a persona as the daughter of Ukrainian immigrants, published a novel under a false name, and even won an award for her work. At that time, she was accused of thoroughgoing plagiarism by having included large tracts of text without attribution from several other authors. It should be noted that whether or not material is in the public domain, quoted materials must be attributed.

Category 4B *Intellectual property: patents, copyrights (law)*

1997-02-20 **piracy**

EDUPAGE

EDUPAGE reported: "According to provisional data released Feb. 13 by the Business Software Alliance and the Software Publishers Association, software company losses due to international piracy totaled around $4 billion last year. The data shows China ranking number one in illegal copying of programs, followed by Brazil, Russia, Italy and Canada. (BNA Daily Report for Executives 14 Feb 97)"

Category 4B *Intellectual property: patents, copyrights (law)*

1997-03-06 **intellectual property copyright**

EDUPAGE

The National Conference of Commissioners on Uniform State Laws proposed to make shrink-wrap license contracts legally enforceable.

Category 4B *Intellectual property: patents, copyrights (law)*

1997-05-01 **copyright**

EDUPAGE

Xerox's new Digital Property Rights Language (DPRL) is being converted to JAVA. The system works with DPRL-compliant equipment (e.g., printers) to control how copyrighted materials are allowed to be used. See <www.parc.xerox.com> for details.

Category 4B *Intellectual property: patents, copyrights (law)*

1997-05-08 **intellectual property theft extortion**

Netly News

The availability of anonymously-created web pages has generated a cottage industry of pirating new recordings. The pirate web sites sometimes last only a day or two before they move to another provider or to new locations with new false names for the authors. AOL, Prodigy, and GeoCities are choice sites for the nomad sites because of their size and tolerance of pseudonyms. Another problem comes from the increasing use of foreign ISPs, few of which care about protecting intellectual property rights. In a recent case, Chico, Calif.-based SciTech Software received e-mail demanding $20K—or their proprietary source code would be splashed publicly all over the Net. FBI investigators traced the e-mail to a Polish ISP, but there the hunt ended, since there is no reciprocity with Poland over such matters. It is unknown whether the ISP user is Polish or from another country.

Category 4B *Intellectual property: patents, copyrights (law)*

1997-05-11 **crypto lawsuit intellectual property patent license**

EDUPAGE, San Jose Mercury News

RSA Data Security Inc. filed a lawsuit against Pretty Good Privacy claiming violation of a licensing agreement. Seems that Lemcom, with which PGP recently merged, allegedly had no right to let anyone else examine RSA source code.

Category 4B *Intellectual property: patents, copyrights (law)*

1997-05-15 **copyright**

EDUPAGE, Reuters

Oasis, a rock band from the UK, announced a 30-day grace period during which unauthorized use of its copyrighted materials (photos, video fragments, song lyrics and excerpts from its albums) should be retired from Web sites. After that, it announced, it would file lawsuits charging violation of copyright laws.

Category 4B *Intellectual property: patents, copyrights (law)*

1997-05-23 **intellectual property software theft**

PA News

Ian Du'Kett, 43, an unemployed man in Peterborough, Cambridgeshire, organized a ring of software pirates who burned CD-ROMs with tens of millions of dollars worth of proprietary software — and sold them throughout England. He was sentenced to 28 months in jail and fined the equivalent of $16,000; his six confederates were sentenced to lesser terms and fines. All of their computer equipment was ordered seized and some of them had to pay court costs in addition to their fines. Du'Kett still didn't understand the issue. "The police have gone completely over the top in this. I am not a criminal," he said. "The price of software is too high. Software is getting out of everybody's reach. The public are being ripped off."

Category 4B *Intellectual property: patents, copyrights (law)*

1997-05-29 **copyright piracy software intellectual property**

Canada NewsWire via PointCast

Microsoft sued PC Village Co. Ltd., an Ontario firm that allegedly repeatedly sold computers with "loaded hard disks." The disks contained illegal copies of Microsoft software, including counterfeit MS-Windows 95 and Office 95. Undercover agents working in collaboration with the Canadian Alliance Against Software Theft (CAAST) bought two computer in a row with illegal software — one immediately after a meeting during which Microsoft representatives discussed the first case with PC Village managers. Microsoft and CAAST urge consumers to be aware of the signs of hard-disk loading:
- No end user license agreement.
- No Certificate of Authenticity
- Prices that are "too good to be true."
- No product registration card.
- No backup disks, manuals, or other materials for software installed on a new computer system.
- Backup disks have hand-written labels, are not shrink-wrapped, or appear to be of inferior quality.
- Manuals are photocopied, are not shrink-wrapped, or appear to be of inferior quality.

Report suspected piracy to Microsoft at 1-800-RU-LEGIT, via e-mail at piracy@microsoft.com or for Canadians, visit <http://www.microsoft.com/Canada/visit/piracy/>.

Category 4B *Intellectual property: patents, copyrights (law)*

1997-06-05 **copyright**

EDUPAGE

Intersect, Inc. announced a new product for scanning Web sites to locate pirated audio and video clips. A week after the announcement, the Recording Industry Association of America announced that it would soon be launching lawsuits against sites on the Internet that support music piracy (regardless of whether the sites charge for their services). A few weeks later, the RIAA filed suit against three pirate Web sites.

Category 4B *Intellectual property: patents, copyrights (law)*

1997-07-03 **software theft intellectual property law**

OTC

Microsoft reported a growing number of piracy cases involving naïve business personnel who allow unscrupulous vendors to "load" their hard disks with illegal copies of software such as Windows NT or Microsoft Office 98. Anyone buying systems with software included should demand full original documentation and a way to register their software. Call Microsoft's Anti-Piracy Hotline (800-RU-LEGIT = 800-785-3448) if you have any doubts about what you are buying.

Category 4B *Intellectual property: patents, copyrights (law)*

1997-07-22 **intellectual property**

EDUPAGE

In July, programmer Evan Brown, formerly of DSC Communications in Plano, TX, appealed a court order that would force him to tell his former employer how to convert old source code into modern equivalents. Apparently he signed an employment agreement years ago that made "all ideas related to DSC's line of business" the property of that company.

Category 4B *Intellectual property: patents, copyrights (law)*

1997-08-05 **copyright law felony**

EDUCOM

Rep. Robert Goodlatte (R-Va.) has proposed a bill to make illegal copying of software a felony. For 10 or more illegal copies with a retail cost of $5,000 or more, the convicted felon would face up to three years in jail, with penalties doubling for a second conviction.

Category 4B *Intellectual property: patents, copyrights (law)*

1997-08-05 **Inslaw copyright software theft**

AP

A long-running software copyright violation case ended in August. In 1982, software developer Inslaw provided the U.S. Justice Department with a case-management program. When the Department of Justice canceled the contract, Inslaw sued the DoJ and received much favorable press coverage in trade magazines. In 1987, a federal bankruptcy judge ruled in favor of Inslaw and awarded $7M to the owners of the defunct company. Finally, after 10 years of litigation, a federal appeals court overruled the original ruling and canceled the award.

Category 4B *Intellectual property: patents, copyrights (law)*

1997-08-14 **copyright intellectual property reproduction**

EDUPAGE

The battle between writers and publishers over electronic reproduction rights continued in August when a federal judge in Manhattan ruled that publishers can continue to reproduce freelance writers' work on CD-ROMs and in databases without paying extra royalties. Writers immediately planned to appeal the decision.

Category 4B *Intellectual property: patents, copyrights (law)*

1997-08-22 **lawsuit defamation copyright industrial espionage theft**

Reuters

In August, the conflict between arch-rivals McAfee and Symantec hit a new high (or low) when McAfee sued Symantec for defamation and asked the courts for $1B in damages. Earlier in the year, Symantec had sued McAfee for alleged copyright violations found in the source code of McAfee's VirusScan. In August, McAfee issued a press release asserting that a programmer had downloaded the 100 lines of code in question from the Internet — and that they were thus not stolen by McAfee from Symantec. The next morning, some enthusiastic hack at Symantec announced in _their_ press release that "McAfee confirms that VirusScan contains misappropriated Symantec code." Within hours, the happy lawyers at McAfee had launched their client's lawsuit for defamation.

Category 4B *Intellectual property: patents, copyrights (law)*

1997-09-02 **IETF S/MIME RSA patents crypto algorithm**

Inter@ctive Week

The IETF dmanded that RSA give up its patents on its proprietary S/MIME scheme if it expected to have it accepted as an Internet standard for e-mail encryption. RSA did not express enthusiasm for this idea.

Category 4B *Intellectual property: patents, copyrights (law)*

1997-09-02 **DNS domain names**

TechWire

The World Intellectual Property Organization (WIPO) tried to establish worldwide control over the domain name system (DNS) and failed when delegates to the meeting in Geneva in September protested that the proposals were ambiguous and would clash with local laws and customs.

Category 4B *Intellectual property: patents, copyrights (law)*

1997-09-07 **copyright intellectual property law**

EDUPAGE

In September, Sen. John Ashcroft (R-MO) introduced the Digital Copyright and Technology Education Act to protect ISPs against lawsuits based on abuse of copyright by their subscribers. At Senate hearings on these issues, ISPs pointed out that monitoring individual traffic on the Net would be an enormous burden. AOL's General Counsel said, "With billions of messages flowing across the Internet on a single day, a monitoring requirement would not be financially feasible or, frankly, consistent with the nation's commitment to communications privacy."

Category 4B *Intellectual property: patents, copyrights (law)*

1997-09-14 **copyright intellectual property public domain**

EDUPAGE

Proposed legislation in the US Congress would extend all current copyrights by 20 additional years. Commentators expressed concern over the erosion of the concept of public domain.

Category 4B *Intellectual property: patents, copyrights (law)*

1997-10-02 **intellectual property Internet technology**

EDUPAGE

The Association of American Publishers proposed the "digital object identifier" to label all documents and multimedia objects with information such as its origin, copyright restrictions, and legal ownership. Clicking on the DOI icon would link the user to the owner's home page on the Web.

Category 4B *Intellectual property: patents, copyrights (law)*

1997-10-03 **intellectual property law**

Wired

Evan Brown used to work for DSC Communications of Texas. He thought up a neat method for reserve engineering executable code by decompiling it into higher-level languages. DSC started off offering him a partnership, but then withdrew the offer and inisted on his giving them his idea for free, citing his employment agreement. Brown argued that his idea was thought up off company premises on his own time and has nothing to do with his job or his (now former) employer's business. They were off to court in Novermber.

Category 4B *Intellectual property: patents, copyrights (law)*

1997-10-09 **intellectual property law Web**

Wired

Intellectual property lawyers have been chasing down amateur Web sites where fiction refers to characters from copyright works. The "fan fiction" tradition takes well-known characters such as the crew of the Millennium Falcon from Star Wars and places them in new fiction, some of it good, some of it bad. The owners of the copyrights generally dislike this uncontrolled use of their creations, so many fans have been getting lawyers' letters telling them to cease and desist. The information-wants-to=be-free crowd protests this rigid interpretation of the existing laws, urging owners to give up their rights for the public good.

Category 4B *Intellectual property: patents, copyrights (law)*

1997-10-13 **intellectual property Web**

CMP TechWeb via PointCast

A new bill on intellectual property rights was approved in October by the House Judiciary Committee. HR 2265 would punish pirates who post copyrighted materials on the Web without permission; fines of up to $250,000 and jail of up to 3 years should provide a disincentive for creative copying if the bill is passed.

Category 4B *Intellectual property: patents, copyrights (law)*

1997-10-16 **intellectual property Internet Web**

EDUPAGE

BMI announced invention of a "Musicbot" to scan the Web for pirated music and count the number of visitors to those sites. Eventually the music licensing organization is expected to initiate legal proceedings against copyright violators who use the Web.

Category 4B *Intellectual property: patents, copyrights (law)*

1997-11-06 **intellectual property copyright theft law**

EDUPAGE

Rep. Bob Goodlatte (R-Va.) introduced draconian legislation that would punish software pirates and other copyright violators with fines of up to $250,000 and jail terms of up to three years — and that's for first-time offenders. Repeat offenders would get whacked even worse.

Category 4B *Intellectual property: patents, copyrights (law)*

1998-02-08 **piracy copyright intellectual property law**

EDUPAGE

The Argentine Supreme Court ruled that the country's copyright laws don't cover software. Software publishers estimate that 70% of the software in Argentina has been stolen in violation of their intellectual property rights. Apparently governments in Argentina are among the worst abusers.

Category 4B *Intellectual property: patents, copyrights (law)*

1998-02-26 **software license unauthorized copying detection**

EDUPAGE

If Cambridge University researchers have their way, illegal copies of software will, in U.S. terms, become "squealers." Appropriate programming of proprietary software could make computers emit specific radio signatures that could be detected using "PC piracy scanners."

Category 4B *Intellectual property: patents, copyrights (law)*

1998-03-15 **software theft piracy**

EDUPAGE

In Canada, reports Decima Research, only 20% of the law-abiding residents (admit that they?) make illegal copies of proprietary sofftware. The report, prepared for CAAST, the Canadian Alliance Against Software Theft, also revealed that more than half of the repsondents rated stealing a chocolate bar as a more serious breach of law than stealing proprietary software.

Category 4B *Intellectual property: patents, copyrights (law)*

1998-05-05 **copyright intellectual property encryption cryptography ISPs**

EDUPAGE

In May, the Senate Judiciary Committee agreed to proposed legislation aimed at protecting copyright online. The bill was criticized by the Computer and Communications Industry Association because it made no provision for replication of materials in cryptography. The proposal did make allowance for continued "fair use" by librarians and by teachers. It also exculpated ISPs that inadvertently host users who violate copyright laws.

Category 4B *Intellectual property: patents, copyrights (law)*

1998-05-07 **copyright piracy audio RealPlayer recording RealAudio**

EDUPAGE

A debate broke out when the British Phonographic Industry (BIA) claimed that it had possession of software capable of recording RealAudio data streams, a warning denied by RealNetworks, makers of the popular audio and video programs.

Category 4B *Intellectual property: patents, copyrights (law)*

1998-05-10 **intellectual property copyright fair use law bill US**

RISKS 19 73

The WIPO Copyright Treaties Implementation Act (H. R. 2281) was introduced in the US Congress. Supported by the Administration, the bill would define a new crime, "circumvention," consisting of any attempt to bypass copy-protection schemes. One possible implication of such a law would be that supplying false information on Web forms in order to access free information would become a criminal offense. Another issue is reverse engineering, which would also be made illegal — with unknown consequences for the software industry. This bill, also known as the Digital Millennium Act, was approved unanimously by the House Commerce Committee on 7 July. The House Judiciary Committee was evaluating a different version of the same bill.

A related bill, the Collections of Information Antipiracy Act (H.R. 2652) would allow compilers of information to copyright the facts themselves, something currently impossible under copyright law. For different views on these issues, see the Digital Future Coalition's (opponents') site at <http://www.dfc.org/> and the Creative Incentive Coalition (proponents') site at <http://www.cic.org/>.

Category 4B *Intellectual property: patents, copyrights (law)*

1998-05-17 **intellectual property law copyright penalties music movies**

EDUPAGE

In May, the Senate of the US unanimously passed the Digital Millennium Copyright Act to extend copyright protection to artistic works and software even in cyberspace. Penalties for piracy-for-profit were raised to$1M and up to 10 years in jail. ISPs and libraries, however, were explicitly excused from liability if their users violate these provisions. The Act became law on 3 Nov 1998 and required ISPs to register with the Copyright Office to avoid prosecution for the depredations of their users.

Category 4B *Intellectual property: patents, copyrights (law)*

1998-06-22 **reverse engineering trade secrets copyright infringement security analysis WIPO treaty law proposal bill**

PC Week http://www.zdnet.com/pcweek/news/0622/22wipo.html

In June, the Senate of the USA passed a bill approving the WIPO (World Intellectual Property Organization) treaty that would make it illegal to apply reverse engineering and even vulnerability testing to software. Opponents of the terms argued that such restrictions would shut down ethical vulnerability analysis and significantly weaken the ability of computer scientists and security experts to identify security problems in commercial software.

Category 4B *Intellectual property: patents, copyrights (law)*

1998-07-02 **trademark infringement lawsuit**

EDUPAGE

Last year there was the ludicrous spectacle of a firm claiming to have trademarked the three letter acronym "Y2K." In June we saw Microsoft pay $5M in settlement over the name of their browser. In July, a new chapter in trademark law opened when a small company (very small: two people) called E Technology Associates LLC sued IBM, a large company (very large: several hundred thousand people) over the use of the letter "e" as in "e-mail", "e-commerce" and so on. In another case, Compaq paid the owner of the registered domain "altavista.com" $3M for the rights to that name.

Category 4B *Intellectual property: patents, copyrights (law)*

1998-07-16 **document archives reference scholarly publications reference**

RISKS 19 86

Eran Gabber commented on the shift to including URLs as references in scholarly papers. He and Avishai Wool cited RISKS but were told by the program committee where they submitted their paper to cite a paper copy — which does not exist for RISKS. The solution was to provide several ways of tracking the reference (USENET, Risks archives). The broader problem raised by Gabber was the longevity of URLs: how long can one expect a Web site to maintain its documents at the same URL — or indeed, in these days of mergers, acquisitions and business failures — at all?

Category 4B *Intellectual property: patents, copyrights (law)*

1998-08-18 **intellectual property patents meter e-commerce stamps postal**

EDUPAGE

Pitney Bowes, the familiar source of everything relating to postage meters, is claiming that its patents cover everything relating to postage meters — including software simulations thereof that allow users to print their own postage labels on their PCs. The USPS has no comment; firms such as E-Stamp are not impressed. Expect a court case soon.

Category 4B *Intellectual property: patents, copyrights (law)*

1998-09-20 **copyright intellectual property universities publishers**

EDUPAGE

Finally waking up to the value of their own intellectual output, academics began seriously discussing policies requiring them to maintain copyright over their articles instead of donating them to publishers.

Category 4B *Intellectual property: patents, copyrights (law)*

1998-09-23 **pornography defamation fraud forgery Web lawsuit settlement**

RISKS 19 97

Nancy Kerrigan, the former Olympic figure-skating champion, was understandably furious when a composite pornographic image (her head, another woman's body) was posted on a Web site by Marvista Computing Co. Ms Kerrigan sued and won a settlement in which the defendants' three computers were donated to a local school (after depornifying the disks).

Category 4B *Intellectual property: patents, copyrights (law)*

1998-11-04 **copyright ISP Internet service provider law register**

CNET news.com http://www.news.com/News/Item/Textonly/0,25,28357,00.html

The U.S. Digital Millennium Copyright Act, signed in late October by President Clinton, required ISPs to register with the U.S. Copyright Office in order to avoid possible liability for stolen copyrighted materials being sent through their networks. By law, every ISP must specify a named individual or position to receive and act upon complaints of copyright violations by the ISP's users..

Category 4B *Intellectual property: patents, copyrights (law)*

1998-12-12 **e-commerce copyright publishing Web online magazine**

New Scientist via New York Times

Abstract from allEC.com: An online magazine has been launched on the Internet with security software that prevents subscribers from passing electronic copies on to friends. The magazine, produced by the British company that publishes Everyday Practical Electronics, believes it is the first system of its kind. The first issue of EPE Online, which can be downloaded free, is now on the Web at http://www.epemag.com. Later issues will have to be paid for. The control software was developed by the multimedia company Maxfield & Montrose of Madison, Ala. It breaks the magazine down into a series of Adobe Acrobat files, each one containing a complete article. But the files also contain an "umbrella" file listing the issue's contents. This file has to be present and working.
New Scientist via NY Times (98.12.08)

Category 4B *Intellectual property: patents, copyrights (law)*

1999-01-05 **trademark lawsuit judgement injunction phrase words**

AP

AOL sued AT&T for daring to announce "You have mail" to its e-mail users. The largest ISP in the world argued that it should have exclusive right to utter those words in an online session. On Christmas eve 1998, U.S. District Judge Claude Hilton (Alexandria, VA) declined to issue an injunction against such use, although he did permit the case to go to court.

Category 4B *Intellectual property: patents, copyrights (law)*

1999-02-05 **copyright law distance education publishers entertainment**

Chronicle of Higher Education

At a hearing in February before the U.S. Copyright Office, educators lobbied for the right to use copyrighted works in their distance-education programs offered via the Internet without having to obtain explicit permission from the copyright owners. Their position was vigorously opposed by publishers and by speakers for the entertainment industry.

Category 4B *Intellectual property: patents, copyrights (law)*

1999-02-11 **copyright trademark infringement search engines pornography**

USA Today

John Gehl and Suzanne Douglas, editors of EDUPAGE, wrote with their usual admirable conciseness about a potentially crucial case in the evolution of Internet law: "Playboy Enterprises is suing portal sites Excite and Netscape for trademark infringement because searches on words trademarked by Playboy, such as `Playboy' and `Playmate,' turn up banner ads for a cluster of hard-core porn sites that are benefiting from a misappropriation of Playboy's `good will and reputation.' "

Category 4B *Intellectual property: patents, copyrights (law)*

1999-03-12 **industrial espionage intellectual property lawsuit court**

SJ Mercury News

In an unusual attempt to extend the anti-compete clauses of many employment contracts in the high-tech fields, Motorola applied to a court for injunctions preventing Intel from hiring ex-employees of Motorola. [Perhaps corporations will someday apply electroconvulsive shock treatments — excellent for causing amnesia — to its best minds when they leave.]

Category 4B *Intellectual property: patents, copyrights (law)*

1999-03-19 **intellectual property database piracy appropriation law bill**

New York Times

A proposed bill introduced in the US Congress by Rep. Howard Coble (R — NC) would protect the interests of database compilers and backed by the Coalition Against Database Piracy lobbying group. Many forces opposed the bill, including the Clinton administration, many academics, Internet service providers, bankers, and medical organizations. The opponents argue that the bill could severely interfere with the free exchange of publicly available information.

Category 4B *Intellectual property: patents, copyrights (law)*

1999-05-03 **copyright music copying illegal intellectual property license player MP3 G2**

New York Times
http://www.nytimes.com/library/tech/99/05/biztech/articles/03real.html

RealNetworks announced that its Real Jukebox software includes copy protection — of a sort. An electronic "tether" warns the user that attempts to copy a downloaded audio CD file on a different computer is a violation of copyright. Because the tether can easily be disabled or ignored, the music industry was not impressed.

Category 4B *Intellectual property: patents, copyrights (law)*

1999-05-03 **music Web intellectual property copyright MP3 recording**

New York Times

Real Networks announced in early May that its new streaming player, Real Jukebox, would allow users to download and store a variety of digital audio formats, including MP3 and the company's own G2 files. In a weak nod to copyright concerns, the software includes an optional feature to limit the number of copies to be stored on disk.

Category 4B *Intellectual property: patents, copyrights (law)*

1999-05-04 **copyright intellectual property e-commerce protection encryption software music MP3**

Los Angeles Times http://www.latimes.com/home/business/t000040006.1.html

InterTrust Technologies launched a copy-protection scheme with Seagram's Universal Music Group in May. The DigiBox system encrypts data of any kind for download to users and offers options such as allowing a brief sampler of a music track or charging a minor fee for a day of listening or of usage before the buyer decides whether to buy that product.

Category 4B *Intellectual property: patents, copyrights (law)*

1999-05-28 **intellectual property universities schools colleges copyright Fair Use Doctrine education non-commercial**

Wired

The U.S. Copyright Office released recommendations urging that public schools and universities be granted exemptions under Fair Use doctrine for educational, non-commercial use of copyright materials.

Category 4B *Intellectual property: patents, copyrights (law)*

1999-06-22 **reverse engineering trade secrets copyright infringement security analysis WIPO treaty law proposal bill**

PC Week http://www.zdnet.com/pcweek/news/0622/22wipo.html

The World Intellectual Property Organization (WIPO) treaty that was passed by the Senate of the United States in May would have serious consequences for consumers and for security experts. The treaty would render reverse engineering of proprietary software and ban real-world testing of security software.

Category 4B *Intellectual property: patents, copyrights (law)*

1999-07-26 **chat instant message proprietary protocol reverse engineering conflict breach**

Washington Post http://washingtonpost.com/wp-srv/WPlate/1999-07/28/118l-072899-idx.html, New York Times, Wall Street Journal

AOL did not take kindly to attempts to make other products compatible with its proprietary Instant Messenger software. The company immediately changed its protocols when Microsoft, Yahoo! And Prodigy attempted to allow their users to communicate with AOL users using chat-popup boxes. AOL even hinted that just trying to chat with its users was a breach of security. Within a few days of the start of the blowup, though, AOL began cooperating with Apple Computer to provide precisely this functionality. In August, Microsoft tried to pressure AOL into cooperating by releasing the code for its own MSN messaging service, hoping thereby to influence the IETF (Internet Engineering Task Force) working group choosing a standard for instant Internet messaging.

Category 4B *Intellectual property: patents, copyrights (law)*

1999-07-29 **software license restrictions antivirus virus copyright reverse engineering testing commercial law shrink-wrapped contract law bill proposal**

Red Rock Eater News

In July, the National Conference of Commissioners on Uniform State Laws (NCCUSL) approved the controversial UCITA (Uniform Computer Information Transactions Act) proposal that would create common licensing rules for software and other IT transactions. The law applies to product
licenses and covers all aspects of modern IT, including data, databases, multimedia files, online transactions and software licenses. Among other protections for vendors, the UCITA provides for
* rigid enforcement of shrink-wrapped licenses even though the buyer may not see or agree to the terms until after the software has been purchased;
* banning reverse engineering of proprietary software;
* allowing vendors to shut down software remotely if they suspect a violation of the licensing terms;
* easier disclaimer of written warranties.
On 1999-06-10, the Business Law Section of the American Bar Association issued a blistering attack on the proposal. Staff of the Federal Trade Commission also submitted a brief opposing the UCITA on grounds of consumer protection and potential damage to competition. The ACM strongly opposed the proposal, and its President commented that theoretically, the UCITA would make anti-virus software illegal because viruses, which are automatically copyrighted by their authors, could no longer be reverse engineered. The Newspaper Association of America and the Magazine Publishers of America also formally opposed the UCITA, saying that the proliferation of different state rules on intellectual property would make their operations unwieldy by distinguishing between print and online media.

Category 4B *Intellectual property: patents, copyrights (law)*

1999-09-28 **copyright writers publishers legal case conflict rights royalties CD-ROM**

Newsbytes

A New York state court ruled in favor of the National Writers Union and against the New York Times and other major publishers in defending the right of writers to control publication of their materials on new media. The publishers wanted to use submissions on CD-ROMs or on the Web without paying additional royalties.

Category 4B *Intellectual property: patents, copyrights (law)*

1999-10-16 **patents Internet operations methods innovations**

New York Times, Computerworld, New Scientist

In 1998, the U.S. Patent and Trademark Office granted 125 patents for online business practices and was expected to issue up to 200 in 1999. Critics suggest that some of these patents merely appropriate common non-electronic ways of doing business; e.g., <Priceline.com> patented the reverse auction, where vendors offer their best price to customers asking for products or services. Such patents are unlikely to be enforceable, according to intellectual-property-law specialists.

Category 4B *Intellectual property: patents, copyrights (law)*

1999-11-26 **intellectual property control license screen copy-protection print**

OTC

BreakerTech, a UK company, announced its new SoftSEAL technology for preventing computer users from using screen-capture commands to foil intellectual property restrictions.

Category 4B *Intellectual property: patents, copyrights (law)*

1999-12-07 **counterfeits intellectual property products**

Times of London

Hasbro, a major toy and game manufacturer, declared war against counterfeiters in December. The company launched a vigorous advertising campaign and arranged for increased cooperation with law enforcement to crack down on companies illegally making unauthorized copies of such popular items as Action Man, Furby, Monopoly and Pokemon.

4B1 Copyrights

Category 4B1 *Copyrights*

2000-01-29 **intellectual property confidentiality source code DVD lawsuit error evidence documents**

RISKS 20 77

In filing documents with the court in the DVD industry's lawsuit against the authors of the DeCSS decoding software, attorneys for the DVD Copy Control Association forgot to ask the judge to prevent disclosure of the industry's encryption source code. The materials were distributed on the Web before the judge sealed the evidence.

Category 4B1 *Copyrights*

2000-02-09 **copyright lawsuit Canada theft Web intellectual property international boundary jurisdiction**

NewsScan, USA Today http://www.usatoday.com/life/cyber/tech/cth190.htm,
San Jose Mercury Times
http://www.sjmercury.com/svtech/news/breaking/ap/docs/188993l.htm

A Canadian Web site, iCraveTV, was sued by a consortium of broadcasters and film owners for posting their intellectual property without license. The owners of iCraveTV retorted that Canadian law does not forbid such piracy. The CRTC (the Canadian equivalent of the US Federal Communications Commission) declined to intervene in the case. A federal judge granted the plaintiffs a temporary restraining injunction to stop the video pirates from further use of unlicensed materials.

[On 9 February,]A U.S. federal judge has issued a 90-day injunction against continued operation of the Toronto-based Web site iCraveTV, which captures TV programs from stations in Toronto and Buffalo and rebroadcast them live (along with new ads sold by iCraveTV) to Canadians. The company's founder takes the position that such activity is permissible under Canadian law, and that iCraveTV will reinforce its security mechanisms to make sure that the rebroadcasts would not be viewable south of the U.S.-Canadian border, and that the company would meet industry standards. But an executive of the Motion Picture Association of America protests: "There is no acceptable industry standard for piracy." (AP/San Jose Mercury News 9 Feb 2000)

Category 4B1 *Copyrights*

2000-04-14 **copyright intellectual property ISP Internet service provider court legal lawsuit common carrier**

NewsScan

Internet service providers in Germany . . . [were] facing a new legal challenge after a Munich court found AOL Europe liable for damages resulting from the downloading of copyrighted music via an online forum. The court's decision is reminiscent of the 1998 ruling that found Felix Somm, former head of CompuServe in Germany, guilty of failing to block access to child pornography. That ruling triggered widespread criticism and was overturned last year. AOL Europe says it had fulfilled its legal obligations and had made a good faith effort to discourage copyright violations by its subscribers. "We are only the messenger," says an AOL spokesman. "Nobody would have sued the Royal Mail or Deutsche Post for delivering a package that contained illegal CDs." Damages have not yet been set, and AOL is considering an appeal. If the Munich verdict is upheld by a higher court, "then the online industry has a major problem," says one industry observer. (Financial Times 14 Apr 2000)

Category 4B1 *Copyrights*

2000-05-15 **intellectual property compilation copyright lawsuit**

NewsScan, Wall Street Journal
http://interactive.wsj.com/articles/SB958348989291026253.htm

Upstart Jurisline.com . . . [was] sued by legal publisher Lexis for copying the CDs containing court opinions and related documents that Lexis sells and distributing the same information free on its Web site. For decades, the database of legal material has been marketed by two companies — Reed Elsevier's Lexis and Thomson Corp.'s West Publishing — which charge premium rates for access to a single document and reap millions of dollars a year in subscription fees from the nation's law firms. Jurisline.com, on the other hand, distributes the information for free, making its revenue on advertising. At issue in the court case is whether Lexis's license agreement prohibiting the purchaser from developing "a database, infobase or other information resource" is legally enforceable, given that the materials in question were written on the taxpayer's dime and can't be copyrighted. . . . (Wall Street Journal 15 May 2000)

Category 4B1 *Copyrights*

2000-06-28 **intellectual property encryption value-added network**

NewsScan, New York Times
http://partners.nytimes.com/library/tech/00/06/biztech/articles/28online.html

In a move that could help diffuse the controversy surrounding the downloading of digital music, America Online says it is teaming up with InterTrust to promote its encryption software in AOL's version 6.0 CDs, to be distributed later this year. The InterTrust system enables a recording company to surround a digital music file with software that ensures it will only be played according to rules specified by the company. In addition, AOL will integrate InterTrust's system into a version of its Winamp music player, a move that could boost Winamp's popularity among companies seeking to distribute digital music. "We could be at the threshold of something very big," says Talal Shamoon, senior VP for media at InterTrust. "A robust electronic community of people exchanging content in a safe way, where rights holders get paid and consumers feel good about the experience." (New York Times 28 Jun 2000)

Category 4B1 *Copyrights*

2000-07-11 **intellectual property IP licensing Web royalties lawsuit judgement**

NewsScan, San Jose Mercury News
http://www.sjmercury.com/svtech/news/breaking/ap/docs/185784l.htm

A federal judge . . . ruled that the Web site Gridiron.com violated the exclusive licensing rights of the National Football League's Player Association by using the names and images of NFL players without paying royalty fees. The site allows visitors to search for players by name, team and position. The executive director of the Player's Association said, "Gridiron.com's Web site was a direct attack on the rights and resources the union uses to protect players through collective bargaining." (AP/San Jose Mercury News 11 Jul 2000)

Category 4B1 *Copyrights*

2000-07-12 **intellectual property IP fair use legislation law proposal**

NewsScan, Washington Post http://www.washingtonpost.com/wp-dyn/articles/A24504-2000Jul11.html

Senate Judiciary Committee chairman Orrin Hatch . . . [said] that Congress may want to "tweak" the definition of "fair use" in intellectual property law because of the unwillingness of the recording industry to allow music fans to use the Internet to download and swap digital music files using Napster or similar new technology. In testimony before that committee, Napster's chief executive Hank Barry insisted: "Napster does not copy files. It does not provide the technology for copying files. Napster does not make MP3 files. It does not transfer files. Napster simply facilitates communication among people interested in music." But Lars Ulrich of the rock group Metallica told the committee: "Napster hijacked our music without asking. We should decide what happens to our music, not some company with no rights in our recordings. The choice has been taken away from us." (Washington Post 12 Jul 2000)

Category 4B1 *Copyrights*

2000-07-21 **intellectual property IP peer-to-peer network music copyright violations infringements trading lawsuit**

NewsScan

A coalition of trade groups representing more than 20 entertainment and film companies has sued Scour, a company backed by Hollywood powerbroker Michael Ovitz, which has developed a Napster-like search engine that enables users to trade films and music on the Web. The case is similar to the recording industry's lawsuit against Napster, whose service enables users to swap songs for free by trading MP3 files. Both suits seek preliminary injunctions to have unauthorized copyrighted material pulled off these sites, claiming losses in revenues and creative control for artists. Scour president Dan Rodrigues expressed surprise at the lawsuit, saying he was engaged in productive talks with Sony, Warner and Bertelsmann's BMG to establish business relationships with these companies. But Jack Valenti, president and CEO of the Motion Picture Association of America, one of the plaintiffs, said: "This is about stealing, plain and simple. Creative works are valuable property and taking them without permission is stealing, whether you download movies illegally or shoplift them from a store." (Financial Times 21 Jul 2000)

Category 4B1 *Copyrights*

2000-07-25 **intellectual property IP culture history**

NewsScan, Los Angeles Times
http://www.latimes.com/business/20000725/t000069563.html

Time Warner president Richard Parsons says the court's decision on Napster will have major effect on the future of society: "I think this is a very profound moment historically. This isn't just about a bunch of kids stealing music. It's about an assault on everything that constitutes the cultural expression of our society. If we fail to protect and preserve our intellectual property system, the culture will atrophy. And corporations won't be the only ones hurt. Artists will have no incentive to create. Worst-case scenario: The country will end up in a sort of cultural Dark Ages." (Los Angeles Times 25 Jul 2000)

Category 4B1 *Copyrights*

2000-08-03 **intellectual property IP royalties shareware publishing**

NewsScan, CNet http://news.cnet.com/news/0-1007-200-2419316.html

The new Stephen King novel, published on the Web with a request that at least 75% of downloaders send the author $1 for the privilege, may well change the way all sorts of intellectual property is marketed, says R. Polk Wagner, a Penn law school professor. "Traditional intellectual property theory holds that producers (that is, King) won't produce unless they have the ability to restrict the access of others to their goods. Here King is doing two significant things: First, he's only asking 75 percent of the people to pay him, thereby engaging in an unusual form of price discrimination where only those who feel the moral pressure to contribute will do so. That is, King acknowledges that not everyone will pay. Second, he's explicitly asking people to pay for his future services. The traditional theory of intellectual property would not consider this possibility. Classic intellectual property theory holds that producers must get paid for the works they've already created, not works they've yet to produce." The result could be troubling for publishers, who depend on the sacredness of intellectual property for their livelihood. "If Stephen King, one of the 'poster boys' of the intellectual property industry, doesn't need intellectual property (protection) anymore, what does that mean for intellectual property generally?" (Knowledge@Wharton 3 Aug 2000)

Category 4B1 *Copyrights*

2000-08-04 **intellectual property IP royalties Web publishing freelance writers**

NewsScan, Hollywood Reporter
http://www.hollywoodreporter.com/archive/hollywood/current/webwatch/webwatch06.asp

The National Writers Union's executive board . . . reached an agreement with Contentville, an online reseller of text-based "content," that will give freelance writers a 30% cut of the fees paid by Contentville customers. Royalties would be distributed through the NWU's Publication Rights Clearinghouse. Contentville sells, for a small fee, "books, magazines, e-books, academic works, transcripts, archived articles, scripts or anything else that qualifies as brain food." The truce signals a new desire on the part of Internet publishers to settle the messy issue of electronic posting of written works that were created under agreements that did not expressly provide for e-publication. The issue has rankled the freelance community as many heavy-handed media companies have for the last few years required freelancers to sign contracts that allow electronic republication of their work without additional compensation. Last September, a U.S. federal appeals court ruled that publishers can't include work by freelance writers in their electronic databases without the writers' permission. Among the companies that had fought the federal case were The New York Times Co., Newsday, Time Inc. Magazine Co., University Microfilms International and Mead Data Central Corp. The Times and Time Inc. have said they will appeal the decision to the Supreme Court. (AP/Hollywood Reporter 4 Aug 2000)

Category 4B1 *Copyrights*

2000-08-07 **intellectual property IP lawsuit infringement copyright**

NewsScan, Los Angeles Times
http://www.latimes.com/business/20000807/t000073815.html

The New York Times, Washington Post, and other traditional media companies are suing the San Diego company GoSMS.com for redistributing articles without their permission. GoSMS.com copies the articles from the original Web sites in order to ship them to the handheld devices of its own customers. (Los Angeles Times 7 Aug 2000)

Category 4B1 *Copyrights*

2000-08-11 **intellectual property IP copyright infringement violation distribution**

NewsScan, Hollywood Reporter
http://www.hollywoodreporter.com/archive/hollywood/current/webwatch/webwatch05.asp

Bowing to pressure from the recording industry, America Online . . . removed a search engine used to find music files on its Winamp.com site, which distributes a popular MP3 player program for Windows. "We don't have an efficient process for distinguishing between legal and illegal MP3s, so we decided to take it down until we can address that," . . . [said] an AOL spokesman. The search engine was located on a site belonging to Nullsoft, an AOL subsidiary, whose staff describes themselves as "legitimate nihilistic media terrorists as history will no doubt canonize us." (AP/Hollywood Reporter 11 Aug 2000)

Category 4B1 *Copyrights*

2000-08-17 **intellectual property IP body image ownership actor model avatar**

NewsScan

The sale of Press Association virtual newscaster Ananova to wireless operator Orange for $143 million signals a new era for virtual reality, in which electronic virtual assistants, or EVAs, are poised to assume the roles of customer service representatives, celebrity spokespersons and shopping assistants. Digital Animations Group, the Scottish creators of Ananova and her successor, TMmy, is gearing up to market similar EVAs to online businesses that want to present a more "human" front. "It is our belief that virtual characters are going to dominate as personal assistants, presenters and even games celebrities," says Digital Animations CEO Mike Hambly. Meanwhile, U.K.-based Stratumsoft believes that EVAs based on real people have more potential. One possibility cited is supermodel Claudia Schiffer: "We could create a body scan of her, then produce an EVA based on her personality. As a marketing device, you would then have a celebrity available 24 hours a day on the Web site to 'chat' to fans and promote your product as part of your advertising campaign." What's not yet clear in all this is who would own such characters — the brand or the "real" celebrity? (Financial Times 17 Aug 2000)

Category 4B1 *Copyrights*

2000-08-21 **peer-to-peer networking intellectual property IP**

NewsScan, Hollywood Reporter
http://www.hollywoodreporter.com/music/index.asp?ee

Music industry officials say the only way to combat music piracy is to develop their own universal platform for selling music online. "We need an open system where all our music is available; we can't leave it to Napster or Gnutella," says Rudi Gassner, a board member for Germany's Edel Music. According to BMG Entertainment exec Thomas Stein, within five years, Internet sales will account for 50% of the music retail business, compared with 3.4% today. Meanwhile, Bertelsmann CEO Thomas Middelhoff says music companies need to digitize their back catalogues, secure the legal rights to sell their music online, and synchronize their technical standards. "We have to sit down — without the entertainment lawyers — and come to an agreement." (Hollywood Reporter 21 Aug 2000)

Category 4B1 *Copyrights*

2000-09-05 **intellectual property IP licensing copyright royalties government proposal law regulation tax**

NewsScan

The German government is considering levying a fee on manufacturers of computer and telecommunications equipment that can be used to duplicate protected works. The fee would be used to compensate authors and other copyright holders. Included under the amendment would be such devices as CD burners, computer printers, hard drives and high-speed modems that facilitate large file downloads. Such fees are already levied on copy machines. Industry officials have denounced the plan, which they say would raise the price of such devices by 30% in Germany. A Hewlett-Packard executive told the Berliner Zeitung that many companies would simply move their operations out of Germany if the tax is passed. (AP/San Jose Mercury News 5 Sep 2000)

Category 4B1 *Copyrights*

2000-10-27 **copyright intellectual property ruling limitations libraries filtering censorship censorware**

NewsScan, Wall Street Journal
http://interactive.wsj.com/articles/SB972602565773912484.htm

In a step toward revamping traditional copyright law to reflect the realities of the digital age, the federal Copyright Office has issued a ruling backing companies' rights to limit access to their content when it is made available on the Internet. The decision came as part of new federal law that makes it illegal for Web users to hack through software that copyright holders use to protect books, films, music and other digital content. Congress had left it to the Copyright Office to create any exemptions that might be needed to facilitate access by libraries and universities. The two exemptions allowed are minor in scope: one enables users of filtering software to access the lists of Web sites being filtered, and the other gives people the right to bypass malfunctioning security features of software and other copyrighted goods they have purchased. The decision came as a blow to libraries and universities because it gives copyright holders a whole new level of protection, which they fear could limit their ability to use materials in digital format. An American Library Association official said the decision will "significantly impede efforts for libraries to continue to provide information in the digital age." (Wall Street Journal 27 Oct 2000)

Category 4B1 *Copyrights*

2000-11-27 **intellectual property government regulation fee tax copyright**

NewsScan, Wall Street Journal
http://interactive.wsj.com/articles/SB975279995969460074.htm

Hewlett Packard became the first company to be snagged by a German law that requires CD burner manufacturers to pay a fee for each device sold in that country. HP reached an agreement last week with GEMA, Germany's main licensing group, to pay DM3.60 (US$1.54) for each CD burner sold since February 1998, when the issue first arose, and DM12 (US$5.16) for each CD burner sold in the future. The fees are distributed by GEMA to copyright owners through recording houses and music distributors. The development is being watched closely by many of Germany's neighbor's, including France, Italy and Greece, which have similar laws levying fees on makers of equipment that can be used to violate copyright laws. (Wall Street Journal 27 Nov 2000)

Category 4B1 *Copyrights*

2000-12-11 **intellectual property copyright fees music government regulations broadcasting Webcasting**

NewsScan, Hollywood Reporter
http://www.hollywoodreporter.com/music/index.asp?ee

[In late November, the] U.S. Copyright Office. . . [began] considering whether radio stations must pay record companies when the stations use their Web sites to offer music over the Internet. The radio industry . . . [was] not happy about the possibility. Dennis Wharton of the National Association of Broadcasters said: "What the music industry is trying to do is saddle broadcasters with new fees that Congress has always exempted us from paying. It could cost broadcasters millions of dollars and would probably cripple or seriously impair the streaming of radio signals over the Internet." (Bloomberg/New York Times 27 Nov 2000)

[In early December, the] recording industry won a victory . . . when the U.S. Copyright Office ruled that Webcasting by radio broadcasters constitutes a second performance of artists' copyrighted works and does not merit the same exemption from royalty payments accorded to traditional over-the-air programming. "Transmissions of a broadcast signal over a digital communications network such as the Internet are not exempt from copyright liability," the Copyright Office wrote. Broadcasters had argued that their Webcasts were exempt because they are "nonsubscription" transmissions licensed by the FCC that serve local communities, but the Copyright Office rejected that argument, pointing out that, in fact, Webcasts exceed "the geographic limits established for broadcast under the FCC license." The decision could mean millions of dollars in royalty fees that companies like Bertelsmann, Universal and Warner Bros. would collect from broadcasters. (Hollywood Reporter 11 Dec 2000)

Category 4B1 *Copyrights*

2001-02-05 **intellectual property rights copyright copying duplication private use Europe regulation**

NewsScan

EUROPEAN PARLIAMENT OKAYS PRIVATE COPYING OF DIGITAL WORKS
The European Parliament has issued a preliminary decision to extend, with some limitations, the private copying permissible in the analog world to digital media. New-media companies, consumer-electronics makers and citizens' rights groups applauded the decision to reject all but 16 of a record 197 proposed amendments to the EU's Copyright Directive, which faces a full vote next week. Among the amendments approved was a provision allowing copyright owners to employ technical protection measures, such as encryption, to prevent their works from being pirated. Copies could, however, be made "by a natural person for private use and for ends that are neither directly nor indirectly commercial." Fair practice lobbyists said the final version represented a reasonable compromise: "Everybody gained something and everybody lost something," said the head of the European Digital Media Association. The music industry, however, was more critical of the decision: "Private copying really has to be fore the private circle," said the European regional director of the Federation of Phonographic Industries. (Wall Street Journal 6 Feb 2001)
http://interactive.wsj.com/articles/SB981401558502841316.htm [subscription req'd]

Category 4B1 *Copyrights*

2001-02-15 **intellectual property music legislation peer-to-peer networking privacy**

NewsScan

EUROPEAN PARLIAMENT BLOCKS SONG SWAPS
The European Parliament has okayed rules that will block companies such as Napster from operating in the 15-member bloc without authorization from recording artists. Wednesday's ruling compromised between extreme measures suggested by both sides on the issue, and seeks to ease record companies' concerns over piracy while at the same time allowing individuals to continue making a limited number of copies for personal use. Publishers and music and film producers will, for the first time, be allowed to use "technical protection measures," including encryption, to prevent unauthorized copying. Enrico Boselli, who guided the legislation through the parliament, noted that the Copyright Directive was badly needed "to set clear rules for consumers, consumer-electronics manufacturers, Internet service providers and others. Copyright owners now have wider protection here than in the U.S." (Wall Street Journal 15 Feb 2001)
http://interactive.wsj.com/articles/SB982159222697782071.htm

Category 4B1 *Copyrights*

2001-03-02 **copyright intellectual property law lawmakers amateurs**

NewsScan

E-MAIL SHARING BANNED BY LAW IN AUSTRALIA
Forwarding e-mail to friends, family or colleagues without permission from the sender is now illegal in Australia, thanks to a new law that took effect yesterday. Penalties for violation could be as much as five years' jail time or fines of AU$60,000 (US$31,400). The motivation behind the law is copyright protection for the sender of the original e-mail. But in addition to material that already has copyright protection, such as excerpts from books or song lyrics, the new measure also affects personal messages. "It's quite possible that the forwarding of an e-mail could be a technical infringement of copyright," says a legal advisor for Australia's attorney general. "E-mailing something is a 'communication' under the Digital Agenda Act and so is putting something up on a Web site." This new interpretation means a simple e-mail about office gossip or holiday plans also carries personal copyright protection. It is estimated that 5 million or more e-mail messages are forwarded around Australia every day. (The Sunday Telegraph 4 Mar 2001)
http://www.news.com.au/common/story_page/0,4057,1768268%5E421,00.html

---

Category 4B1 *Copyrights*

2001-06-28 **copyright intellectual property CD-RW fees**

NewsScan

GERMAN COURT IMPOSES FEES ON HP TO COMPENSATE MUSICIANS
Upholding a law passed by Germany's copyright society (GEMA) that targets manufacturers of equipment used to violate piracy laws, a court in that country is assessing fees on CD burners sold by Hewlett-Packard to compensate musicians whose copyrighted works are being downloaded from the Internet without their permission. HP plans to appeal and says that the best way to oppose piracy is not by inflating the price of equipment but by offering individual licensing and user fees.
(AP/Washington Post 28 Jun 2001)
http://washingtonpost.com/wp-dyn/articles/A56397-2001Jun28.html

---

Category 4B1 *Copyrights*

2001-07-12 **copyright intellectual property moral rights authors distributors lawsuit**

NewsScan

COPYRIGHT BATTLE ERUPTS OVER E-BOOKS [6 May 2001]
Bertelsmann's Random House and startup Rosetta Books will square off this week in a court battle that could have as much influence on the future of publishing as Napster had on the music industry. Random House is pursuing its claim that authors who sign over the rights to publish their works in "book form" before the existence of the Internet also granted the rights for e-publications. Rosetta Books had contracted directly with a group of authors, including William Styron and Kurt Vonnegut, for the electronic publishing rights to some of their Random House titles, which it says are not included in the print contracts. E-books are poised to become the third branch of online copyright disputes, which are already causing upheaval in the music and film industries. The music industry has pressured Napster to add filters to its popular file-sharing service, and the film industry last week announced plans to go after Gnutella users who traffic in pirated movies. (CNet News.com 6 May 2001)
http://news.cnet.com/news/0-1005-200-5826755.html?tag=lh

WHEN IS A BOOK NOT A BOOK? WHEN IT'S AN E-BOOK! [12 Jul 2001]
Federal District Judge Sidney H. Stein has ruled that the term "book" in a book contract does not automatically include the right to offer digital versions of that same book. Judge Stein therefore denied a request by Random House to enjoin RosettaBooks from publishing new digital editions of such Random House authors as Robert B. Parker, Kurt Vonnegut, and William Styron. The case will now go to full trial, although the judge said that "Random House is not likely to succeed on the merits of its copyright infringement claim." [(NY Times, 12 Jul 2001)]
http://partners.nytimes.com/2001/07/12/technology/ebusiness/12BOOK.html

---

Category 4B1 *Copyrights*

2001-08-02 **intellectual property moral rights actors streaming radio rebroadcast**

NewsScan

RADIO STATIONS HALT STREAMING OVER ACTOR DISPUTE [21 Apr 2001]
Hundreds of commercial radio stations have put a stop to Internet broadcasts, prompted by a dispute with the actors on commercials who want to be paid extra to have their voices streamed online. The American Federation of Television and Radio Artists (AFTRA) says the stations have known for months that they were responsible for paying the actors, and are shutting down to avoid paying record labels and artists, who also want extra payments for streamed broadcasts. Four of the largest U.S. commercial radio companies -- Clear Channel, Citadel Broadcasting, Emmis Communications and Jefferson Pilot Communications -- ended their real-time audio feeds last week. "We are working hard to resolve outstanding issues with all concerned parties," says Clear Channel CEO Kevin Mayer. "It is our intention to put the streams back up when it makes legal and financial sense." Mayer says his company is looking into technology that could strip the commercials out of the streams. (AP 21 Apr 2001)
http://news.excite.com/news/ap/010421/18/internet-radio

COURT BACKS ONLINE RADIO RULING [2 Aug 2001]
The broadcasting industry suffered a setback Wednesday when a U.S. district judge threw out a challenge to the U.S. Copyright Office, which ruled last year that radio stations must pay additional royalties to stream music over the Internet. The National Association of Broadcasters responded that the ruling would upset a long-standing, mutually beneficial relationship between the broadcasting and recording industries. "Broadcasters currently pay in excess of $300 million annually in music licensing fees to compensate songwriters and music publishers. Any additional fee to compensate record companies would be unfair and unreasonable," said NAB president and CEO Edward O. Fritts. The ruling was hailed as a victory by the Recording Industry Association of America. "Any licensing fees that these companies would be paying would pale in comparison... to the cost to stream their signal over the Internet," said RIAA senior VP Steven M. Marks. (AP 2 Aug 2001)
http://news.excite.com/news/ap/010802/22/online-radio

Category 4B1 *Copyrights*

2001-08-30 **music royalties copyright intellectual property distribution proposal legislation**

NewsScan

US REGULATORS FOCUS ON ONLINE MUSIC COPYRIGHT LAW [30 Aug 2001]
Questions on copyright laws for online music have been raised by Web companies, which contend that vague rules have enabled music publishers to seek multiple royalty payments that could stymie their fledgling industry. Currently, music publishers get paid in two ways: once when songs are performed and once when they are recorded. Some publishers have argued that they should be paid in both ways whenever Web users choose to hear a song online. The U.S. Copyright Office has therefore asked Congress to pass legislation that stipulates payment rules. The Copyright Office says online music services shouldn't have to pay royalties on "buffer" copies of songs that enable smoother audio streaming, and contends that when Web companies sell music downloads, they shouldn't have to pay a performance fee. The Digital Media Association characterized the Copyright Office's stand as a "home run," but music publishers were concerned that the recommended rules "may not adequately protect creators or copyright owners." (Wall Street Journal 30 Aug 2001)
http://interactive.wsj.com/articles/SB999125016154381702.htm (sub req'd)

Category 4B1 *Copyrights*

2001-12-07 **international intellectual property WIPO law treaty agreement moral rights related residual copyright protection**

NewsScan

WORLD COPYRIGHT LAW TO PROTECT DIGITAL WORKS [7 Dec 2001]
A World Intellectual Property Organization treaty protecting copyrighted digital works will go into effect in March, and a second WIPO treaty will protect the so-called "related rights" of performers, producers and broadcasters whose work is transmitted on the Internet. WIPO director-general Kamal Idris says the treaties "will let composers, artists, writer and others to use the Internet with confidence to create, distribute and control the use of their works within the digital environment." (AP/Washington Post 7 Dec 2001)
http://www.washingtonpost.com/wp-dyn/articles/A8037-2001Dec7.html

---

Category 4B1 *Copyrights*

2001-12-17 **copyright intellectual property journalists freelance writers Web CD-ROM Web republication derivative works moral rights residuals database CD-ROM Web publishing Webcast lawsuits court rulings judgements agreements**

NewsScan

ONLINE USE OF FREELANCE WORK TO BE DECIDED BY COURT [28 Mar 2001]
The U.S. Supreme Court is hearing a case about whether freelance authors are entitled to receive additional compensation when their articles are incorporated into electronic databases and commercial CD ROMs. On the side of the writers: organizations such as the American Library Association and the Association of Research Libraries. On the publisher side: the New York Times, Newsday, Time, AOL Time Warner, the Washington Post, Gannett, Lexis/Nexis, and UMI. The central issue is whether a published article entered into an archival database is a mere "revision" of the original work (in which case the publisher wins, since it has already paid for the work once), or whether the article must be considered an entirely new product (in which case the author wins). The writers argue that the search capabilities of databases give publications completely new and separate lives, for which the authors should get completely separate compensation. (Washington Post 28 Mar 2001)
http://washingtonpost.com/wp-dyn/articles/A1815-2001Mar27.html

FREELANCE WRITERS VS. PUBLISHERS [28 Mar 2001]
The U.S. Supreme Court heard oral arguments yesterday in a case that will decide what rights freelance writers have when their work is incorporated into electronic databases. Representing the publishers, Laurence H. Tribe insisted that an article is not made into something new just by being incorporated into a database, it is a mere "revision" of the original article that the publisher has already paid for and shouldn't have to pay for again. Representing the freelance writers, Laurence Gold argued that when publishers put articles into the "undifferentiated mass" of an electronic database they "are creating a quite different work." (New York Times 29 Mar 2001)
http://partners.nytimes.com/2001/03/29/technology/29WRIT.html

COURT SIDES WITH WRITERS OVER COPYRIGHT DISPUTE [26 Jun 2001]
In a blow to big media firms, the U.S. Supreme Court ruled Monday that freelance writers may control whether articles they write for print publication can then be reproduced in electronic form. Large publishers have argued that if they have to renegotiate over electronic publication rights, they probably will remove a substantial amount of material from their electronic databases. "Historians, scholars and the public lose because of the holes in history created by the removal of these articles from electronic issues of newspapers such as the Times," said New York Times chairman Arthur Sulzberger Jr. The ruling will affect primarily content written before the mid 1990s, which most publishers updated their contracts to include electronic as well as print publishing rights. The National Writers Union, however, estimates a range of potential liabilities between $2.5 billion and $600 billion. The decision in this case could have broad ramifications in similar disputes in the book and music publishing businesses. (Wall Street Journal 26 Jun 2001)
http://interactive.wsj.com/archive/retrieve.cgi?id=SB993473705172238884.djm (sub req'd)

LIBRARIANS LEFT TO CLEAN UP ELECTRONIC DATABASES [29 Jun 2001]
In the wake of the recent Supreme Court ruling over freelancers' right to control distribution of electronic versions of their work (Tasini et al. vs. the New York Times et al.), publishers are deleting tens of thousands of freelance articles spanning decades. And who gets stuck with the job? "The librarians, of course," says Tim Rozgonyi, assistant technology systems editor for the Pittsburgh Post-Gazette. "The librarians will save the publishers' bacon by cleaning up the data... [The] Tasini [decision] is the closest thing to a lifetime employment guarantee for news librarians that you will ever see." Meanwhile, some newspapers are turning back to microfilm, which is exempt from the ruling, to digitize a complete archive of their collections. But microfilm could prove another source of legal contention in the future. "The royalty potential [of digitizing over 100 years of microfilm] is massive," says Tampa Tribune archive and research manager Jody Habayeb. Some archivists have suggested that publishers could post citations only, rather than the full text of articles that don't comply with the Tasini ruling, but others argue that most users don't want to have to go through a third party to find an article online. "I hate to see it go that way, but it's an option," says Habayeb. "The beauty of the Internet is the immediacy of it." (Wired.com 29 Jun 2001)
http://www.wired.com/news/culture/0,1284,44905,00.html

NY TIMES "SOLUTION" NOT WHAT FREELANCE WRITERS HAD IN MIND [6 Jul 2001]
A Pyrrhic victory for freelance writers? Maybe. After the U.S. Supreme Court ruled last week that the New York Times (and two other publishers) had violated the rights of freelancers by not paying them new compensation for old material made accessible in electronic databases, the Times decided simply to remove the disputed material entirely. Characterizing the newspaper's action as a "complete violation of the spirit of the Supreme Court decision," the writers are insisting that "there is no need to delete articles" and are filing a new lawsuit. They say they want their works to remain in the databases, and merely want to be receive what they consider appropriate compensation. (New York Times 6 Jul 2001)
http://partners.nytimes.com/2001/07/06/technology/06WRIT.html

JOURNALISTS WIN ANOTHER CONTEST OVER DIGITAL RIGHTS [10 Oct 2001]
The U.S. Supreme Court has refused to hear an appeal by National Geographic after an appellate court sided with a photo journalist who sued the publication for including his work in CD-ROM form without his permission and without offering him additional payment. The freelancer's photographs had appeared in the National Geographic over three decades. (San Jose

Mercury News 10 Oct 2001)
http://www.siliconvalley.com/docs/news/svfront/072212.htm

GROUPS REACH TENTATIVE DEAL ON WEBCAST ROYALTIES [17 Dec 2001]
Attorneys representing radio broadcasters, record labels and music artists have signed a tentative settlement in an ongoing dispute over whether radio broadcasters owe additional royalty payments when they put their stations' programming online. If the deal is finalized, it could be an important step toward resolving the tangle of legal issues surrounding online music. Radio companies currently do not pay recording firms royalties on songs they broadcast over the airwaves and have argued that the exemption should apply to online "Webcasts" as well. That issue is now on appeal. The current agreement depends on the U.S. Copyright Office to support arbitration to resolve the question of a royalty rate to be paid by Internet-only Webcasters who offer music online but don't own any radio stations. (Wall Street Journal 17 Dec 2001)
http://interactive.wsj.com/articles/SB100854764550867360 0.htm

---

Category 4B1 *Copyrights*

2002-01-08 **copyright fair use intellectual property CD music DMCA amendment proposal legislation**

NewsScan

BILL AIMS AT PROTECTING RIGHT TO COPY DIGITAL FILES [8 Jan 2002]
Rep. Rick Boucher (D-Va.) says he will introduce legislation that would amend the Digital Millennium Copyright Act to protect consumers' right to make copies of digital files, such as songs on a CD. Boucher also has written a letter to the Recording Industry Association of America, suggesting that copy-protected CDs may violate the 1992 Audio Home Recording Act. Under that law, consumers pay a few cents extra each time they buy a blank CD, with the money going toward the recording industry to compensate them for potential losses caused by unauthorized copying. Boucher says, "I am particularly concerned that some of these technologies may prevent or inhibit consumer home recording." (Los Angeles Times 8 Jan 2002)
http://www.latimes.com/technology/la-000001793jan08.story?coll=la%2Dheadlines%2Dtechnology

---

Category 4B1 *Copyrights*

2002-03-01 **digital copyright protection embedded hardware legislation hearing conflict technologists movies music**

NewsScan

HOLLYWOOD, HIGH-TECH CLASH OVER PIRACY PROTECTION [1 Mar 2002]
The heads of several media and high-tech companies squared off yesterday before a panel of Washington lawmakers, presenting conflicting views of what should be done about digital copyright protection. The hearing was focused on legislation to be sponsored by Senate Commerce Committee Chairman Ernest Hollings (D-S.C.) that would require computer makers and consumer-electronics manufacturers to imbed copyright-protection technology in all of their products. The bill is backed by content providers, such as Walt Disney and News Corp., who accused the high-tech industry of hypocrisy in their opposition to technical safeguards for entertainment content. "They work hard to protect their own intellectual property. I would just like them to work modestly to protect the intellectual property of another industry," said Disney CEO Michael Eisner. Meanwhile, computer makers said it was unfair to place the burden of developing and installing copyright protection technology on them, warning that such technology could make it more difficult for consumers to legally record TV shows or music. "The focus in this debate needs to change from content protection to consumer protection," said Intel executive VP Leslie Vadasz. (Wall Street Journal 1 Mar 2002)
http://online.wsj.com/article/0,,SB101494577449898000.djm,00.html

---

Category 4B1 *Copyrights*

2002-03-06 **intellectual property international treaty laws music piracy circumvention encryption WIPO**

NewsScan

DIGITAL COPYRIGHT TREATY GOES INTO EFFECT
A landmark international copyright treaty, negotiated by the World Intellectual Property Organization in 1996, takes effect today [March 6, 2002] amid controversy over whether tougher copyright rules encourage or inhibit intellectual creativity in cyberspace. A companion treaty specifically protecting digital music goes into effect in May. Both treaties outlaw attempts to circumvent encryption and other techniques used to prevent unauthorized copying and to ensure royalty payments. The treaties have been criticized by civil liberties advocates who claim the prohibitions will stymie freedom of speech on the Net, but their views have met little sympathy either in the U.S. or abroad. WIPO Director General Kamil Idris says the treaties will provide a secure platform for creators to further exploit the Internet with confidence. (Financial Times 6 Mar 2002)
http://news.ft.com/news/industries/infotechnology

Category 4B1 *Copyrights*

2002-03-07 **intellectual property e-commerce lawsuit settlement business method patent**

NewsScan

AMAZON, BARNES & NOBLE SETTLE 1-CLICK DISPUTE
Amazon and Barnesandnoble.com have settled their long-running patent infringement lawsuit. Terms of the settlement were not disclosed. The lawsuit, filed by Amazon in 1999, alleged that Barnesandnoble.com used a customer checkout procedure that violated Amazon's patent on its "1-Click" checkout technology. The lawsuit was assailed at the time by critics who opposed "business method" patents granted for overly broad and unoriginal concepts. "Patents such as yours are the first step in vitiating the Web, in raising the barriers to entry not just for your competitors, but for the technological innovators who might otherwise come up with great new ideas that you could put to use in your own business," said technical publisher Tim O'Reilly in a letter to Amazon CEO Jeff Bezos. Bezos eventually suggested that business method patents should be limited to a three- to five-year life span, rather than the standard 20 years for patents. (Wall Street Journal 7 Mar 2002)
http://online.wsj.com/article/0,,SB1015466420659042800.djm,00.html (sub req'd)

Category 4B1 *Copyrights*

2002-03-12 **intellectual property residual rights authors publishers electronic distribution e-commerce**

NewsScan

E-PUBLISHER WINS ROUND TWO IN COURT
E-publisher RosettaBooks won a second legal round against Random House when a three-judge panel unanimously upheld an earlier ruling rejecting Random House's request for a preliminary injunction against Rosetta. RosettaBooks is selling electronic versions of Kurt Vonnegut's "Cat's Cradle" and seven other old Random House titles. RosettaBooks had reached contractual agreements with the authors or their representatives regarding the rights to electronic publishing, but Random House has argued that electronic rights are not implicit because e-books are simply another version of a paper book. A RosettaBooks victory in the case would open the doors for hundreds of old titles to become available in electronic versions. (AP 11 Mar 2002)
http://apnews.excite.com/article/20020311/D7I6HQ200.html

Category 4B1 *Copyrights*

2002-03-22 **intellectual property digital rights legislation law proposal fair use technical standard hardware**

NewsScan

HOLLINGS OFFERS BILL TO STOP ILLEGAL MUSIC AND VIDEO SHARING
Senator Ernest Hollings (D., SC) has introduced legislation that would require computermakers and Hollywood producers to agree on a technical standard that can be used to prevent computers and other devices from playing copyrighted digital files without permission. Media companies (such as Disney) favor the legislation, which protects their intellectual property, but computer and equipment companies (such as Intel) oppose it because it would restrict the functionality of new products. A Hollings aide says that the legislation respects traditional "fair use" rights for personal use. (Reuters/USA Today 22 Mar 2002)
http://www.usatoday.com/life/cyber/tech/2002/03/22/digital-piracy.htm

---

Category 4B1 *Copyrights*

2002-03-29 **international law copyright infringement judgement**

NewsScan

KAZAA JUDGMENT OVERTURNED BY DUTCH COURT
A Dutch appeals court has ruled that KaZaA, which makes software that enables users to download music, videos and other copyrighted material, is not liable for copyright infringement. The decision overturns a judgment rendered last November, which found KaZaA guilty of violating copyright law. The appellate court ruling maintains that it's the users of KaZaA's Media Desktop software who are the infringers, and adds that Media Desktop was not exclusively designed to pirate copyrighted works. (Reuters/Los Angeles Times 29 Mar 2002)
http://www.latimes.com/technology/la-000022513mar29.story?coll=la%2Dheadlines%2Dtechnology

---

Category 4B1 *Copyrights*

2002-05-05 **e-commerce advertising intellectual property consumer privacy rights**

RISKS 22 05

A chorus of protest arose over comments by television industry officials who criticized viewers who skip over commercials on TV (this was in connection with the TiVo digital recording device which allows such shocking behavior). Analogies included suggestions that anyone failing to read all the advertisements in a newspaper or magazine should be prosecuted; that deep linking should be outlawed and everyone should have to start at a home page and navigate according to the Web owners' intentions; and that blocking or even ignoring pop-up ads should also be criminalized.

Category 4B1 *Copyrights*

2002-05-13 **intellectual property copyleft copyright public access**

NewsScan

A 'CREATIVE COMMONS' FOR INTELLECTUAL PROPERTY
A new nonprofit organization called "Creative Commons" is being formed by a group of law and technology scholars who want to encourage owners of intellectual property to donate some of their material to the public domain. Their first goal is to create a set of licenses that would clearly state the terms under which the public would be invited to copy a particular work and to make such works easy to identify and search for on the Web. The chairman of Creative Commons is Stanford law professor Lawrence Lessig, an intellectual property expert. (New York Times 13 May 2002)
http://partners.nytimes.com/2002/05/13/technology/13FREE.html

---

Category 4B1 *Copyrights*

2002-05-21 **intellectual property music license fees radio commercial non-commercial Internet**

FindLaw Download This 86

WEBCASTERS SPARED EXTRA ROYALTIES
Associated Press / Wired

The Librarian of Congress has rejected proposed royalty rates that would have charged Internet broadcasters based on each Web user that listens in. Librarian James H. Billington will issue a final decision setting the new rates by June 20, the U.S. Copyright Office said Tuesday. The Copyright Office ruled in December 2000 that organizations distributing music and other radio content over the Internet must pay additional fees to record companies that hold song copyrights. In February, an arbitration panel proposed rates based on each person who is receiving a broadcast sent online. The rates ranged from .07 of a penny per song for a radio broadcast to .14 of a penny for all other copyrighted audio sent on the Internet.

http://www.wired.com/news/politics/0,1283,52691,00.html

U.S. Copyright Office
http://www.loc.gov/copyright/

Category 4B1 *Copyrights*

2002-05-23 **TV television commercials advertising broadcasting research consumer recording**

NewsScan

NETWORKS REALLY WISH YOU'D WATCH THE COMMERCIALS
A survey from NextResearch reports that 20% of the people who own digital video recorders (DVR) from TiVo or Replay TV never watch any commercials -- a finding that is scaring the advertising and broadcasting industry. Jamie Kellner of Turner Broadcasting warns that if DVR technology destroys the economics of paid advertising, the result will be the rapid expansion of pay-TV: "The free television that we've all enjoyed for so many years is based on us watching these commercials. There's no Santa Claus. If you don't watch the commercials, someone's going to have to pay for television and it's going to be you." And Daniel Jaffe of the Association of National Advertisers concurs: "You start losing marginal dollars when people who you thought you were buying are not viewing. This is not just a theoretical problem that might be happening somewhere down the line. This is happening now." What should advertisers do? Mollie Watson, a product manager for Best Buy, thinks their only hope is to do a better job and "put advertisements out there that people are actually going to choose to watch." Apparently there are such things. (New York Times 23 May 2002)
http://partners.nytimes.com/2002/05/23/technology/23VIDE.html

---

Category 4B1 *Copyrights*

2002-05-28 **privacy surveillance Web browsing class action lawsuit**

FindLaw Download This 87

COMCAST SUED OVER WEB RECORDINGS
Comcast Corp., the nation's third-largest cable company, is being sued in U.S. court in Michigan over accusations it violated a federal privacy law when it recorded the Web browsing activities of each of its 1 million high-speed Internet subscribers. Lawyer Steven Goren of Bingham Farms, Mich., filed a class-action complaint against Comcast and its cable subsidiary Tuesday. Goren, who predicted "months or years" of litigation, is seeking attorney's fees plus damages of at least $100 per day for every Comcast subscriber during the period from December to Feb. 13, when Comcast pledged to stop the practice.
http://news.findlaw.com/ap/ht/1700/5-25-2002/20020525103003_17.html

Cyberspace Privacy Resources
http://www.findlaw.com/01topics/10cyberspace/privacy/

Category 4B1 *Copyrights*

2002-06-07 **lawsuit rights fair use copyright intellectual property advertising recording replay**

NewsScan

IS THERE A LAW THAT SAYS YOU HAVE TO WATCH COMMERCIALS?
Surely there isn't -- says Rep. Rick Boucher (D-Va.) in his support for a consumer lawsuit seeking to confirm that users of Sonicblue's ReplayTV system have the lawful right to skip commercials when they record TV programs for later viewing. The suit has been filed in the same federal court in Los Angeles that is hearing a complaint from movie and television studios that ReplayTV allows customers to violate their copyrights, arguing that skipping commercials amounts to stealing. Sonicblue's position is: "Basically we believe that consumers have 'fair-use' rights, and everything consumers do with a ReplayTV is covered with 'fair use'." (Reuters/USA Today 6 Jun 2002)
http://www.usatoday.com/life/cyber/tech/2002/06/06/replaytv-sue.htm

---

Category 4B1 *Copyrights*

2002-06-21 **intellectual property music license fees radio commercial non-commercial Internet**

NewsScan

WEB RADIO ROYALTY RATE CUT IN HALF
Librarian of Congress James H. Billington has reduced the proposed royalty rate to be paid by Internet-only radio stations to 0.07 cents per song per listener -- half of the rate proposed by arbitrators last February. The rate now matches that proposed for traditional radio stations that also put their broadcasts on the Web. It will remain in effect only until the end of this year, when a new, as-yet-undetermined rate is supposed to take effect. The new, reduced rate came under fire from both sides, with Webcasters complaining it was still too high, and the Recording Industry Association of America arguing that it meant that "artists and record labels will subsidize the Webcasting businesses" of big Internet and radio companies, and that the fee "simply does not reflect the fair market value of the music as promised by the law." On the other side of the issue, the National Association of Broadcasters said the rate "places a prohibitive financial burden on radio-station streaming and will likely result in the termination of this fledgling service to listeners." (Wall Street Journal 21 Jun 2002)
http://online.wsj.com/article/0,,SB1024608353756633200.djm,00.html

EDUPAGE editors added the following information:

WEB RADIO FEES SET
A final schedule of fees that radio stations must pay record companies for playing music online has been released by James Billington, the Librarian of Congress. College radio stations claim that the fees are too high and will put them out of business, while the Recording Industry Association of America say they are too low and don't fairly recompense artists and recording studios. The fees are two-hundredths of a cent per listener per song for noncommercial stations and seven-hundredths of a cent for commercial radio stations. A minimum fee of $500 per year will be assessed on all radio stations that play music online, and the fees are retroactive to October 1998, when the Digital Millennium Copyright Act took effect. (Chronicle of Higher Education, 21 June 2002)
http://chronicle.com/free/2002/06/2002062101t.htm

Category 4B1 *Copyrights*

2002-07-15 **lawsuit Web intellectual property advertisments**

NewsScan

PUBLISHERS SUE WEB SITE FOR MISAPPROPRIATING THEIR ADS
A group of major U.S. publishing companies, including the Washington Post Company and the New York Times Company, is suing Gator Corp., a Web site operator based in Redwood City, California, for taking ads on the publishers' Web sites and reselling them on Gator sites without authorization. The publishers say the misappropriation amounts to unfair competition with them, since Gator's competing offer to advertisers makes it harder for publishers to sell ads themselves. (Washington Post 27 Jun 2002)
http://www.washingtonpost.com/wp-dyn/articles/A52132-2002Jun26.html

PUBLISHERS WIN ONE AGAINST GATOR
Federal Judge Claude Hilton on Friday granted a motion for a temporary injunction that will force software firm Gator to stop displaying pop-up advertising over Web publishers' pages without permission. The ruling came in response to a lawsuit filed last month by The Washington Post, The New York Times, Dow Jones and seven other publishers, which alleges Gator's ads violate their copyrights and steal their revenue. The suit seeks a permanent injunction against Gator's ads and monetary damages for any advertising revenue derived from the publishers' Web pages. Gator develops software that manages passwords and fills out forms for about 10 million Web surfers who often download the application unwittingly through other popular file-sharing programs. Bundled in the software is a program called OfferCompanion that monitors the user's surfing habits and delivers targeted pop-up ads based on that information. For instance, if a surfer visits Toyota.com, Gator might launch a pop-up ad for Ford Motor. According to the lawsuit, Gator is "essentially a parasite on the Web that free rides on the hard work and the investments of plaintiffs and other Web site owners. In short, Gator sells advertising space on the plaintiffs' Web sites without their authorization and pockets the profits from such sales." (CNet News.com 12 Jul 2002)
http://news.com.com/2100-1023-943515.html

Category 4B1 *Copyrights*

2002-08-06 **intellectual property digital images advertising**

NewsScan

DIGITAL ALTERATIONS IN 'SPIDER-MAN' OKAYED AS FREE SPEECH
A federal judge in New York has thrown out a lawsuit filed by billboard and building owners against Sony and other companies involved in making and distributing the movie "Spider-Man," saying that digital alterations of the billboards in Times Square for the movie are protected free speech. "What exists here is for artistic purposes a mixture of fictionally and actually depicted Times Square? this has First Amendment protection," ruled Judge Richard Owen. In the "Spider-Man" movie and trailers, ads for companies such as Cingular Wireless and USA Today were superimposed over those of Samsung and NBC. The judge also rejected claims that Sony's use of lasers to digitally film the buildings amounted to trespassing: "Light beams bounce off the plaintiff's three buildings day and night in the city that never sleeps," said Owen. The practice of altering real-life scenes for the purpose of film artistry or to satisfy marketing deals is becoming more common as digital technology makes it easy to do so. USA Today said it didn't pay for the advertising, but Cingular said it has a marketing deal with Sony tied to the film. (CNet News.com 6 Aug 2002)
http://news.com.com/2100-1023-948441.html?tag=fd_top

Category 4B1 *Copyrights*

2002-08-13 **copyright intellectual property control surveillance tracking court order lawsuit injunction commercials advertisements recording swapping exchange**

NewsScan

SONICBLUE WINS TEMPORARY REPRIEVE ON TV TRACKING ORDER
SONICblue, maker of the ReplayTV digital video recorder, has won a stay of a court order that would have forced it to track the television viewing habits of its customers. Movie studios, including Paramount and Walt Disney, have sued the company, saying that the recording features included in the ReplayTV devices, including the ability to skip commercials and exchange recorded programs with other users, enable users to violate studios' copyrights. Consumer advocates have objected to the court order, calling it an invasion of privacy. (Reuters 15 May 2002)
http://story.news.yahoo.com/news?tmpl=story&cid=581&ncid=581&e=4&u=/nm/20020515/tc_nm/tech_sonicblue_dc_2

CONSUMER SUIT SIDETRACKED IN HOLLYWOOD-VS.-REPLAYTV
A federal judge has brushed to the side legal efforts by the Electronic Frontier Foundation on behalf of five owners of ReplayTV systems who claim they are threatened by a lawsuit against SonicBlue, the Santa Clara company that makes that device. The ReplayTV 4000 system is an advanced recording device that allows watchers to make digital copies of TV shows and to skip commercials, and SonicBlue is being sued by 28 movie studios and TV networks on the grounds that the device encourages piracy and its widespread adoption would harm the industry. The Electronic Frontier Foundation and the consumers it represents argue that the decision would affect them and even make them indictable for piracy, and that they should therefore be allowed to participate in the lawsuit; however, Judge Florence-Marie Cooper says that "many, if not all" of their issues can be resolved by the trial without their direct input. (San Jose Mercury Times 12 Aug 2002)

Category 4B1 *Copyrights*

2002-09-05 **DMCA Digital Millennium Copyright Act extension lawsuit inttellectual property**

NewsScan

DUKE LAW SCHOOL TO CHALLENGE COPYRIGHT LAW EXPANSION
Duke University's law school has received an anonymous $1 million gift earmarked for a new Center for the Study of Public Domain, which will focus on finding "the correct balance" between intellectual property rights and material that ought to be part of the public domain. Center co-director James Boyle says one target of study will be the 20-year extension of copyright duration contained in the Digital Millennium Copyright Act. Boyle says he is not a copyright abolitionist, but adds, "The burden of proof should be on those who say we need to have property rights in this situation? Why is this necessary? We see the system getting out of control, out of balance? If you want to have a rich culture an innovative society, you have to leave a large amount of material freely available for all to use." (CNet News.com 4 Sep 2002)
http://news.com.com/2100-1023-956637.html?tag=fd_top

Category 4B1 *Copyrights*

2002-09-20 **intellectual property music license fees radio commercial non-commercial Internet**

NewsScan

WEB RADIO STATIONS OBJECT TO PAYING ROYALTIES
Told last month by a federal court that they would have to pay seven one-hundredths of a cent in royalties to record companies every time one of its listeners hears a copyrighted song transmitted over the Web, a group of radio stations led by the National Association of Broadcasters (NAB) and Clear Channel Communications is appealing that ruling to a higher court. The appeal challenges the right presumed right of the Copyright Office to set the royalty rates. (Bloomberg/New York Times 17 Jul 2002

ROYALTY FEES MAY BE THE DEATH OF INTERNET RADIO
All kinds of radio stations — both Web-based and traditional over-the-air broadcasting stations — have to pay copyright royalties to songwriter associations, but only the Web stations are required to pay a new performer's fee that goes to record companies. At a rate of seven-hundredths of a cent per song per listener, the fee is expected to undo the economic viability of almost all of the 10,000 Web radio stations now in existence. The 200 stations that have already ceased operations include nonprofit stations at UCLA, NYU, and other colleges and universities, and people seem to be punching different calculators to attack or defend what's going on: Congressman Rick Boucher (D, VA) is introducing a bill in support of small Webcasters and says its goal is "to make sure that Webcasters who measure their revenues in the tens of thousands are not put out of business by a copyright payment requirement in the hundreds of thousands."; using a different calculator, Hilary Rosen of the Recording Industry Association of America (RIAA) says that most college stations won't owe more than $500 a year, and adds, "Given our problems with digital piracy on university servers, it is almost comical that they have the nerve to complain about $500." (USA Today 21 Jul 2002)

WEBCASTERS LOBBY AGAINST ROYALTY ASSESSMENTS
Internet-radio proponents swarmed Capitol Hill Thursday to urge Congress to delay or lower the royalties they will have to begin paying record labels beginning Oct. 20. The webcasters have argued that the rates are too high for a new medium and are planning to appeal the rate of 0.07 cent per song per listener, which was set last June by the Librarian of Congress. The music companies are also appealing the rates, which they say are too low. The two groups are engaged in discussions in an effort to head off dueling lawsuits, but so far the talks have not produced a settlement. Some Internet radio firms and broadcasters have already shut down their webcasting operations, at least in part because of the upcoming royalty payment. "It was purely an economic decision," says the CEO of Jefferson-Pilot Corp.'s radio operations, which has stopped streaming 15 of its 17 stations online because of the fees. (Wall Street Journal 20 Sep 2002)

Category 4B1 *Copyrights*

2002-10-04 **intellectual property copyright copying consumer rights bill proposed legislation**

NewsScan

NEW COPYRIGHT BILL WOULD GIVE POWER TO THE PEOPLE
Rep. Rick Boucher (D-Va.) and Rep. John Doolittle (R-Calif.) have introduced legislation aimed at restoring specific fair use rights to copy digital works that were lost under the 1998 Digital Millennium Copyright Act, as well as bestowing "circumvention" rights to bypass copy protections when done "solely in furtherance of scientific research." The Digital Media Consumers Rights Act has drawn support from a broad coalition of electronics and computer interests, consumer groups and academics. "It's just time," said Consumer Electronics Association president Gary Shapiro. "Consumers have been pushed up against the ropes. This is the first time in 20 years in which consumers are going on the offense rather than on the defense." Meanwhile, entertainment groups bemoaned this latest development in the battle over digital media rights. "If this bill were to be enacted, content owners would be left with two unhappy choices: Protect their valuable works by not making them available in digital formats such as DVD, or lose all control over unauthorized reproduction and distribution," said Jack Valenti, president of the Motion Picture Association of America. The bill has no chance of passage this year, but will set the stage for debate in the next session of Congress. (Wired.com 4 Oct 2002)
http://www.wired.com/news/politics/0,1283,55569,00.html

Category 4B1 *Copyrights*

2002-10-09 **intellectual property copyright royalties fees Web radio broadcasters**

NewsScan

COMPROMISE SOUGHT ON WEBCASTER ROYALTY FEES
Congressman F. James Sensenbrenner (R-Wisc.) is hoping that new legislation will help preserve small, independent Internet radio stations, which are threatened with insolvency because of the royalty fees imposed by a Library of Congress Copyright Arbitration Panel. The Panel had established flat fees for Web broadcasting of copyrighted music, whereas under the proposed legislation smaller stations would calculate music royalty fees as a percentage of revenue. The proposal is controversial, and an executive of Live365.com, a group of Web radio stations, says it's not much different from the current arrangement. (San Jose Mercury News 2 Oct 2002)

HOUSE APPROVES ROYALTY SCHEDULE FOR WEB RADIO OPERATORS
The U.S. House of Representatives has approved an arrangement that will allow smaller Web radio stations to pay a percentage of revenue or expenses (whichever is larger) rather than a flat per-song rate of .07 cents a song as was set by the Library of Congress. The deal still has to go to the Senate, but approval there seems highly likely. (Reuters/USA Today 9 Oct 2002)

Category 4B1 *Copyrights*

2002-10-10 **copyright extension judicial review lawsuit legislation constitutionality**

NewsScan

COURT TO REVIEW COPYRIGHT EXTENSION LAW [20 Feb 2002]
The U.S. Supreme Court announced it will review a challenge to a 1998 law that extends by 20 years the lifetime of all existing copyrights and increases the lifetime of future copyrights from 50 to 70 years after the death of the creator. The legislation, called the Sonny Bono Copyright Term Extension Act, was named after the late Sonny Bono, congressman and former entertainer. Stanford University law professor Lawrence Lessig, an attorney for one of the groups seeking to declare the legislation unconstitutional, says the case is important "so that the next Walt Disney can do to Disney what Disney did to Grimm's fairy tales" — entirely transform material taken from the public domain. But the court likely will focus not on the substance of the law but on the issue of whether the law extends a copyright's duration far longer than what was envisioned by the framers of the Constitution. Wayne State University law professor Jessica Litman argues: "It's important for the Supreme Court to reassert that there's no copyright exception in the Constitution that Congress can do whatever it pleases. Congress has limited powers." Lawyers for the government insist that there are no legal precedents barring Congress from enacting the legislation. (Washington Post 20 Feb 2002)
http://washingtonpost.com/wp-dyn/articles/A35750-2002Feb19.html

COURT TO REVIEW COPYRIGHT-EXTENSION LAW [10 Oct 2002]
The U.S. Supreme Court has accepted the first copyright case in decades — a constitutional challenge to the Sony Bono Copyright Term Extension Act, which Congress passed in 1998 to extend copyright protections an additional 20 years. Under the law, creative works by an individual (such as Ernest Hemingway) are protected for 70 years after the person's death, and works by a corporation (such as the Disney Corp.) are copyright-protected for 95 years from the date of their creation. Stanford University law professor Lawrence Lessig told the court: "Just at the time that the Internet is enabling a much broader range of individuals to draw upon and develop this creative work without restraint, extensions of copyright are closing off this medium to a broad swath of our common culture." In rebuttal, the Solicitor General's position is that the issue is one that should be addressed to the legislature, not to the courts. (San Jose Mercury News 9 Oct 2002)

Category 4B1 *Copyrights*

2002-12-02 **copyright intellectual property patents lawsuit precedent**

NewsScan

FILE-SHARING'S FATE HANGS ON BETAMAX RULING
Like the previous lawsuits that shuttered Napster and Aimster, the latest lawsuit brought by the major record labels against peer-to-peer file-swapping networks will hinge on a legal precedent set in 1984 when the Supreme Court ruled that Sony wasn't liable for copyright infringement because its Betamax VCRs had "substantial" legitimate uses as well as illegal ones. That argument proved insufficient in the earlier cases, in part because Napster and Aimster kept central directories of the files on users' computers, and were therefore in a better position to know what their users were doing. The companies now under fire — Morpheus, Kazaa and Grokster — don't maintain any central directories, and their lawyers say that means they have no way to monitor or control what their users do. However, to bolster their case, the companies behind Morpheus, Kazaa and Grokster are now encouraging copyright owners to use file-sharing technology as a legitimate promotional or distribution tool — for instance, by offering independent musicians the means to disseminate sample songs. In a joint brief Monday, however, the record companies indicated they're not fooled by that tactic and have reiterated their position that the companies should be held accountable for widespread piracy on their networks. "The Supreme Court in deciding the Sony case couldn't have intended to permit a massive system of infringement to be called exempt from the copyright law. It just defies reason to think otherwise," says one copyright expert. (Los Angeles Times 10 Sep 2002)

COURT HEARS ARGUMENTS AGAINST FILE-SWAPPING FIRMS
A federal court is scheduled to hear arguments by entertainment attorneys today, urging the judge to grant a "summary judgment" in their lawsuit against the Morpheus and Grokster file-swapping networks. The defendants have responded by asking that the case be dismissed and that they be allowed to distribute their software unmolested. If the case does go to trial, it will be the first time that any of the peer-to-peer companies have made it that far in the legal process — Napster and Madster (formerly Aimster) fell into bankruptcy before a full trial could be held. Legal experts agree that the copyright holders' case is potentially more influential than the suit against the now-defunct Napster, and that a full trial would set an important legal precedent for the technology community. Meanwhile, the file-swapping software remains popular: according to Download.com, Morpheus was downloaded nearly 400,000 times last week and Grokster 112,000 times. Kazaa, which the entertainment groups are hoping to add to the current lawsuit, remained the most popular, with more than 3.4 million downloads last week. (CNet News.com 2 Dec 2002)
http://news.com.com/2100-1023-975618.html

Category 4B1 *Copyrights*

2002-12-04 **intellectual property e-commerce distribution licensing electronic publishing copyright authors' rights**

NewsScan

RANDOM HOUSE, ROSETTA END QUARREL OVER E-BOOKS
Random House has settled its lawsuit against RosettaBooks over Rosetta's sales of electronic versions of eight popular titles, including Kurt Vonnegut's "Cat's Cradle" and William Styron's "Sophie's Choice." Rosetta will continue to publish the disputed works and will work with Random House on bringing additional titles to the e-book market. "We are very glad to be able to put our differences behind us and to now work collaboratively rather than combatively to enhance RosettaBooks' and our commitment to electronic publishing," said Random House senior VP Katherine J. Trager. The case has been watched closely by other publishers, but Wednesday's settlement leaves the core issue in the lawsuit unresolved — whether the rights to publish electronic versions of books are implied and therefore covered in contracts signed with authors in pre-Internet days. "The settlement seems neutral about rights ownership; it doesn't move things forward or back," says Paul Aiken, executive director of the Author's Guild, which represents thousands of published authors. (AP 4 Dec 2002)
http://apnews.excite.com/article/20021204/D7NN77LO0.html

Category 4B1 *Copyrights*

2003-01-08 **copyright laws international variations**

NewsScan

EU COPYRIGHT LAWS SPAWN 'FREE-SWAPPING ZONE' FOR OLDIES
European and Canadian copyright protections for audio recordings last just 50 years, compared with 95 years in the U.S., a disparity that has spawned a boomlet in legitimate sales of golden oldies from 1950s artists, ranging from Miles Davis to Elvis Presley. The expiration of music copyrights overseas just adds one more piece to an antipiracy puzzle that is growing increasingly complex. "There are some implications for enforcement, creating an additional wrinkle," says Neil Turkewitz, executive VP for international affairs at the Recording Industry Association of America. "But it doesn't affect the legality of a U.S. user accessing a foreign hard drive and downloading a file." Record industry officials say they are keeping an eye out for the emergence of Web sites that offer archives of material that is in the public domain in a foreign country but still illegal to trade freely in the U.S. If a Web-based service comes online, it may be possible to block access to the site from the U.S. by going through ISPs, says Turkewitz. Trying to shut down peer-to-peer services would be more difficult, however, he acknowledges. That's part of the reason that the RIAA has been pressuring European policy-makers to extend their copyright protections to match those of the U.S., but so far those efforts have met with little success. (CNet News.com 7 Jan 2003)
http://news.com.com/2100-1023-979532.html

Category 4B1 *Copyrights*

2003-01-14 **intellectual property copyright digital rights technology negotiation**

NewsScan

TECH FIRMS, HOLLYWOOD HEADED TO NEGOTIATING TABLE
About 20 lobbyists representing technology and entertainment companies are headed for a closed-door meeting today to try to hammer out some of their differences in the long-running squabble over digital copyright. Companies and trade associations represented at the meeting will include: Microsoft, Verizon, the Business Software Alliance, AOL Time Warner, the Motion Picture Association of America and the Fox Entertainment Group. "We're pleased that so many people who are important players in this debate are willing to sit down with us to discuss the consumer perspective on digital copyright," says Alan Davidson, deputy director of the Center for Democracy and Technology, which is sponsoring the series of meetings. "We don't know what the outcome will be, but we're hopeful that we can make progress in representing what has been an underrepresented voice — consumers." Political tension between the two groups has increased significantly in the last year, which has resulted in an impasse. (CNet News.com 21 Nov 2002)

MUSIC, TECH GROUPS REACH COMPROMISE ON COPYRIGHT ISSUES
The Recording Industry Association of America, the Business Software Alliance and the Computer Systems Policy Project have hammered out a compromise agreement that they say will protect copyrights on music and movies without the need for further government intervention. The pact is intended to head off efforts by Congress to legislate the inclusion of government-approved copy restriction technology in all new "digital media devices." This latest agreement, described by participants as a "landmark consensus," politically isolates the powerful Motion Picture Association of America, which was noticeably absent from the negotiations. MPAA has aggressively advocated new government requirements for built-in locking controls on new devices, such as DVD players. (AP 14 Jan 2003)

Category 4B1 *Copyrights*

2003-01-23 **copyright law intellectual property fair use**

NewsScan

COPYRIGHT LAW IS A TWO-WAY STREET
Robin Gross, head of the new watchdog group IP Justice and former Electronic Frontier Foundation attorney, says copyright holders are taking unfair advantage of new technologies to restrict use of their content: "Sure, (digital technology) makes it easier for people to copy and share works, but digital technology also makes it easier for copyright holders to restrict what people can do with their works. So it's not fair to say that this technology is very harmful to these industries because it's actually providing them with more power than they've ever had before to control what people can do with their works. That point is often overlooked — that they're controlling it to the point that they're taking away from the public side of the copyright bargain. So while it's not fair for consumers to copy and distribute copyright works in a fashion that doesn't compensate the creators, it's also not fair for the creators to use digital technology to take away the rights of the public. For example, making sure these works fall into the public domain at some point, or making sure that consumers are able to exercise their fair-use rights. It's simply not fair for the copyright holders to take all of the rights and have none of the responsibilities associated with copyright law." (CNet News.com 23 Jan 2003)
http://news.com.com/2008-1082-981663.html

Category 4B1 *Copyrights*

2003-01-24 **copyright intellectual property organization lobby battle**

NewsScan

HIGH-TECH GROUP BATTLES HOLLYWOOD ON COPYRIGHT ISSUES
The Alliance for Digital Progress (ADP) — a new Washington, D.C.-based lobbying group whose members include Microsoft, Dell, Motorola and the Information Technology Association of America (ITAA) — will fight Hollywood's positions on access to digital music, movies, and books, and the entertainment industry's efforts to require anti-copying technology in digital entertainment devices. ITAA president Harris N. Miller says sarcastically that Hollywood leaders "would have organized to burn down Gutenberg's printing press, if they were alive during that period of rapid change and innovation." (AP/USA Today 24 Jan 2003)

Category 4B1 *Copyrights*

2003-02-03 **copyright intellectual property sanitizing censorship bowdlerizing video TV television lawsuits**

NewsScan

HOLLYWOOD THREATENED BY CONTENT-CLEANSING SOFTWARE
The entertainment industry is taking aim at new technology that has spawned a growing business dedicated to cleaning up movies and TV programs. On one side are a chain of video rental stores and a number of software companies that cater to an audience sick of gratuitous sex, violence and foul language in today's Hollywood offerings. On the other are film studios and the Directors Guild of America (DGA). The two groups are at legal loggerheads over software, such as MovieMask and ClearPlay, which filter out objectionable content, either by skipping certain frames entirely, or by substituting new dialogue, or in some cases by clothing naked actors or turning steel swords into light sabers. Last August, the owner of a Colorado "CleanFlicks" video store, which rents sanitized video tapes, fired the first volley by suing the DGA and asking a federal judge to declare the editing practices protected under federal copyright law. The following month, DGA filed a countersuit against CleanFlicks as well as the software companies that do the editing. Eight Hollywood studios have now joined DGA's fight, alleging that the companies violated trademark law when they rent or sell an altered movie in the original packaging. Meanwhile, moviemakers warn that the same software used to sanitize content could also be used to spice up G-rated fare. "It's a double-edged sword," says Jack Valenti, head of the Motion Picture Association of America. "If there are people who want to do it for benign reasons, that's one thing. But they can take 'Spider-Man' and make it into a pornographic movie, and that's a problem." A hearing on the CleanFlicks case is scheduled for Feb. 14. (AP 3 Feb 2003)
http://apnews.excite.com/article/20030203/D7OV77582.htm

Category 4B1 *Copyrights*

2003-02-21 **copyright intellectual property music P2P peer-to-peer swapping piracy international court ruling**

NewsScan

MUSIC INDUSTRY THREATENED BY DUTCH RULING
A court ruling in the Netherlands last March appears to provide legal protection for businesses that enable peer-to-peer services, where users can swap copyrighted songs and movies for free. The Dutch decision is being appealed, but the ruling demonstrates the breadth of the challenge facing music companies and other owners of copyrighted works as more P2P providers move their operations overseas. Still, record-label officials maintain that the Netherlands ruling was an aberration that will be reversed in the appeals process, noting that courts in South Korea and Japan have ruled against P2P services in copyright cases. "We intend to enforce our rights not just in the United States, but worldwide," says Cary Sherman, president of the Recording Industry Association of America. Meanwhile, when U.S. courts side with the music industry, as in last month's federal ruling against Sharman Networks, which is based in Vanuatu and offers Kazaa file-swapping software, the question of enforcement looms large. "How are they going to enforce" the judgment, questions one of Sharman's lawyers. And even in the Netherlands case, a U.S. judgment isn't automatically enforced, says Tim Kuik, director of Brein, a Dutch foundation that deals with copyright enforcement, but would probably have to go through a separate Dutch court proceeding. (Wall Street Journal 21 Feb 2003)

Category 4B1 *Copyrights*

2003-03-11 **intellectual property copyright copying consumer rights bill proposed legislation**

NewsScan

BILL AIMED TO PROTECT CONSUMERS' DIGITAL MEDIA RIGHTS
New legislation called the "Digital Choice and Freedom Act" is being introduced in Congress by Zoe Lofgren (D-Calif.) to ensure that consumers may legally copy CDs, DVDs, and other digital works for their personal use, just as they do now with TV shows and audio tapes. Paula Samuelson, a law professor at University of California-Berkeley's Boalt Hall, says: "Lofgren's bill aims to restore what Congress thought it was doing [when it passed the 1998 Digital Millennium Copyright Act] — preserving fair use for people who have lawful rights to use stuff. The Lofgren bill offers meaningful protections for a number of ordinary activities by consumers that should be lawful under copyright law but about which the law is presently ambiguous." (San Jose Mercury News 1 Oct 2002)

LEGISLATION TO ESTABLISH DIGITAL COPYING RIGHTS
Rep. Zoe Lofgren (D, CA) is reintroducing legislation called the Balance Act, intended to give people the right to make back-up copies of copyrighted digital works for use on other devices (such as car CD players) and to protect consumers who break technological locks in order to view DVD movies on their computers. Lofgren says, "Most people — at least, most adults — don't expect to get content as a freebie. But when people pay good money to buy something and then can't use it in the way they've become accustomed to, it makes them mad." The Motion Picture Association of America (MPAA) and the Business Software Alliance (BSA) strongly oppose the proposed legislation, which is thought to have just a long-shot chance of being passed. Arguing that such legislation "would provide safe harbor for pirates," Jack Valenti of the MPAA said, "As drafted, this legislation essentially legalizes hacking." (San Jose Mercury News 11 Mar 2003)

Category 4B1 *Copyrights*

2003-03-27 **copyright Internet download peer-to-peer P2P issues PDF**

NewsScan

WHEN IS A FREE DOWNLOAD NOT?
It seemed like a good idea at the time — author Glen Fleishman reasoned that by offering his book, "Real World Adobe GoLive 6," as a free download, he might be able to kickstart sales, which were languishing. Rather than taking the time to download the 922 pages of the PDF file, maybe readers would decide to buy a hard copy on Amazon or elsewhere. It turns out that instead of the few hundred downloads that Fleishman was anticipating, the book was downloaded 10,000 times in just 36 hours, racking up a bandwidth bill of $15,000 (Fleishman's provider, Level 3, charges incrementally for bandwidth used). "It's a financial catastrophe. I'm a working stiff with a mortgage… I never suspected the penalty would be so high for giving something away… It's like living in Singapore and getting 15 years in jail for chewing gum… I was aware I would be charged a fortune for high bandwidth. But I never suspected we would have topped a few hundred downloads." Fleishman could have made use of file-sharing networks like Kazaa or Gnutella, which require users to bear the cost, says sci-fi author Cory Doctorow, who recently released his first novel, "Down and Out in the Magic Kingdom," as a free download. Alternatively, Fleishman could have released the book under an open Creative Commons license, which would have allowed it to be posted to the Internet Archive and other open content Web sites, says Doctorow. "It doesn't make any sense to be the sole point of distribution for a file like this. It highlights the design flaw in the client-server Internet. The more popular a file becomes, the more of a penalty people pay to get it. I think the lesson is 'Use P2P networks.'" (Wired.com 27 Mar 2003)

Category 4B1 *Copyrights*

2003-03-27 **music webcasting copyright issues reform held**

NewsScan

PANEL PUTS WEBCAST ROYALTIES REFORM ON HOLD
A House subcommittee has indefinitely postponed deliberation of a new bill, titled the Copyright Royalty and Distribution Act, which calls for the Library of Congress to hire a full-time judge to settle disputes over "reasonable" copyright royalty fees for webcasts. The measure, sponsored by Reps. Lamar Smith (R-Texas) and Howard Berman (D-Calif.), had been expected to receive a favorable reception at today's hearing. Fees for streaming music via the Internet have been a bone of contention since the enactment of a 1998 copyright law in which Congress required webcasters to pay record labels and artists a royalty fee for playing their music online. Under the Smith and Berman bill, the appointed judge would be required to consider a "fair income" for the copyright holder and could adjust rates for inflation. (CNet News.com 27 Mar 2003)

Category 4B1 *Copyrights*

2003-05-14 **dvd copying court District Court 321 studios Digital Millennium Copyright Act's anti-circumvention**

NewsScan

BATTLE OVER DVD-COPYING HEADS TO COURT
U.S. District Court Judge Susan Ilston in San Francisco will be overseeing a case that analysts say will have important ramifications not only for software developers and the movie industry, but also for consumers who want to make back-ups of the DVDs they buy. Seven major movie studios have filed suit against software startup 321 Studios, seeking to prohibit it from shipping its DVD X-Copy and DVD Copy Plus software programs. The lawsuit invokes the 1998 Digital Millennium Copyright Act's "anti-circumvention" provision, which bans the sale of products that can "get around" copyright protection measures. Legal experts say this case is of particular interest because Judge Ilston is being asked to clarify whether the law prevents all circumvention, or whether there are cases in which circumvention is legal. "That's a big open issue that this will help define," says an intellectual property lawyer, who adds, "This is one of the first tough cases" to address this issue. Courts in the past have allowed copyright exemptions for personal use, such as using a VCR to record a TV show for later viewing, but up until now those exemptions have not extended to digital media. "The court is going to have to come up with a new, nuanced interpretation of the statute," says 321 attorney Daralyn Durie. "What's at stake here is the ability to engage in fair use in a digital environment." (CNet News.com 14 May 2003)

Category 4B1 *Copyrights*

2003-06-10 **copyright TV digital lawtechnology electronics**

NewsScan

LEGISLATOR URGES FAIR USE RIGHTS FOR DIGITAL TV
U.S. Rep. Lamar Smith (R-Texas), chairman of the House subcommittee overseeing copyright law, urged the Federal Communications Commission to ensure that future regulations involving digital TV do not "have an adverse effect on how consumers may legitimately use lawfully acquired entertainment products." Smith voiced his firm opposition to legislation introduced last year that would require consumer electronics makers to implant mandatory copy-protection technology in PCs and other devices. "I am skeptical of government mandates on the technology industry… Until evidence shows otherwise, I believe existing copyright law is adequate," said Smith. He also urged greater cooperation on the part of colleges and universities in disciplining perpetrators of peer-to-peer music piracy, noting that research shows 16% of files available on Kazaa are located on their networks. "It's unlikely that this amount of file-sharing activity is in furtherance of class assignments," he said. (CNet News.com 10 Jun 2003)

Category 4B1 *Copyrights*

2003-06-18 **machines copyright destroying computers music**

NewsScan

MACHINES OF COPYRIGHT VIOLATORS MAY NEED TO BE ZAPPED
Senator Orrin Hatch (R, UT) — who, besides being Chairman of the Senate Judiciary Committee, is a composer whose royalties were $18,000 last year from songs he's written — says that maybe people who keep abusing copyright laws should get their computers destroyed. That kind of action "may be the only way you can teach somebody about copyrights. If we can find some way to do this without destroying their machines, we'd be interested in hearing about that. If that's the only way, then I'm all for destroying their machines... There's no excuse for anyone violating copyright laws." (AP/San Jose Mercury News 18 Jun 2003)

Category 4B1 *Copyrights*

2003-07-09 **Google search engine caching copyright intellectual property concern**

NewsScan

GOOGLE CACHING FEATURE SPARKS COPYRIGHT CONCERNS
A caching feature on the Google search site sometimes enables users to call up snapshots of archived Web pages that for whatever reason are either restricted or no longer available at the original source, such as newspaper articles that require user registration to access or those that "expire" after a certain number of days. The feature has raised the ire of some publishers. "We are working with Google to fix that problem — we're going to close it so when you click on a link it will take you to a registration page," says a New York Times Digital spokeswoman. "We have established these archived links and want to maintain consistency across all these access points." Google says its caching feature benefits Web surfers trying to access a site that's experiencing technical difficulties, but some copyright experts say they expect the issue will end up in court: "Many of us copyright lawyers have been waiting for this issue to come up: Google is making copies of all the Web sites they index and they're not asking permission. From a strict copyright standpoint, it violates copyright," says Electronic Frontier Foundation attorney Fred Lohman. Most search engines make a statistical record of a Web page when they "spider" it, or use "robots" to scan the page's content for meaning or context, but Google goes one step beyond by snapping a digital picture of pages and making them available to users. The picture exists on Google's site until the next time it crawls that particular page, whether it's a few days or six weeks or more. Web sites can block the caching feature, but some publishers are reluctant to do so because they fear losing favor in the company's powerful search rankings, even though Google has assured them the "no cache" tags do not affect search results. (CNet News.com 9 Jul 2003)

Category 4B1 *Copyrights*

2003-07-22 **intellectual property copyright infringement theft AOL**

NewsScan

HARLAN ELLISON, CUDGEL IN HAND AGAINST COPYRIGHT THIEVES
Well-known science fiction writer Harlan Ellison is suing America Online for copyright infringement because it didn't respond quickly enough to delete from its Web site a fan's posting of some of Ellison's stories, without permission, on an AOL online forum. America Online says it removed the stories as soon as it was aware of them. Ellison has always been a fierce protector of copyright protections, and now says: "People like AOL have turned this nation and its kids into a nation of thieves, who have no more notion of what's right than the man on the moon. I really see myself as standing there on the g-d- barricade, with a cudgel in my hand.... We are up against inimical forces. We are up against city hall." Ellison's lawsuit, to be heard by the Ninth U.S. Circuit Court of Appeals, is being supported by a number of major software firms and record labels. (Wall Street Journal 22 Jul 2003)

Category 4B1 *Copyrights*

2003-07-24 **download movies legal Disney intellectual property**

NewsScan

MOVIELINK AND DISNEY SIGN MOVIE DOWNLOAD DEAL
Dozens of Disney films are going to be made available for downloading from the Internet through a licensing deal just reached between Disney and online movie service Movielink. With this new agreement in place, Movielink will have access to film titles from all the major studios except Twentieth Century Fox, and will have a library of about 400 digitized films. Movies from Walt Disney Pictures, Touchstone, Miramax and Dimension will be available through the service, and among the first releases will be "Gangs of New York," "The Recruit" and "The Jungle Book 2." Disney will set the retail price for the movie downloads (typically ranging between $2.95 and $4.99), and the downloaded movies will be viewable either on a PC or on a TV connected to a computer. (AP/USA Today 24 Jul 2003)

Category 4B1 *Copyrights*

2003-07-31 **copyright intellectual property RIAA Pacific Bell DMCA privacy constitution**

NewsScan

SBC'S PAC BELL JOINS LEGAL BATTLE AGAINST RIAA
SBC Communications' Pacific Bell Internet Services unit has filed a complaint against the Recording Industry Association of America, alleging that many of the subpoenas recently served against online music swappers were done so improperly. Pac Bell contends that more than 200 subpoenas seeking file-sharers' e-mail addresses were issued from the wrong jurisdiction, and also states that the RIAA's demand for information on multiple file-sharers cannot be grouped under one subpoena. An SBC spokesman added that the RIAA's use of a provision in the Digital Millennium Copyright Act to force ISPs to reveal information on their subscribers interferes with customer privacy: "The action taken by SBC Internet Services is intended to protect the privacy of our customers. Misapplication of DMCA subpoena power raises serious constitutional questions that need to be decided by the courts, not by private companies who operate without duty of due diligence or judicial oversight." (AP 31 Jul 2003)

Category 4B1 *Copyrights*

2003-08-28 **intellectual property copyright RIAA webcaster lawsuit**

NewsScan

WEBCASTER ALLIANCE THREATENS RIAA WITH ANTITTRUST SUIT
Angry over a new music royalty rate structure it says may force nine out ten small Internet radio stations to shut down, the 300-member Webcaster Alliance of small stations is threatening an antitrust lawsuit against the Recording Industry Association of America. The Librarian of Congress worked out a compromise fee-structure last year between the music industry and Internet radio station operators, but small stations continue to argue that they're being asked to pay too much for the right to play music. The RIAA has not yet commented officially on the newly threatened lawsuit, but a spokesman says: "We have worked diligently to negotiate fair agreements that offer a broad and flexible array of rates and terms to large, small, and non-commercial webcasters." (Washington Post 9 Jul 2003)

WEBCASTERS SUE RIAA
Webcaster Alliance, an organization of 400 music broadcasters, has filed a federal lawsuit charging that the major music labels and the Recording Industry Association of America (RIAA) are monopolists who violated federal antitrust laws when they went about setting music royalty rates for the Internet. The webcasters seek an injunction to prevent the major labels from enforcing their intellectual property rights and collecting royalty payments. The RIAA calls the suit a publicity stunt without merit." (AP/USA Today 28 Aug 2003)

Category 4B1 *Copyrights*

2003-09-03 **apple itunes consumer reselling music files cds digital copyrights pre-owned digital tune**

NewsScan

'PRE-OWNED' DIGITAL TUNE HITS AUCTION BLOCK
George Hotelling is pushing the envelope in digital music with his attempt to auction off a song that he purchased on Apple's iTunes Music Store. Hotelling says he's not concerned about recouping his 99-cent investment in Devin Vasquez's rendition of "Double-Dutch Bus," but he's interested in probing the murky legal ground surrounding digital copyrights. "I'd just like to know that if I buy something, whether it's physical or intellectual property, that I'll have my right of 'First Sale,'" says Hotelling. The terms of service contract that accompanies iTunes songs doesn't say much about the rules that guide resale of songs but does stipulate that the songs are only for "personal, noncommercial use." One nagging question concerns the lack of legal guidelines governing the rights of an owner of a second-hand digital song, says Fred von Lohmann, senior staff attorney at the Electronic Frontier Foundation. "If you were to win that auction and get that song, you have no relationship with Apple. You didn't agree to the terms of service. What governs that song after you've repurchased it?" (CNet News.com 3 Sep 2003)

Category 4B1 *Copyrights*

2003-09-08 **pop-ups ads copyright violation gator whenu.com screen savers web surfing habits**

NewsScan

JUDGE SAYS POP-UP ADS DON'T VIOLATE COPYRIGHTS
A federal judge in Virginia has ruled that pop-up ads for rival companies' products that obscure the original Web site's offerings do not violate trademark or copyright laws, potentially giving a green light to more aggressive online advertising tactics. The pop-ups — distributed mainly by Gator and WhenU.com — often divert online shoppers to competitors' offers, an action that infuriates Web site operators. According to Judge Gerald Bruce Lee's reasoning, however, consumers have accepted these ads when they agree to download Gator's and WhenU's free programs, such as screen savers or games, which piggyback on software that tracks users' Web surfing habits and then delivers ads based on their apparent interests. In the case brought by U-Haul International, Lee ruled that when WhenU's software delivers a competitor's ad to a Web surfer perusing U-Haul's Web site, it doesn't "copy or use U-Haul's trademark or copyright material" and therefore can't be accused of infringing on them. "Computer users, like this trial judge, may wonder what we have done to warrant the seizure of our computer screens by pop-up advertisements for secret Web cameras, insurance, travel values and fad diets," the judge wrote. But he argued that people "invited" those ads when they downloaded the free software, and that "(u)ltimately, it is the computer user who controls how windows are displayed on the computer desktop." The legal battle isn't over however — U-Haul lawyers are contemplating an appeal, and similar suits have been filed by several Web-site operators, including Hertz Corp. (Wall Street Journal 8 Sep 2003

Category 4B1 *Copyrights*

2003-09-10 **RIAA file sharing music 12-year-old lawsuits against song-sharing**

NewsScan

FILE-SHARING COMPANIES PAY FOR GIRL'S MUSIC SETTLEMENT
A coalition of companies that run Internet song-sharing services have offered to pay the $2,000 settlement a mother agreed to pay the Recording Industry Association of America (RIAA) after it lodged lawsuits against her 12-year-old daughter (and 260 other defendants) for music copyright infringement. Wayne Rosso, president of the Internet file-sharing service Grokster charges: "These people give Joe Stalin a good name." And the group's executive director, Adam Eisgrau, adds: "We don't condone copyright infringement, but it's time for the RIAA's winged monkeys to fly back to the castle and leave the Munchkins alone." Before it filed the lawsuits, the RIAA was dismissive of predictions that "the recording industry's aggressive legal strategy might result in a consumer backlash." (Washington Post 10 Sep 2003)

Category 4B1 *Copyrights*

2003-09-26 **California RIAA Gray Davis governor film music theft business loss money piracy**

NewsScan

NEW CALIFORNIA LEGISLATION FRIENDLY TO ENTERTAINMENT INDUSTRY
California Gov. Gray Davis says he will sign new legislation that is friendly to the entertainment industry and aimed at stopping the theft of film and music. Cary Sherman, president of the Recording Industry Association of America (RIAA), is pleased with the legislation: "The piracy problem is severe and we're seeing it in terms of layoffs. We are really grateful for anything that can be done to deal with this problem... Thousands of people in the recording industry have lost their jobs, artists are having trouble being signed ... retailers are going out of business." (AP/San Jose Mercury News 26 Sep 2003)

Category 4B1 *Copyrights*

2003-10-03 **file-sharing copyright infringement peer-to-peer fines reduced**

NewsScan

SENATOR SEEKS TO REDUCE FILE-SHARING FINES
Senator Norm Coleman (R-Minn.) says the penalties currently on the books for downloading copyrighted music are too stiff and he will sponsor legislation to reduce them. "I can tell you that $150,000 per song is not reasonable, and that's technically what you can put in front of somebody. That forces people to settle when they may want to fight, but they're thinking, 'goodness, gracious, what am I going to face?'" Coleman says he will also push for changes in the 1998 Digital Millennium Copyright Act that would restrict the recording industry's subpoena power, instituting a judicial review process which currently is unnecessary. Coleman's recommendations come as a followup to a high-profile congressional hearing on the subject that included representatives of the recording and file-sharing industries as well as rappers LL Cool J and Chuck D. (AP 3 Oct 2003)

Category 4B1 *Copyrights*

2003-10-07 **intellectual property copyrights digital DRM CD copy-protection disable Princeton**

NewsScan

DISABLING CD LOCK IS EASY AS PRESSING THE SHIFT KEY
A Princeton University student has posted instructions for disabling the copy-protection "lock" incorporated into the latest CD released by soul artist Anthony Hamilton on the BMG label. The anti-copying software, developed by SunnComm Technologies, is automatically loaded onto a Windows PC whenever the Hamilton CD is played in its CD drive, but graduate student John Halderman found that he could prevent the software from being loaded simply by holding down the shift key for awhile. The discovery was confirmed by BMG and SunnComm, but they downplayed its significance. "This is something we were aware of," said a BMG spokesman. "Copy management is intended as a speed bump, intended to thwart the casual listener from mass burning and uploading. We made a conscious decision to err on the side of playability and flexibility." SunnComm's technology is one of the most flexible on the market, and includes "pre-ripped" versions of songs on the CD, which buyers are free to transfer to a computer, burn to a CD several times, or transfer to a variety of portable devices. The Anthony Hamilton CD is the first release to come with these "second session" tracks designed for use on a computer, but holding down the shift key prevents access to that feature. (CNet News.com 7 Oct 2003)

Category 4B1 *Copyrights*

2003-10-24 **Amazon search inside book feature intellectual property book page**

NewsScan

AMAZON'S NEW 'SEARCH INSIDE THE BOOK' FEATURE
Amazon.com has announced a new feature called "Search Inside the Book" that is making the text of 120,000 books (more than 33 million pages) fully searchable at no charge. The feature makes it possible to scan a database for the word or phrase entered by a visitor to Amazon's site for each relevant portion of a searchable book. The pages that are found can be read onscreen and printed but not copied or downloaded. University of Washington computer scientist Oren Etzioni says: "It's an impressive feat — a bold concept, coupled with nice execution and clear business thinking. This really shows Amazon is a technology company, not innovating just with things like free shipping but putting something out there that's brand new."(Seattle Post-Intelligencer 24 Oct 2003)

Category 4B1 *Copyrights*

2003-10-27 **MIT LAMP analog transmission music library**

NewsScan

EXTENDING THE MUSIC LIBRARY
Two students at MIT have developed an electronic music library that allows anyone on campus to access 3,500 CDs. Called the Library Access to Music Project (LAMP), the system lets a student go to its Web site to select a CD and have it delivered through the campus closed-circuit cable TV to the student's dorm room or other campus site. One of the students who conceived of LAMP explains: "We had a library in school that closed at 7 p.m. The school had this great music in the library, but you couldn't get there. I was thinking, how could we get students better access to this library?" In 2001, the two creators of LAMP received a grant from iCampus, a Microsoft-backed alliance with MIT. (San Jose Mercury News 27 Oct 2003)

Category 4B1 *Copyrights*

2003-10-27 **MIT file-swap copyright infringement workaround analog transmission music**

NewsScan

STUDENTS CREATE A FILE-SWAP WORK-AROUND
Two students at MIT have discovered a way to give their fellow attendees free dorm-room access to a library of 3,500 CDs without breaking copyright laws. Keith Winstein and Josh Mandel developed software that routes the tunes over the school's cable TV network, making it an analog transmission. Unlike digital copies swapped over the Internet, analog transmissions are not exact copies, which makes the likelihood of prosecution much more remote since most universities already have licenses to "perform" analog music. "I think it's fascinating. As a copyright lawyer, I think they've managed to thread the needle," says Electronic Frontier Foundation legal counsel Fred Von Lohmann. "They've basically managed to cut the record labels out of the equation altogether." The students managed to circumvent the Recording Industry Association of America completely by purchasing MP3 versions of the CDs from Seattle-based Loudeye under license from the National Music Publishers Association. "The students get access to a broad array of music, and the copyright owners get paid. This is where we should all be heading. I hope the record industry takes not and realizes this is a whole lot more promising than suing people," says Von Lohmann. (AP 27 Oct 2003)

Category 4B1 *Copyrights*

2003-10-30 **copyright law Library Congress DMCA Digital Millenium Copyright Act**

NewsScan

COPYRIGHT LAW EXEMPTIONS NIXED
The Librarian of Congress has rejected requests for exemptions to a provision in the 1998 Digital Millennium Copyright Act that forbids "circumventing" the electronic locks on copyrighted works, including making backup copies and other personal uses of digital movies, games and music owned by consumers. However, exemptions were granted for software programs and video games locked to obsolete media or equipment, and cases of electronic books whose digital rights management software would prevent them from being translated into audio or other formats for the visually impaired. (Los Angeles Times 30 Oct 2003)

Category 4B1 *Copyrights*

2003-10-31 **amazon book inside search security property rights copying abuse user**

NewsScan

AMAZON TURNS OVER A NEW LEAF ON BOOK SEARCHES
Amazon says its new "Search Inside the Book" feature does not allow users to print pages from within books, allaying authors' fears that unscrupulous readers might use it to print out recipes, hotel recommendations or other such reference material. Amazon VP Steve Kessel refused to confirm that Amazon had changed the feature to prevent such abuses, citing security concerns, but acknowledged that 15 authors had requested their books to be removed from the Search the Book database. Up until Friday, according to Authors Guild executive director Paul Aiken, the Search Inside the Book tool allows users to search the complete text of a book for words or phrases and print out pages where the phrases appeared. That feature appears to be disabled, said Aiken, who praised the feature but said "we just think it needs a little work." (AP 31 Oct 2003)

Category 4B1 *Copyrights*

2003-11-04 **anti-piracy digital broadcast flag stop copying hard drive internet information**

NewsScan

DIGITAL ANTI-PIRACY MEASURE
In a 5-0 vote, the Federal Communications Commission has approved a requirement that some personal computers and other consumer electronic devices be equipped with technology to help block Internet piracy of digital entertainment. The movie industry is happy with the FCC's decision, but consumer advocates are worrying that the move will force people to buy new equipment, will result in new regulation of how computers are designed, and will hinder the copying of programming that's not entitled to industry protection (e.g., shows no longer covered by copyright). Under the new rules, a piece of digital code known as a "broadcast flag" could be embedded into a piece of program content, which then could only be copied by a digital recording device equipped with technology that recognizes the flag. A computer could not copy the file to its hard drive or send it over the Internet. (Washington Post 4 Nov 2003)

Category 4B1 *Copyrights*

2003-12-23 **unix battle linus torvalds linux code SCO Darl McBride Novell**

NewsScan

UNIX COPYRIGHT BATTLE HEATS UP
Novell has thrown a monkey wrench into SCO Group's plan to extract hundreds of millions of dollars in licensing fees and damages from IBM and other companies using the Linux operating system, which SCO says violates its copyright and license because it includes some Unix code. In the past few months, Novell has quietly registered for the copyrights on many of the Unix versions claimed by SCO, which says it acquired them through a transfer from Novell back in 1995. SCO has reacted with outrage, calling Novell's recent move a backdoor attempt to reclaim code that is rightfully SCO's. "We see this as a fraudulent attempt by Novell to get something they don't have," says SCO president and chief executive Darl C. McBride, who added that Novell's actions were probably prompted by IBM, the lead Linux seller in the corporate market. "It's not just Novell. It's an attack by IBM." Meanwhile, Novell executives maintain they have full ownership of the copyrights in question: "Novell believes it owns the copyrights in Unix, and has applied for and received copyright registrations pertaining to Unix consistent with that position. SCO has been well aware that Novell continues to assert ownership of the Unix copyrights," said the company in a statement. (New York Times 23 Dec 2003)

Category 4B1 *Copyrights*

2003-12-24 **SCO Linus Torvalds Linux intellectual property rights code unix**

NewsScan

SCO OR LINUS? WHO'S RIGHT?
The Utah-based SCO Group, which owns the rights to the Unix operating system, claims that Linux creator Linus Torvalds violated its intellectual property rights. To buttress its case, SCO provided the court a list of Linux files that "have been copied verbatim from our copyrighted Unix code and contributed to Linux." But Torvalds, who created the kernel of Linux while still a student in Finland, said in a message to a reporter that he wrote the code in those files all by himself and now feels "a bit ashamed" because some of the program macros he wrote are "so horribly ugly that I wouldn't admit to writing them if it wasn't because somebody else claimed to have done so ;). I can show, and SCO should have been able to see, that the list they show clearly shows original work, not copied." But SCO chief executive Darl C. McBride insists: "As a social revolutionary, Linus Torvalds is a genius. But at the speed the Linux project has gone forward something gets lost along the way in terms of care with intellectual property." (New York Times 24 Dec 2003)

Category 4B1 *Copyrights*

2004-01-08 **intellectual property rights violations South Korea US warn**

NewsScan

U.S. WARNS SOUTH KOREA ON INTELLECTUAL PROPERTY VIOLATIONS

The Bush Administration is warning South Korea that it's not doing enough to stop the pirating of U.S. movies and music; U.S. Trade Representative Robert B. Zoellick says: "The pirating of U.S. intellectual property robs Americans and hurts those countries whose economies rely on innovation, technology and investment. Open markets and the protection of intellectual property are critical to the continued growth of our economy, and we'll vigorously press our trading partners to follow the rules." The South Korean response to the complaint was that the U.S. action was "very disappointing and regrettable." An executive of the Recording Industry Association of America (RIAA) says: "Online piracy of recorded music is rampant in Korea and has had a devastating impact on our industry already, significantly decreasing sales for international and local repertoire alike. Incomprehensibly, Korea has thus refused to provide the legal tools necessary for the recording industry to fight back." (Washington Post 8 Jan 2004)

Category 4B1 *Copyrights*

2004-02-26 **EFF digital music intellectual property rights copyright RIAA download free music**

NewsScan

FREE THE MUSIC

The Electronic Frontier Foundation is proposing legalization of online file-sharing through a voluntary music license that would compensate artists. EFF lawyer Fred von Lohmann says: "Everyone agrees that file-sharing does a better job distributing music than anything else out there. It gives people a much broader selection of software to choose from. And, of course, it's better-priced. The problem is that artists and copyright holders aren't being compensated." But music industry people say the EFF plan has little chance of success without the support of the major music labels, and Mitch Glazier of the Recording Industry Association of America (RIAA) says: "We've got a new, dynamic marketplace with Napster announcing its 5 millionth download. ITunes is just starting to get corporate partners. That's not failure at all. That's experimentation. Why the government should come in and take over a marketplace that's starting to develop is conceptually flawed in my mind." Wayne Rosso of the company that created Blubster and Piolet file-swapping services says: "I think it's one of several solutions that all reasonable men could probably understand and accept. The only problem is we're not dealing with reasonable men." (San Jose Mercury News 26 Feb 2004)

Category 4B1 *Copyrights*

2004-03-01 **copyright intellectual property rights issues digital report laws innovation**

NewsScan

MEMO TO COPYRIGHT ENFORCERS: SLOW DOWN, TAKE A BREATH

A report from the policy group called Committee for Economic Development warns against efforts to support copyrights by preventing digital TV from being transmitted online. Called "Promoting Innovation and Economic Growth: The Special Problems of Digital Intellectual Property," the report concludes: "We are sympathetic to the problems confronting the content distribution industry. But these problems — perfect copies of high-value digital works being transmitted instantly around the world at almost no cost — require clear, concentrated thinking, rather than quick legislative or regulatory action." Not everyone is likely to agree with that recommendation. Jack Valenti, the president of the Motion Picture Association of America, has been highly critical of the notion that his industry is trying to place unfair burdens on consumers. "They say it will stifle innovation — that's malarkey. If all of this digital property is free, who is going to invest 50 to 60 million dollars to make a movie?" The report from the Committee for Economic Development has called for a two-year moratorium on changes to copyright laws and regulations: "Our first concern should be to 'do no harm.'" (New York Times 1 Mar 2004)

Category 4B1 *Copyrights*

2004-05-03 **microsoft DRM digital rights management software songs movies portable players expire**

NewsScan

MICROSOFT'S NEW COPYRIGHT-PROTECTION SOFTWARE

Microsoft is introducing DRM "digital rights management" software software to allow rented songs or movies to be used on portable players, cellular phones and other devices. Songs and videos purchased through subscription services will be given digital expiration dates. The Walt Disney Co. and other companies are interested in using the new technology for their content. (Los Angeles Times 3 May 2004)

Category 4B1 *Copyrights*

2004-05-12 **copyright act congress Digital Millennium Act DVD CD locks**

NewsScan

CONGRESS REVISITS 'FAIR USE' RESTRICTIONS IN COPYRIGHT ACT

A House subcommittee on consumer protection heard arguments yesterday on proposed amendments to the 1998 Digital Millennium Copyright Act, which imposed broad restrictions on bypassing technological "locks" on DVDs and some music CDs and software programs. The amendments, sponsored by Rick Boucher (D-Va.) and John Doolittle (R-Calif.), would reinstate the provision for "fair use" of such materials, even if circumvention of copy-protection software were necessary for such use. The sale of pirated DVDs and other forms of copyright infringement would remain illegal. "Without a change in the existing law, individuals will be less willing to purchase digital media if their use of the media within the home is severely circumscribed," says Boucher. "In addition, manufacturers of equipment and software which enable circumvention for legitimate purposes will be reluctant to introduce the products into the market." It's unclear whether the Boucher-Doolittle bill has much momentum behind it — so far, it has only 15 co-sponsors in the House, and there is no companion Senate bill as yet. (CNet News.com 12 May 2004)

Category 4B1 *Copyrights*

2004-06-23 **copyright infringement intellectual property rights illegal file-swapping Senate broad law proposal**

NewsScan

FRIST AND DASCHLE UNITE AGAINST ILLEGAL FILE-SWAPPING

Senate majority leader Bill Frist and minority leader Tom Daschle have joined up in attack against online music and video file-sharing services and have co-introduced legislation to make anyone who "induces" illegal copying just as liable for breaking copyright law as the person who makes the copies. Wayne State University law professor Jessica D. Litman says she finds the bill "sort of scary" because it's "worded so broadly" and could be used against devices and technologies that have non-infringing as well as infringing uses, and Gary Shapiro of the Consumer Electronics Association says: "The VCR would not be a legal product; TiVo would not be a legal
product. I'm surprised the leadership would jump on this bill without hearing from the other side." But Emery Simon of the Business Software Alliance argues that such legislation is needed: "We have a huge piracy problem. Current law makes it difficult" to go after all the infractions." (Washington Post 23 Jun 2004)

Category 4B1 *Copyrights*

2004-07-01 **internet service provider ISP Canada Supreme Court lawsuit litigation copyright law infringement intellectual property rights jurisdiction**

NewsScan

ISPs WIN MUSIC DOWNLOAD CASE

Canada's Supreme Court has ruled 9-0 that Internet service providers do not have to pay royalties to composers and artists for music downloaded by Web customers, since companies providing wide access to the Web are merely "intermediaries" who aren't bound by Canadian copyright legislation. At issue was an effort by the Society of Composers, Authors and Music Publishers of Canada (SOCAN) to force Internet service providers to pay a tariff. SOCAN also wanted to extend Canadian copyright law beyond the country's borders and apply it to offshore Web sites that serve Canadians.
Opposing the effort was the Canadian Association of Internet Service Providers. (The Australian 1 Jul 2004) Rec'd from John Lamp, Deakin U.

Category 4B1 *Copyrights*

2004-08-05 **source code stolen Jolly Inc. Mumbai intellectual property rights outsourcing concern**

DHS IAIP Daily;
http://www.computerworld.com/governmenttopics/government/legalissues/story/0,10801,95045,00.html

August 05, IDG News Service — Source code stolen from U.S. software company in India.

Jolly Technologies, a division of U.S. company Jolly Inc., reported Wednesday, August 4, that an insider at its research and development center in Mumbai, India, stole portions of the source code and confidential design documents relating to one of its key products. As a result, the company has halted all development at the center. A recently hired software engineer used her Yahoo e-mail account to upload and ship the copied files out of the research facility. Most U.S.-based software companies require their employees to sign an employment agreement that prohibits them from carrying the company's source code out of a development facility or transferring it in any way. Though the Indian branch of Jolly Technologies requires employees to sign a similar employment agreement, the sluggish Indian legal system and the absence of intellectual property laws make it nearly impossible to enforce such agreements, the company said.

Category 4B1 *Copyrights*

2004-08-12 **Nowergian hacker Jon Lech Johansen DVD-Jon iTunes encryption crack posting Website copyright infringement proprietary software**

NewsScan

HACKER WANTS TO MAKE iTUNES EVERYBODY'S TUNES

Jon Lech Johansen, the Norwegian hacker who gained notoriety for developing DVD encryption-cracking software, has created a software key that unlocks the encryption Apple uses for its AirPort Express -- which lets users broadcast digital music from Apple's online iTunes Music Store on a
stereo not plugged into a computer. Johansen, who posted the key on his Web site (mockingly named "So Sue Me"), is an open source advocate critical of Apple for using a proprietary system to ensure that its products work only with each other. Apple has not yet reacted to this new intrusion. (AP/San Jose Mercury News 12 Aug 2004)

Category 4B1 *Copyrights*

2004-08-25 **copyright bill changes proposed legislation intellectual property rights file-sharing pressure**

NewsScan

CHANGES TO NEW COPYRIGHT BILL URGED

The Consumer Electronics Association and the American Library Association, along with other technology and consumer groups, have recommended changes to the controversial Inducing Infringement of Copyrights Act (SB 2560), which is intended to discourage illegal file-sharing. The bill, sponsored by Sens. Orrin Hatch (R-Utah) and Patrick Leahy (D-Vt.), is supported by the record labels and Hollywood studios, who complain that illegal file-sharing is ruining their livelihood. But
consumer groups recommend amending the legislation so "only someone who distributes a commercial computer program that is 'specifically designed' for wide-scale piracy on digital networks would be held liable for copyright violations," according to a press release. The proposed change would absolve ISPs, venture capitalists, credit card companies, banks, advertising agencies, IT help desks and librarians from liability. Emily Sheketoff, executive director of the American Library Association's Washington office, says she worries that SB 2560 "will quash innovation and
creativity and the fair use of these technologies. The answer to protecting copyright is not to stop developing new technologies. The answer is to educate people on how to use these technologies properly and encourage people to use these technologies properly. There are many legal, legitimate
file-sharing activities." (Wired.com 25 Aug 2004)

Category 4B1 *Copyrights*

2004-10-12 **P2P peer-to-peer supreme court**

NewsScan; http://www.nytimes.com/2004/10/12/technology/12share.html

HOLLYWOOD PETITIONS SUPREME COURT ON FILE-SHARING

The entertainment industry is fighting back against peer-to-peer (P2P) file-sharing, petitioning the U.S. Supreme Court to overturn a federal appeals court decision reached in August that upheld file-sharing companies' right to distribute their software regardless of whether that software is later used to violate copyrights. That decision drew heavily on the precedent established by the 1984 Sony-Betamax case, which gave electronic device makers legal protection against claims of copyright infringement. This latest petition, which targets P2P purveyors Grokster and Streamcast Networks, cites a conflicting ruling reached in 2003, which upheld an injunction against P2P service Aimster on the grounds that it facilitated copyright infringement. However, critics say even the Aimster case upheld the basic tenets of the Sony-Betamax case. "They want to argue that there's some sort of national emergency here. But Betamax is the law of the land and it's not undermined by either of these two decisions," says Susan Crawford, a professor of Internet law at Cardozo School of Law in New York.

Category 4B1 *Copyrights*

2004-10-20 **music industry business model copyright Waldfogel strategy**

NewsScan;
http://knowledge.wharton.upenn.edu/index.cfm?fa=viewArticle&id=1066

MUSIC INDUSTRY ON THE WRONG COURSE

Wharton business professor Joel Waldfogel says the music industry is mistakenly pursuing a short-term strategy in backing the Inducing Infringement of Copyrights Act of 2004, which would hold liable any entity that "intentionally aids, abets, induces or procures" copyrighted material. Rather than fighting technological advances through litigation, the music industry must come up with new business models -- for instance, taking advantage of the Internet to slash its distribution costs. "Instead of putting out CDs and shipping them on trucks, they can send them directly at a very low cost. That does suggest a very different business model than charging $15 or $20 for a CD. It might be a much more attractive way to do things. Stuff that is easy to distribute wants to be free. Given that force, I think [the recording industry] needs to come up with a new model for generating income," says Waldfogel. (Knowledge@Wharton Oct 20-Nov 2 2004)

Category 4B1 *Copyrights*

2004-10-31 **venture capital Internet music**

NewsScan;
http://news.com.com/iTunes+aside%2C+Web+is+changing+the+music+industry
/2100-1027_3-5433891.html

INTERNET MUSIC REWRITES INDUSTRY RULES

While the music industry has been focusing on music piracy, another phenomenon is slowly emerging -- the Web as venture capital source. Chart-topping rockers The Darkness have sold enough downloads, T-shirts and other fan-abilia to finance their next album, and British band Marillion has used its site to raise funds for its last two albums -- before they recorded them. "The Internet is our savior. Without it, we wouldn't be what we are today. It's really turned the business around," says Marillion's marketing manager. Meanwhile, Universal Music has begun using the Web as a testing/breeding ground for new acts, signing them to a "digital rights" contract before committing serious money to their promotion. "It acts as an incubation label, if you will," says Universal Music UK new media services director Rob Wells. "It's the Marillion concept." (Reuters/CNet 31 Oct 2004)

Category 4B1 *Copyrights*

2004-11-15 **music Napster Snocap Universal P2P peer-to-peer**

NewsScan; http://online.wsj.com/article/0

UNIVERSAL AND SNOCAP MAKE MUSIC TOGETHER

Vivendi Universal has agreed to license its catalog of 150,000 songs to Snocap, a new venture headed up by Napster founder Shawn Fanning. It's unclear how Snocap's peer-to-peer service will work, but people close to the deal say one possibility is that the service would allow users to share a low-quality copy of a licensed song for free but would require a fee for access to a high-quality version. The other three big labels -- Warner Music, EMI Group and Sony BMG -- all are seeking ways to license legitimate copies of their songs to peer-to-peer network, but Universal's move marks the first such partnering deal. (Wall Street Journal 15 Nov 2004)

Category 4B1 *Copyrights*

2004-12-16 **copyright music Hatch MPAA Specter politics**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A4003-2004Dec16.html

WHAT PROSPECT FOR CHANGE IN COPYRIGHT POLICY?

On the issue of protecting music and movies from Internet piracy, Senator Orrin Hatch (R, UT), a songwriter himself, has been the entertainment industry's most powerful ally in Congress, but in 2005 Sen. Arlen Specter (R, PA) will replace Hatch as chairman of the Senate Judiciary Committee. Will there be much change? One aide says that Specter "has been a follower rather than a leader on these issues" and therefore might let Hatch keep holding the reins. However, David Green of the Motion Picture Association of America (MPAA) predicts that Specter will rise to the occasion: "Copyright issues are important and they're going to percolate up, and it's really impossible for him to ignore them. He might be right now more interested in something else, but because these issues are important to America they are going to be important to Arlen Specter." (Washington Post 16 Dec 2004)

Category 4B1 *Copyrights*

2005-01-04 **appeals court RIAA Digital Millennium Copyright Act Internet identities subpoenaing**

EDUPAGE; http://www.siliconvalley.com/mld/siliconvalley/10565129.htm

APPEALS COURT TURNS DOWN RIAA AGAIN

The Recording Industry Association of America (RIAA) this week lost the same court battle for a second time, in a different court. Echoing a December 2003 decision by the U.S. court of appeals in Washington, the appeals court in St. Louis rejected the trade group's argument that the Digital Millennium Copyright Act compels Internet service providers to reveal the identities of their customers who are accused of trading copyrighted songs. The court said in its 2-1 decision that in order to obtain users' identities, the RIAA must file "John Doe" lawsuits against those individuals. Filing such lawsuits, which the RIAA has been doing since the Washington ruling, is more costly and time-consuming than its earlier practice of simply subpoenaing identities of suspected illegal file traders. Despite losing its argument a second time, the RIAA said it will continue to seek prosecution of copyright infringement and that its "enforcement efforts won't miss a beat." Circuit Judge Diana E. Murphy, who wrote the dissenting opinion in the St. Louis court, called the process of filing individual lawsuits "cumbersome and expensive" and said the courts' rulings impose unnecessary hurdles to the protection of copyrighted material.

Category 4B1 *Copyrights*

2005-01-05 **DMCA Digital Millennium Copyright Act BSA Business Software Alliance ISP Internet service provider law legislation proposal change immunity piracy**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A51966-2005Jan5.html

SOFTWARE GROUP WANTS TO CHANGE COPYRIGHT ACT

The Business Software Alliance, whose members include Microsoft, IBM, Intel, Adobe, and other high-tech giants, wants Congress to clamp down on Internet service providers who allow their users who swap copyrighted software, music or video files online through services such as Kazaa, Grokster and Morpheus. The group wants Congress to amend the 1998 Digital Millennium Copyright Act but has so far offered no specifics on how that law should be changed -- except to suggest that Internet service providers should no longer enjoy blanket immunity from liability for piracy by users. However, the BSA approach has a number of critics, such as Mike Godwin of the group Public Knowledge, who calls the approach a "terribly bad idea," and Verizon attorney Sarah B. Deutsch, who warns: "The best policy is not to have the service provider become Big Brother. BSA wants its own shortcut, at the expense of consumer privacy and the ISPs." (Washington Post 5 Jan 2005)

Category 4B1 *Copyrights*

2005-01-07 **BSA copyright legislation white paper government laws digital piracy Microsoft Intuit Symantec patents**

EDUPAGE; http://news.com.com//2100-1030_3-5516568.html

BSA CALLS FOR STRONGER COPYRIGHT LEGISLATION

The Business Software Alliance (BSA) has released a white paper calling on government to strengthen laws meant to protect copyright holders from digital piracy. Fearing a situation like the one that record companies are grappling with, the BSA--which includes such companies as Microsoft, Intuit, and Symantec--urged lawmakers to take appropriate steps to ensure the enforceability of software copyrights and patents. An attorney for the group, Emery Simon, said the goal of the paper was not to encourage specific action but simply to identify a "problem that needs attention." The paper contends that a series of court rulings regarding the Digital Millennium Copyright Act have resulted in an "impediment to effective enforcement," but the group did not specifically call on lawmakers to revise that law.

Category 4B1 *Copyrights*

2005-01-11 **trial questions exposing software flaws copyright antivirus Viguard prison fine**

EDUPAGE; http://news.com.com/2100-7348_3-5531586.html

TRIAL RAISES QUESTIONS ABOUT EXPOSING SOFTWARE FLAWS

French researcher Guillaume Tena is currently on trial in a Paris court for violating copyright laws when he exposed software flaws in an antivirus application called Viguard, developed by Tegam International, a French company. Tena, who is a researcher at Harvard University, faces a prison term and fine, and Tegam has also filed a civil suit against Tena for about $1.2 million. Although K-OTik, a French computer security organization, conceded that Tena did technically break French copyright law, the group said that a decision against him could set a dangerous precedent for prosecuting individuals for exposing software vulnerabilities. Officials from K-OTik said a ruling against Tena would be "unimaginable and unacceptable in any other field of scientific research." The court's final ruling is expected March 8. CNET, 11 January 2005

Category 4B1 *Copyrights*

2005-01-14 **Apple Mac Mini Mac iPod Thinksecret.com suit**

NewsScan; http://online.wsj.com/article/0

APPLE SUES STUDENT FOR DIVULGING SECRETS

Nicholas Ciarelli launched what has become one of the most influential Apple-focused Web sites when he was 13 as a hangout for fellow Mac enthusiasts, but his penchant for posting trade secrets has gotten the now-19-year-old Harvard student, who publishes online under the name Nick dePlume, in hot water. Apple filed a lawsuit Jan. 4 against ThinkSecret.com and its unnamed tipsters, charging: "Apple is informed and believes that Defendant Nick dePlume is an individual who uses the pseudonym 'Nick dePlume' but whose true name and identity cannot be confirmed at this time." Apple, known for its highly secretive culture, says it believes ThinkSecret obtains its information by illegally soliciting information about unreleased Apple products from individuals who violate their confidentiality agreements. In fact, on Dec. 28 the site correctly predicted Apple's debut of its $499 Mac Mini and a low-cost iPod. In response to Apple's accusations, Ciarelli replies, "I didn't do anything wrong. My reporting practices are the same that any journalists use. I talk to sources, I confirm details, I follow up on tips and leads that I get." It will be difficult for Apple to prove that Ciarelli's coverage has violated its trade secrets, says an intellectual property attorney, noting that trade secrets usually refer to the formula behind products, not simply the details about their release. (Wall Street Journal 14 Jan 2005)

Category 4B1 *Copyrights*

2005-01-14 **scholarly republishing Cornell University articles journals Emarald**

EDUPAGE; http://chronicle.com/prm/weekly/v51/i19/19a03102.htm

NEW QUESTIONS ARISE OVER SCHOLARLY REPUBLISHING

A librarian at Cornell University has uncovered evidence that academic publisher Emerald has for many years republished articles in its journals without acknowledging previous publication. Philip M. Davis first noticed republished articles dating back to 1989 in online archives maintained by Emerald. Davis then broadened his search to include paper copies of Emerald journals going back to 1979 and said he found many more examples of such republished articles. Davis said some articles were published more than once in the same journal, several years apart, and noted that as a result libraries may have spent money on material they already owned. A spokesperson from Emerald said the company does not have a practice of republishing, though in some cases Emerald officials who thought a particular article especially valuable would republish it "to make it available to another audience." Davis said, "It's clearly unethical to republish materials without attribution."

Category 4B1 *Copyrights*

2005-01-19 **file sharing conviction copyright infringement federal court entertainment civil trading restitution equipment**

EDUPAGE; http://online.wsj.com/article/0,,SB110610434199329863,00.html

TWO CONVICTED FOR FILE SHARING

Two men have pleaded guilty to criminal copyright infringement charges in federal court. Although entertainment companies have won a number of civil judgments against individuals for file trading, the cases against William Trowbridge and Michael Chicoine mark the first convictions for such activity under federal criminal charges. The two face prison terms of up to five years and fines of as much as $250,000, as well as restitution and forfeiture of computer equipment used in the crimes. Trowbridge and Chicoine admitted to operating Internet hubs from which others could download software, movies, and other copyrighted material. The two men were part of a group called the Underground Network, an organization of 7,000 users who made computer files available to one another. Investigators reportedly downloaded files from Chicoine valued at $4,820.66 and files from Trowbridge worth $20,648.63.

Category 4B1 *Copyrights*

2005-01-25 **broad coalition file trading case organizations entertainment industry Supreme Court illegal file trading networks Grokster Morpheus piracy Justice Department Copyright Office Patent Trademark Office**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=7428570

BROAD COALITION FILES BRIEFS IN FILE-TRADING CASE

A broad group of organizations has filed legal briefs siding with the entertainment industry in its upcoming Supreme Court case over whether P2P services should be held liable for illegal file trading on their networks. Groups including the National Football League and the Christian Coalition of America joined with the U.S. government and 40 states and territories in calling for the court to overturn lower court rulings and find companies such as Grokster and Morpheus liable for P2P music piracy. A brief submitted by the Justice Department, the Copyright Office, and the Patent and Trademark Office said P2P companies have built their businesses on "massive copyright infringement." Adam Eisgrau, executive director of the P2P United trade group, said that a ruling against P2P companies would suppress technological innovation and would punish a technology that simply is not mature. According to Eisgrau, "If the standard for a technology in its relative infancy is whether at that instant it is used more for ill than for good, then we will almost never foster the development of breakthrough technologies." The case will be presented to the Supreme Court in March; a decision is expected in June.

Category 4B1 *Copyrights*

2005-01-26 **MPAA lawsuits illegally copyrighted movie hubs BitTorrent eDonkey DirectConnect networks Parent File Scan**

EDUPAGE; http://news.com.com/2100-1030_3-5551903.html

ROUND TWO OF MPAA SUITS

The Motion Picture Association of America (MPAA) has filed a second round of lawsuits against an undisclosed number of U.S. users suspected of illegally trading copyrighted movie files. The group first filed lawsuits against individuals in November, followed by legal action against Web sites that function as file-trading hubs, including BitTorrent, eDonkey, and DirectConnect networks. MPAA Chief Executive Officer Dan Glickman said, "We cannot allow people to steal our motion pictures and other products online, and we will use all the options we have available to encourage people to obey the law." The MPAA also released a software tool called Parent File Scan that identifies file-sharing software on a computer, as well as movie and music files that might be protected by copyright. The software does not differentiate between legal and illegal files, and it does not monitor or block any downloads. Rather, it identifies files of a wide range of formats and leaves decisions about which are legitimate up to users, most of whom presumably will be parents.

Category 4B1 *Copyrights*

2005-01-28 **court reimburse music industry copyright violations Napster MP3 Web**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4216551.stm

COURT ORDERS MAN TO REIMBURSE MUSIC INDUSTRY

The Supreme Court of Norway has ordered Frank Allan Bruvik to pay 100,000 kroner (about $16,000 U.S.) to the country's music industry for copyright violations stemming from a Web site he operated. The Web site that Bruvik set up when he was a student, napster.no, was not associated with Napster but offered links for users to locate MP3 files on the Web. Bruvik's site was only online for about four months in 2001, and it did not host any music files. Nevertheless, a court ruled in 2003 that Bruvik was liable for copyright violations that his site facilitated. An appeals court overturned that ruling, but the Supreme Court has decided against Bruvik. In its ruling, the court said that Bruvik's actions did violate copyright law in that he abetted an illegal act and that his actions were premeditated. The music industry in Norway said it was pleased with the ruling, saying it demonstrates the court will not tolerate copyright violations.

Category 4B1 *Copyrights*

2005-02-07 **Google copyright volumes libraries scan academic publishers permission**

EDUPAGE; http://chronicle.com/prm/daily/2005/02/2005020703n.htm

DOES GOOGLE FACE COPYRIGHT TROUBLES?

Google's recently announced plans to scan millions of volumes in several libraries has some wondering if the project is at risk of running into copyright limitations. Google will scan books that are in the public domain and make those texts available online; the company will also scan copyrighted books and offer short excerpts of a few lines each. Some publishing groups argued that putting even small pieces online will violate copyright and that the company should seek explicit permission from copyright owners. Critics also expressed reservations about copyright determinations for books that might, for example, be in the public domain in one country but not in another. Sally C.L. Morris, chief executive of the Association of Learned and Professional Society Publishers, said that although the sheer number of academic publishers represents a powerful disincentive to obtaining permissions from all of them, "that doesn't mean there's not a legal requirement to do it." For its part, Google insists that its actions are acceptable. Google spokesperson Steve Langdon said, "In every case, Google's presentation of the works to the public will keep authors and publishers in mind and be well within the bounds of copyright law."

Category 4B1 *Copyrights*

2005-03-11 **file sharing illegal downloading UK British ISP BPI identity disclosure intellectual property rights violation copyright infringement**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=7877847

BRITISH ISPS TOLD TO TURN OVER FILE TRADERS

A British court has ruled that ISPs in that country must disclose the identities of alleged copyright violators to the British Phonographic Industry (BPI). The BPI had sought the names of about 30 individuals suspected of uploading significant numbers of songs to file-sharing networks. The court has given the six ISPs named in the suit 14 days to turn over the requested identities, which are known currently only by their IP addresses. The BPI will then contact those individuals and offer to settle the charges against them outside court. The British music industry has recently reached its first round of settlements with alleged copyright infringers, a process that Geoff Taylor, general counsel of the BPI, said showed the organization that "people from all walks of life are engaged in this activity." Reuters, 11 March 2005

Category 4B1 *Copyrights*

2005-03-11 **Sweden file sharing illegal downloading ISP raid intellectual property rights violation copyright infringement MPAA**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=7882727

SWEDEN RAIDS ISP FOR FILE TRADING

Police in Sweden raided the Stockholm offices of Bahnhof, the country's largest and oldest Internet service provider (ISP), long suspected of facilitating rampant copyright violations. According to John Malcolm of the Motion Picture Association of America (MPAA), which had urged Swedish authorities to carry out such a raid, Bahnhof operated some of the largest and fastest servers in Europe. Of the four servers seized in the raid, one is thought to be the largest pirate server in Europe, according to the MPAA. Malcolm said the raid uncovered evidence not only of organized piracy in Sweden but also of such activity throughout Europe. Equipment seized in the raid reportedly contained 1,800 digital movies, 5,000 software files, and 450,000 audio files. Reuters, 11 March 2005

Category 4B1 *Copyrights*

2005-03-12 **intellectual property confidentiality instant messaging internet service provider ISP value added network VAN AOL AIM**

RISKS; http://www.aim.com/tos/tos.adp 23 79

AOL CLAIMS INTELLECTUAL PROPERTY RIGHTS TO AIM CONTENT

Alistair McDonalt wrote:

>AOL has changed their Terms of Service for users of their services….

Users of their services, for example AOL Instant Messenger (AIM) in particular should note the details, including: "by posting Content on an AIM Product, you grant AOL, its parent, affiliates, subsidiaries, assigns, agents and licensees the irrevocable, perpetual, worldwide right to reproduce, display, perform, distribute, adapt and promote this Content in any medium".<

Category 4B1 *Copyrights*

2005-03-14 **Holland Netherlands file sharing illegal downloading warning intellectual property rights violation copyright infringement**

EDUPAGE; http://www.usatoday.com/tech/world/2005-03-14-dutch-download_x.htm

DUTCH ISPS ISSUE WARNINGS TO FILE TRADERS

Five Internet service providers (ISPs) in the Netherlands have agreed to send notices from the Brain Institute, the antipiracy arm of the country's entertainment industries, to subscribers suspected of illegally trading copyrighted music, movies, and software. The ISPs did not go so far, however, as agreeing to disclose the identities of those users to entertainment companies. Maaike Scholten, spokesperson for two of the five ISPs, described the move as "a service, a warning to clients that they are doing things that are against the law." In 2003, the Dutch Supreme Court ruled that file-sharing applications are legal, leaving copyright owners the option of pursuing individuals who use such applications for copyright violations, as in the United States. Tim Kuik, director of the Brain Institute, said his organization hopes to reach settlements with illegal file traders but anticipates it will be forced to file civil lawsuits against some. Associated Press, 14 March 2005

Category 4B1 *Copyrights*

2005-03-16 **Microsoft lawsuit Windows XP Office academic discount eBay sale David Zamos intellectual property rights violation**

EDUPAGE; http://chronicle.com/prm/daily/2005/03/2005031606n.htm

MICROSOFT AND STUDENT SETTLE OVER SOFTWARE RESALE

Microsoft and David Zamos have reached a settlement in their dispute over Zamos's sale on eBay of Microsoft software he purchased while a student at the University of Akron. After Zamos bought Windows XP Pro and Microsoft Office from the university bookstore, he found he was not permitted to return it, though it was unopened. Zamos, who paid about $50 for both products because of deep educational discounts, decided to sell the software on eBay, where he sold each for about $100. The sale prompted Microsoft to file a lawsuit alleging that Zamos improperly benefited from academic pricing, in violation of company policies. Zamos argued that such policies were not explained on the packaging, and he countersued the company, alleging that because of Microsoft's actions and policies, obtaining a refund for software is virtually impossible. Although both parties expressed their satisfaction with the resolution, a confidentiality agreement covering the settlement prevents disclosure of any details. A statement from Microsoft did note, however, that the company will "continue its commitment to protecting those intended to benefit from its academic program,"
suggesting it will continue to look unfavorably on anyone reselling academic purchases. Chronicle of Higher Education, 16 March 2005 (sub. req'd)

Category 4B1 *Copyrights*

2005-03-18 **Agence France Presse AFP lawsuit Google intellectual property rights violation copyright infringement without permission**

EDUPAGE; http://news.com.com/2100-1030_3-5626341.html

AGENCE FRANCE PRESSE TAKES GOOGLE TO COURT

Agence France Presse (AFP) has filed a lawsuit against Google in the U.S. District Court for the District of Columbia, alleging that the search engine gives access to AFP headlines, stories, and photographs without proper permission. AFP does not make its content available free online, instead charging users subscription fees to access it. Officials from AFP said they have notified Google about the alleged copyright violations but that Google "continues in an unabated manner to violate AFP's copyrights." AFP is seeking damages of at least $17.5 million as well as an injunction forbidding Google from displaying further AFP content. CNET, 18 March 2005

Category 4B1 *Copyrights*

2005-03-18 **John Wiley and Sons publisher lawsuit selling guidebooks online intellectual property rights violation copyright infringement cheating**

EDUPAGE; http://www.insidehighered.com/news/2005/03/18/cheating

STUDENTS SUED FOR SELLING GUIDEBOOKS ONLINE

Publisher John Wiley and Sons has filed lawsuits against a number of individuals for selling guidebooks online that include answers to tests and assignments in certain of the company's textbooks. The publisher also said it has reached settlements with about 150 individuals, most of them students, after investigating sales of the guidebooks--which the company does not sell but provides only to professors--on eBay. No faculty have been implicated so far. Those named in the suits did not respond to the publisher when it contacted them about the illicit sales. According to Roy S. Kaufman, legal director of Wiley, illegal copies of the text are still widely available online, despite the company's efforts. "This is a new form of cheating and copyright violation," said Kaufman, "with a Malthusian growth cycle." Inside Higher Ed, 18 March 2005

Category 4B1 *Copyrights*

2005-03-24 **intellectual property rights violation copyright infringement Apple Tiger source code leak lawsuit settlement**

EDUPAGE; http://news.com.com/2100-1047_3-5632119.html

APPLE SETTLES WITH MAN ACCUSED OF LEAKING CODE

Apple Computer has settled a lawsuit against Doug Steigerwald of North Carolina for leaking the company's upcoming Macintosh operating system, called Tiger. As part of the Apple Developer Connection (ADC) program, Steigerwald, a recent graduate of North Carolina State University, had prerelease access to the operating system. The ADC program allows software developers to create products that will operate with a new operating system before it is released to the public, and participants in the program are required to sign a contract that prohibits disclosure of information about Apple products before they are launched. In a statement, Steigerwald admitted distributing prerelease copies of Tiger over the Internet in violation of the ADC contract he signed. Specifics of the settlement were not released, but a statement from Apple said, "While Apple will always protect its innovations, it is not our desire to send students to jail." The statement also expressed the company's satisfaction that Steigerwald took responsibility for his actions. CNET, 24 March 2005

Category 4B1 *Copyrights*

2005-03-29 **media companies class-action lawsuit freelance writers electronic database inclusion fees**

EDUPAGE; http://www.wired.com/news/politics/0,1283,67063,00.html

MEDIA COMPANIES SETTLE WITH FREELANCERS

A settlement has been reached in a class action lawsuit between media companies and freelance writers over stories included in electronic databases. The class action suit was the combination of three separate suits and represented defendants including the American Society of Journalists and Authors, the Authors Guild, the National Writers Union, and almost two dozen freelance writers. Defendants in the suit, including Time, Knight Ridder, Reed Elsevier, and The New York Times Company, agreed to pay between $10 million and $18 million for works originally published between August 1977 and December 2002. Under the terms of the settlement, writers who did not sign away electronic publishing rights can apply for payments of as much as $1,500 for works that have been added to electronic databases. Although many payments will be significantly smaller than that, "some freelancers … will make six figures under this settlement," according to Jim Morrison, one of the negotiators of the settlement and a past president of the American Society of Journalists and Authors. Wired Magazine, 29 March 2005

Category 4B1 *Copyrights*

2005-04-07 **University of California electronic reserves Fair Use exceeded publishers complaint intellectual property rights violation copyright infringement**

EDUPAGE; http://chronicle.com/prm/daily/2005/04/2005040701t.htm

UC ELECTRONIC RESERVES RANKLE PUBLISHERS

A system that handles electronic reserves at the University of California (UC) in San Diego has prompted complaints from publishers that the university has far exceeded the bounds of fair use. With the system, materials that faculty put on reserve are made available electronically, allowing students to access and even print them from outside the university library. The Association of American Publishers objected, saying that electronic access substantially changes the traditional terms of reserve materials and deprives publishers of sales. Publishers have previously won legal challenges to the production of coursepacks, which the courts said do not fall under the terms of fair use. The publishing group insisted the same applies to electronic resources. Representatives of UC disputed the claims, saying the reserve system does not infringe on sales of texts. Jonathan Franklin, associate law librarian at the University of Washington, noted that the fair use law is not clear and commented that if the disagreement is ultimately settled by the courts, such a resolution might provide needed clarification for all concerned. Chronicle of Higher Education, 7 April 2005 (sub. req'd)

Category 4B1 *Copyrights*

2005-04-12 **music piracy peer-to-peer P2P file sharing illegal downloading intellectual property rights violation copyright infringement RIAA IFPI increased lawsuits**

EDUPAGE; http://news.bbc.co.uk/2/hi/entertainment/4436223.stm

MUSIC INDUSTRY STEPS UP LAWSUITS

Efforts to stem illegal file trading were ratcheted up this week with announcements about new rounds of lawsuits against individuals accused of piracy. The International Federation of the Phonographic Industry said it plans to file 963 lawsuits in 11 countries in Europe and Asia, representing the largest single action against file traders. Meanwhile, the British Phonographic Industry (BPI) said it will file actions against 33 users in the United Kingdom. Previously, the BPI has filed suits against 57 individuals, some of whom have reached settlements with the organization. Geoff Taylor, general counsel of the BPI, said his group has warned users repeatedly that illegal file trading will not be tolerated and that those found guilty will have to pay. BBC, 12 April 2005

Category 4B1 *Copyrights*

2005-04-13 **music movie piracy Internet2 i2hub peer-to-peer P2P file sharing illegal downloading intellectual property rights violation copyright infringement RIAA lawsuit threat**

EDUPAGE; http://chronicle.com/prm/daily/2005/04/2005041302t.htm

ENTERTAINMENT INDUSTRY TARGETS INTERNET2 USERS

Organizations representing record companies and movie studios announced this week they will begin filing copyright infringement lawsuits targeting users of i2hub, a file-sharing system that lets users exchange data over Abilene, Internet2's high-speed research network. Because of the network's speed--and a belief among some users that their actions on i2hub could not be detected by the entertainment industry--students on a number of Internet2 campuses have engaged in widespread illegal file trading, according to Cary Sherman, president of the Recording Industry Association of America (RIAA). The RIAA said it will file suits against 405 of what it described as the most egregious violators at 18 campuses. The trade group also sent letters to the presidents of 140 other colleges and universities, indicating what it sees as rampant abuse of the Internet2 network for trading copyrighted songs and movies and asking those institutions to work to limit activities that "violate the law and [their] own Acceptable Use Policies." The Motion Picture Association of America also said it will file similar suits but declined to say how many. Officials from
Internet2 acknowledged that trading unlicensed material over its network violates its policies and those of its member institutions. Greg Wood, spokesperson for Internet2, said the group has been working with member institutions on technologies that support effective and legal uses of the network. Chronicle of Higher Education, 13 April 2005 (sub. req'd)

Category 4B1 *Copyrights*

2005-04-15 **University of Wyoming old tests posting Website intellectual property rights violation copyright infringement university policy violation**

EDUPAGE;
http://www.cnn.com/2005/EDUCATION/04/15/old.tests.website.ap/

STUDENT FORCED TO TAKE TESTS OFF THE WEB

The University of Wyoming has insisted that a student remove copies of old tests from his Web site. Aaron Narva, a senior at the university, had posted the tests online and initially sold them to other students. Later, Narva gave the tests away for free. Narva said that old tests are a useful study aid, noting that the athletics department as well as sororities and fraternities make copies of tests available to their members. Dane Ciolino, professor of copyright law at Loyola University, said that Narva's comparison fails because by posting the tests online, he is making many more copies available. Ciolino also noted that fair use cannot apply if Narva was charging money for the tests. Narva is charged with violating university policies and will have a hearing at the university later this month. CNN, 15 April 2005

Category 4B1 *Copyrights*

2005-04-20 **file sharing illegal downloading BPI UK identity disclosure intellectual property rights violation copyright infringement lawsuit**

EDUPAGE; http://www.theregister.com/2005/04/19/bpi_p2p_lawsuits/

BRITISH COURTS ORDER FILE SHARERS TO BE IDENTIFIED

A British judge has ordered five ISPs to disclose the identities of 33 individuals accused by the British Phonographic Industry (BPI) of sharing more than 72,000 music files over the Web. The ruling is the latest win for the BPI in its efforts to combat illegal file sharing. ISPs have previously been forced to reveal the identities of another 57 individuals, all of whom were targeted for copyright violations. A recent study by research group TNS estimated that illegal file sharing cost the music industry more than 650 million pounds over the past two years. TNS also found that nearly 20 percent of people in the United Kingdom between the ages of 12 and 74 download music on the Internet, though the study did not distinguish between legal and illegal downloads. Representatives of the BPI contend that their efforts are working, noting that nearly 85 percent of those who do not currently download music said they would not do so illegally and that 15 percent of those who download illegally said they will begin to pay for music online. The Register, 20 April 2005

Category 4B1 *Copyrights*

2005-04-20 **file sharing debate Cornell University intellectual property rights violation copyright infringement**

EDUPAGE; http://chronicle.com/prm/daily/2005/04/2005042001t.htm

STUDENTS AT CORNELL DEBATE FILE SHARING WITH INDUSTRY

A recent colloquium at Cornell University pitted representatives of the entertainment industry against critics who say the copyright system is too restrictive and stifles innovation. Cary Sherman, president of the Recording Industry Association of America, and Fritz Attaway, executive vice president and general counsel of the Motion Picture Association of America, debated with Fred von Lohmann, lawyer with the Electronic Frontier Foundation, and Siva Vaidhyanathan, professor of communications at New York University, in front of a lively audience of about 200 students. Tracy Mitrano, policy adviser to Cornell's Office of Information Technologies, commented that the presence and participation of so many students indicated their earnest concern over legal and ethical issues surrounding file sharing. Though not the direct subject of the debate, Cornell is currently running a pilot program of the legal music-download service Napster, and participants on both sides offered their perspectives. A representative of Napster called the program a success, pointing to the large percentage of students who use the service regularly. On the other hand, von Lohmann said that the service is not a good deal for universities. "It feels free," he said, "but one way or another, you're paying for it." Chronicle of Higher Education, 20 April 2005 (sub. req'd)

Category 4B1 *Copyrights*

2005-04-28 **US intellectual property rights copyright anti-piracy law Family Entertainment and Copyright Act stiffer penalties violations**

EDUPAGE; http://networks.silicon.com/webwatch/0,39024667,39129955,00.htm

U.S. STRENGTHENS COPYRIGHT LAW

President Bush this week signed into law the Family Entertainment and Copyright Act, which allows for stiffer penalties for copyright violations. Under the law, individuals found guilty of possessing one or more copyrighted movie, music, or software files that have not been released to the public face a fine and prison term of up to three years. The law also criminalizes using a camcorder to record movies in theaters. Copyright holders supported the measure. Dan Glickman of the Motion Picture Association of America thanked Congress for what he called "their strong advocacy for intellectual property rights." Although some consumer groups opposed the law, some observers described it as a relatively minor expansion of existing law. Eric Goldman, professor of copyright law at Marquette University Law School, said he expects the Justice Department to use its new authority responsibly. Silicon.com, 28 April 2005

Category 4B1 *Copyrights*

2005-05-23 **Google book scanning digitize Library Project Association of American University Presses intellectual property rights violation copyright infringement**

EDUPAGE; http://chronicle.com/free/2005/05/2005052301t.htm

GOOGLE UNDER FIRE FOR LIBRARY PROJECT

The Association of American University Presses has become the latest group to voice objections to Google Print for Libraries, a project in which the search engine is scanning some or all of the books in five university and public libraries in the United States and Britain. In a letter to Google, the organization questions the notion that copyright law allows Google to scan copyrighted works into its database, even if only small portions of those texts are available online. Peter Givler, the group's executive director, said that copyright law fundamentally applies to making copies, regardless of what is done with them. The Publishers Association, which represents publishers in England, has also objected to the project, raising many of the same objections as the Association of American University Presses. For its part, Google said it is working with publishers to address their concerns and to make the project beneficial to them as well. Hugh P. Jones, copyright counsel of the Publishers Association, said he has been in contact with Google but that so far the two groups have failed to agree. Chronicle of Higher Education, 23 May 2005

Category 4B1 *Copyrights*

2005-06-20 **Google book scanning digitize Library Project University of Michigan Ann Arbor contract sharing Harvard Stanford New York intellectual property rights violation copyright infringement**

EDUPAGE; http://chronicle.com/prm/daily/2005/06/2005062001t.htm

MICHIGAN SHARES GOOGLE CONTRACT

In an effort to address concerns that have arisen over Google's project to digitize vast numbers of books from several libraries, the University of Michigan at Ann Arbor has made its contract with Google available online. Google has entered into agreements with libraries at Michigan, as well as Stanford University, Harvard University, the University of Oxford, and the New York Public Library, to scan most or all of their books, including those still protected by copyright. Books in the public domain will be made available on the Web; for those under copyright, only short excerpts will be online. Critics have contended that simply making digital copies of copyrighted books is a violation of copyright protections. The contract states that if either party becomes aware of copyright infringement, it will be quickly addressed. The contract also indicates that, aside from compensation for costs of transporting books, the university will receive no money for its participation in the project. John P. Wilkin, associate university librarian at Michigan, said he hopes that by making the university's contract publicly available, critics will see that there is nothing sneaky going on between Google and the library. Chronicle of Higher Education, 20 June 2005 (sub. req'd)

Category 4B1 *Copyrights*

2005-06-27 **music file sharing intellectual property rights violation copyright infringement Supreme Court decision precedent peer-to-peer P2P Grokster StreamCast**

EDUPAGE; http://online.wsj.com/article/0,,SB111927666876564101,00.html

SUPREME COURT RULES FOR ENTERTAINMENT INDUSTRY

In a long-awaited decision, the U.S. Supreme Court ruled unanimously that providers of file-sharing services can be held liable for copyright infringement that takes place on their networks. The decision overturns a lower-court ruling that companies including Grokster and StreamCast were not liable for such infringement because their P2P services have legitimate, legal uses as well. Citing the Betamax ruling of 1984, which permitted technology to videotape movies and television, the Ninth Circuit found in favor of the file-sharing companies. That decision was appealed to the Supreme Court by entertainment companies, which argued that file-sharing services are built on a model of facilitating infringement and that the companies charged have gone so far as to "disable mechanisms that would prevent the very infringement that sustains their businesses." The Supreme Court agreed, saying, in part, that "one who distributes a device with the object of promoting its use to infringe copyright … is liable for the resulting acts of infringement by third parties." Wall Street Journal, 27 June 2005 (sub. req'd)

Category 4B1 *Copyrights*

2005-06-29 **music file sharing intellectual property rights violation copyright infringement Supreme Court decision precedent peer-to-peer P2P Harvard professor side**

EDUPAGE; http://chronicle.com/prm/daily/2005/06/2005062902t.htm

HARVARD PROF CHANGES MIND, SIDES WITH ENTERTAINMENT INDUSTRY

Although he previously filed a brief supporting the defendants in the Grokster case recently decided by the Supreme Court, Harvard Law Professor Charles R. Nesson said he now believes the court decided appropriately in finding for the entertainment industry. Nesson, who specializes in technology law and serves as the faculty codirector of the Berkman Center for Internet and Society, said that during oral arguments in the case, which were held in March, he was convinced that file-sharing businesses that cater to individuals who violate copyright should be held accountable. "It is a good decision," he said, "because it says you can't be a total predator." In his earlier brief, Nesson had highlighted his concern that a ruling in favor of studios would inhibit plans to establish a digital library at the Berkman Center. Because the center is a nonprofit, however, and because the center would take demonstrable steps to limit copyright violations, Nesson said the courts would be unlikely to apply similar standards of liability to the digital library. Chronicle of Higher Education, 29 June 2005 (sub. req'd)

Category 4B1 *Copyrights*

2005-07-09 **file sharing trading downloading iMesh Sony BMG deal intellectual property rights violation copyright infringement**

EDUPAGE; http://news.com.com/2100-1027_3-5781196.html

IMESH INKS DEAL WITH SONY BMG

File-trading service iMesh has signed a deal with Sony BMG, one of the four leading U.S. record labels. Following the Supreme Court's recent ruling that exposes file-trading services for the copyright infringement of their users, iMesh announced it would develop a service "sanctioned" by the music industry. iMesh is reportedly also close to a deal with another of the big record labels, Universal Media Group, though iMesh would not comment on that. Similar to Mashboxx, iMesh uses technology that works to identify copyrighted songs so that record labels can claim royalties. In 2003, iMesh settled a copyright-infringement lawsuit with record labels for $4.1 million. CNET, 9 July 2005

Category 4B1 *Copyrights*

2005-07-14 **Australian copyright infringement music piracy link lawsuit ISP intellectual property rights violation**

EDUPAGE; http://news.com.com/2100-1030_3-5788344.html

AUSTRALIAN MAN AND ISP FOUND GUILTY OF LINKING TO PIRATED MUSIC

A court in Australia has found Stephen Cooper guilty of copyright infringement, as well as his Internet service provider (ISP) and several of its employees. Although Cooper did not provide copyrighted music files for download, he did create a Web site that directed users to sites that offered pirated music. Record companies had alleged that Cooper conspired with individuals at Comcen, the ISP named in the suit, to use the site to drive traffic to the ISP, thereby increasing opportunities for advertising revenue. The court agreed, marking the first time in Australia that someone has been convicted for the act of linking to pirated material online. The judge in the case has not yet determined damages. After the verdict, Michael Kerin, general manager of Music Industry Piracy Investigations, hailed the ruling as an important victory in the fight against piracy. "The verdict showed that employees of ISPs who engage in piracy can be seen in the eyes of the court as guilty," he said. CNET, 14 July 2005

Category 4B1 *Copyrights*

2005-07-19 **legal music downloading California universities anti-piracy peer-to-peer P2P intellectual property rights violation copyright infringement**

EDUPAGE;
http://www.cnn.com/2005/EDUCATION/07/19/campus.downloads.ap/index.ht
ml

LEGAL DOWNLOADS AT CALIFORNIA UNIVERSITIES

Two university systems in California have signed deals with Cdigix Inc. to provide legal downloads of songs and movies as part of their efforts to discourage illegal file trading. The 13 campuses of the University of California system and the 23 campuses of the California State University system are covered by the deal, though each campus must separately decide if it will participate and, if so, how to pay for it. The two systems are also negiating with other providers of online music and movies, including Sony, Napster, and Mindawn. David Walker, director of advanced technology at the University of California, said, "We're doing this because we do recognize that there is illegal file sharing of intellectual property." The two university systems include approximately 600,000 students across the state. CNN, 19 July 2005

Category 4B1 *Copyrights*

2005-07-28 **Congress peer-to-peer P2P abuse limit intellectual property rights violation copyright infringement child pornography**

EDUPAGE; http://news.zdnet.com/2100-9588_22-5809223.html

CONGRESS PRESSES P2P TO LIMIT ABUSE

Members of the Senate Commerce Committee took at tough stance in a hearing with members of the P2P community, saying that if developers of P2P technology do not take actions to limit copyright violations and keep pornography out of the hands of minors, Congress will. Sen.
Barbara Boxer (D-Calif.) said, "If you don't move to protect copyright, if you don't move to protect our children, it's not going to sit well." Sen. Ted Stevens (R-Alaska), chair of the committee, said he does not believe suggestions that there is nothing that can be done to control pornography on the Internet. Speaking for P2P interests, Adam Eisgrau, executive director of P2P United, responded that there is no "technological magic bullet" that will address copyright concerns or those regarding children's exposure to inappropriate content. Eisgrau urged Congress to revise copyright law to change the amount of compensation copyright holders can claim from those accused of infringement. He called for those involved "to intelligently and civilly discuss" the possibility of a voluntary licensing system. ZDNet, 28 July 2005

Category 4B1 *Copyrights*

2005-08-01 **peer-to-peer P2P intellectual property rights violation copyright infringement music piracy file sharing downloading lawsuits litigation UK Britain BPI**

EDUPAGE; http://news.bbc.co.uk/2/hi/entertainment/4735821.stm

BRITISH MUSIC INDUSTRY SUES FILE TRADERS

After reaching settlements with more than 60 alleged illegal file traders, the British Phonographic Industry (BPI) has filed civil charges against five individuals who reportedly refused to settle with the organization, according to Geoff Taylor, BPI general counsel. In March, a British court ruled that Internet service providers must disclose the names of those accused of copyright violations to the BPI. The suit alleges that the five defendants shared a total of nearly 9,000 songs on the Internet. "We will be seeking an injunction and full damages for the losses they have caused," said Taylor, "in addition to the considerable legal costs we are incurring as a result of their illegal activity." Although growing numbers of computer users are taking advantage of legal online music services, the BPI said it will continue efforts to prosecute illegal file traders. BBC, 1 August 2005

Category 4B1 *Copyrights*

2005-08-07 **intellectual property rights copyright Kansas Supreme Court ruling public institutions faculty work ownership revenue sharing**

EDUPAGE; http://insidehighered.com/news/2005/08/08/kansas

KANSAS SUPREME COURT TO RULE ON OWNERSHIP OF FACULTY WORK

The Kansas Supreme Court will evaluate an appellate court decision giving public institutions in Kansas the right to claim ownership of any faculty work, including books, with no negotiation on terms required. The lower court treated faculty work as "work for hire" under federal copyright law, classifying scholarly work as within the scope of employment of a faculty member. The current policy, designed in 1998, allows faculty to keep their book rights and has a revenue-sharing model for technology copyrights. Should the higher court decide in favor of the board, the policy could be changed at will. The case pits the Kansas Board of Regents against the Kansas National Education Association. Inside Higher Ed, 7 August 2005

Category 4B1 *Copyrights*

2005-08-12 **Google book scanning digitization Library project intellectual property rights violation copyright infringement AAP**

EDUPAGE; http://chronicle.com/free/2005/08/2005081201t.ht

GOOGLE MODIFIES LIBRARY PROJECT

Google has announced some changes to its Library Project following vocal criticism from a number of publishers. Under the terms of the project, Google made arrangements with five major libraries to scan some or all of their books, posting at least a portion of each book in an online repository for public access. Publishers complained that making such electronic copies of copyrighted works--regardless of whether they are put online--violates the rights of the copyright holder. Google now says it will not scan any book that a publisher specifically asks to be exempted, and it will not scan any copyrighted books until November, giving publishers time to review titles they might want excluded. Publishers appeared unmoved, however, with the Association of American Publishers (AAP) saying that Google's new plan "places the responsibility for preventing infringement on the copyright owner rather than the user." Peter Givler of the Association of American University Presses echoed the AAP's dissatisfaction with the changes to the project. He was glad that Google is trying to address publishers' concerns but said of the new policy that it "doesn't seem to me that it gets us very far." Chronicle of Higher Education, 12 August 2005

Category 4B1 *Copyrights*

2005-08-25 **file movie sharing peer-to-peer P2P illegal downloading logs MPAA lawsuit BitTorrent intellectual property rights violation copyright infringement**

EDUPAGE; http://news.com.com/2100-1025_3-5843082.html

MOVIE STUDIOS USE P2P SERVER LOGS AGAINST FILE TRADERS

The Motion Picture Association of America (MPAA) has filed 286 lawsuits for copyright infringement against individuals it identified from the server logs from file-trading services. MPAA efforts have resulted in the closure of a number of such services, many of which used BitTorrent technology. Information on file traders from those sites led to the "John Doe" lawsuits filed this week, marking the first time P2P logs have been used to seed such lawsuits. Indeed, Bram Cohen, who created BitTorrent to streamline downloading of very large files, said that using the technology for illegal file trading would be a "dumb idea" because it was never designed to conceal the identities of users. A statement from MPAA Senior Vice President John Malcom warns those who illegally download copyrighted movies, "You have no friends in the online community when you are engaging in copyright theft." CNET, 25 August 2005

Category 4B1 *Copyrights*

2005-08-31 **Google book scanning digitization project intellectual property rights violation copyright infringement lawsuits litigation**

EDUPAGE; http://www.internetnews.com/xSP/article.php/3531221

GOOGLE PRESSES FORWARD SCANNING BOOKS

Google is moving ahead with its plans to digitize vast numbers of books and make them available online. The search engine this week expanded its book search service to 14 countries, including the United Kingdom, Canada, India, New Zealand, South Africa, and Australia, where users can now search English-language books. Although laws in each country dictate small differences in how the service works, according to Jim Gerber, director of content partnerships, in all countries the service offers three types of results: for books in the public domain, the entire text is available online; copyrighted works whose publishers have signed agreements with Google are available to the extent that those agreements allow; for copyrighted books whose publishers have not made agreements with Google, only selected portions will be available online. This last group of results has raised the ire of publishers, who argue that Google has no right to display any part of copyrighted works without permission. Google has offered publishers the opportunity to identify specific titles that will be excluded from the service, but most publishing groups have said that approach is inherently backwards, giving Google blanket authority until and unless publishers complain. Internet News, 31 August 2005

Category 4B1 *Copyrights*

2005-09-02 **lawsuit litigation intellectual property rights violation copyright infringement graduate student paper sale vendor Website**

EDUPAGE; http://www.insidehighered.com/news/2005/09/02/papers

STUDENT SUES ONLINE TERM-PAPER VENDORS

A graduate student has filed a lawsuit charging three online vendors of term papers with selling a paper she wrote without her permission. Blue Macellari is currently pursuing graduate degrees at Johns Hopkins University and Duke University. The paper in question, which was written when she was a student at Mount Holyoke College, was posted on Macellari's personal Web page in 1999 but turned up for sale on DoingMyHomework.com, FreeforEssays.com, and FreeforTermPapers.com, all of which are owned by an Illinois company called R2C2. Macellari said she did not give her permission to use the paper, which itself could violate honor codes at Johns Hopkins and Duke. John Palfrey, law professor at Harvard University and executive director of the Berkman Center for Internet and Society, said that the defendants will have difficulty prevailing if Macellari's complaint is accurate. On the question of whether the action would have an appreciable effect on the sale of papers online, Palfrey was less optimistic. Comparing Macellari's lawsuit to similar actions to limit spam, he noted that spam continues to grow unabated. "It's hard to bring enough spam lawsuits to make a big difference," he said. Inside Higher Ed, 2 September 2005

Category 4B1 *Copyrights*

2005-09-06 **intellectual property rights violation copyright infringement Kazaa guilty ruling Australia music piracy**

EDUPAGE; http://www.internetnews.com/xSP/article.php/3532336

KAZAA FOUND GUILTY OF COPYRIGHT VIOLATIONS IN AUSTRALIA

An Australian court this week ruled in favor of the Recording Industry Association of America (RIAA) in its lawsuit against the developers of the Kazaa file-sharing service for copyright violations. The ruling is the second major blow to file traders this year, after the U.S. Supreme Court in June found Grokster liable for the copyright violations of its users. The court in Australia said that Sydney-based Sharman Networks, which owns and operates Kazaa, is well aware that its network is widely used to illegally trade copyrighted files and has done little to curb the practice other than adding warnings on the site. Those warnings, as well as an end user agreement that users must sign, "are ineffective to prevent, or even substantially to curtail, copyright infringements by users," said Judge Murray Wilcox in his ruling. Wilcox ordered Sharman to install filters on Kazaa to limit copyright violations within two months or discontinue the service. Wilcox also ordered Sharman to pay the majority of the RIAA's legal costs, and later this year a hearing will be held to assign damages that Sharman must pay to the entertainment industry. Internet News, 6 September 2005

Category 4B1 *Copyrights*

2005-09-12 **intellectual property rights copyright IBM source code business-process models donation insurance body**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1858051,00.asp

IBM DONATES CODE TO KATRINA EFFORT

In the wake of Hurricane Katrina and the Asian tsunami IBM has donated programming code and intellectual property to the Association for Cooperative Operations Research and Development (ACORD), the insurance industry's computing standards body. IBM has contributed more than 100 business-process models, model definitions and other industry content to ACORD in last week.

Category 4B1 *Copyrights*

2005-09-15 **RIAA peer-to-peer P2P Grokster Supreme Court ruling music piracy intellectual property rights violation copyright infringement**

EDUPAGE; http://news.com.com/2100-1030_3-5867085.html

RIAA TARGETS MORE P2P SERVICES

Following its Supreme Court victory against Grokster in June, the Recording Industry Association of America (RIAA) has sent cease-and-desist letters to seven unnamed providers of P2P services. In the Grokster case, the Supreme Court unanimously ruled that operators of P2P services are in part liable for the copyright infringements of their users and bear some responsibility for trying to prevent illegal file trading on their networks. The new cease-and-desist letters mention the Grokster case, saying the newly targeted companies are subject to similar legal standards, and invites those companies to contact the RIAA if they are interested in "pre-litigation resolution of these claims against you." Although the RIAA did not name the P2P providers who received the letters, likely candidates include eDonkey, LimeWire, Kazaa, BearShare, WinMX, and Free Peers. According to an RIAA spokesperson, "Companies situated similarly to Grokster have been given ample opportunity to do the right thing." CNET, 15 September 2005

Category 4B1 *Copyrights*

2005-09-19 **peer-to-peer P2P file sharing intellectual property rights violation copyright infringement Grokster Supreme Court shut down acquisition Mashboxx**

EDUPAGE; http://online.wsj.com/article/0,,SB112709561414344552,00.html

GROKSTER IN TALKS TO BE ACQUIRED

Following a Supreme Court defeat this summer, P2P service provider Grokster is reportedly considering being acquired by Mashboxx, a provider of legal downloads that is expected to start operating in the next few months. The Supreme Court's decision opened the door to record studios' suing Grokster and its codefendant Morpheus for damages from copyright violations taking place on their networks. The Recording Industry Association of America (RIAA), which brought the suit and has since notified other P2P providers of its intention to force them to limit copyright violations, is reportedly considering dropping its complaint against those providers that agree to adopt a business model of legal downloads. Indeed, the RIAA has already reached a settlement with iMesh, though the organization declined to comment on any discussions with Grokster. Wayne Rosso, cofounder of Mashboxx and formerly the president of Grokster, said his current company will talk to any P2P provider that wants to transition to a legitimate, legal service. Mashboxx has signed a deal with Sony and is negotiating deals with other major record labels. Wall Street Journal, 19 September 2005 (sub. Req')

Category 4B1 *Copyrights*

2005-09-21 **intellectual property rights violation copyright infringement Google book scanning project lawsuit litigation Authors Guild**

EDUPAGE; http://news.com.com/2100-1030_3-5875384.html

AUTHORS GUILD TAKES GOOGLE TO COURT

The latest challenge to Google's Print Library Project has come in the form of a lawsuit from the Authors Guild. Since Google announced its initiative to scan millions of books in several academic and public libraries and put those materials--or portions of them--online, the search engine has been roundly criticized by publishers and others who say the entire project represents copyright infringement. Nick Taylor, president of the Authors Guild, said, "It's not up to Google or anyone other than the authors, the rightful owners of these copyrights, to decide whether and how their works will be copied." Google continues to assert that it respects copyright and that the project does not violate copyright laws. Moreover, Google contends that the project will be a boon for publishers due to the broad exposure that scanned books will have online. Plaintiffs, who are seeking class action status for their suit, are asking the courts for damages and an injunction against scanning the texts in question. CNET, 21 September 2005

Category 4B1 *Copyrights*

2005-09-21 **Baida China search engine MP3 music download intellectual property rights violation copyright infringement lawsuit damages**

EDUPAGE; http://online.wsj.com/article/0,,SB112725336407246620,00.html

BAIDU TO APPEAL RULING IN COPYRIGHT CASE

Chinese search engine Baidu said it will appeal a ruling by a Beijing court that found the company guilty of copyright violations for providing access to sites that offer illegal music downloads. Baidu has a dedicated MP3 search feature that has been extremely popular, but with the search engine's success has come criticism from record companies, some of which are said to have initiated legal action against the company, though Baidu's lawyer did not comment on that. The Beijing court ordered Baidu to stop providing access to the illegal downloads and to pay copyright owners damages of about $8,500 for each of 34 copyrights that were allegedly violated. Li Decheng, Baidu's lawyer, said the verdict hinges on a misunderstanding of what the search engine's technology actually does. Wall Street Journal, 21 September 2005 (sub. req'd)

Category 4B1 *Copyrights*

2005-09-28 **Wikibooks Wikipedia online free Internet open source book publishing Google digital library intellectual property rights copyright**

EDUPAGE; http://news.zdnet.com/2100-9588_22-5884291.html

WIKIBOOKS ENTERS TEXTBOOK PUBLISHING FIELD

The Wikimedia Foundation launched the Wikibooks project to create a kindergarten-to-college curriculum of textbooks based on an open source development model. Material written for the new texts can be short or long and easily modified, and the resulting Wikibooks would be freely licensed. The goal is to produce thousands of books and smaller entries on a range of topics by employing a worldwide community of writers and editors. Any reader or student could create a personalized book or edit an existing title. Wikibooks currently contains more than 11,000 submissions from volunteers (professionals in many fields, college and graduate students, and professors). The project is still in the early stages and faces competitors such as Google's digital library project, which has run into copyright issues.
ZDNet, 28 September 2005

Category 4B1 *Copyrights*

2005-09-29 **RIAA lawsuit John Doe college student music piracy peer-to-peer P2P music file downloading intellectual property rights violation copyright infringement Supreme Court Kazaa Grokster**

EDUPAGE; http://www.internetnews.com/xSP/article.php/3552651

RIAA CONTINUES TO SUE SWAPPERS, MANY ON CAMPUS

The Recording Industry Association of America (RIAA) has filed a new batch of 757 John Doe lawsuits against users of P2P networks, accusing them of copyright violations. Included in the new suits are cases against individuals at 17 college and university campuses accused of illegally trading songs over Internet2's high-speed network using a file-sharing application called i2hub. The current action is the third time the RIAA has targeted users of i2hub and brings to 39 the number of campuses where students have been accused of copyright infringement using the application. Cary Sherman, president of the RIAA, invoked this summer's Supreme Court ruling against Grokster in a statement he issued with the new lawsuits. "The authority of the Supreme Court's unanimous ruling in the Grokster case," he said, "should not be ignored by students returning to campus this fall with sights set on free music." Sherman praised efforts at some campuses to educate users and restrict their ability to illegally trade copyrighted material on university networks. Internet News, 29 September 2005

Category 4B1 *Copyrights*

2005-10-03 **Yahoo intellectual property rights copyright book scanning project Open Content Alliance Internet Archive**

EDUPAGE; http://chronicle.com/free/2005/10/2005100301t.htm

YAHOO ANNOUNCES BOOK-SCANNING PROJECT

Yahoo has announced a plan to scan large collections of texts into an online digital archive, though officials said their approach differs in important ways from Google's similar venture, which has drawn extensive criticism and legal action. Yahoo's initiative, called the Open Content Alliance (OCA), represents a partnership with the University of California, the University of Toronto, the Internet Archive, and several other companies and organizations. Unlike Google's project, they will not scan any copyrighted work without explicit permission. Organizers of the project said the goal is to digitize and make freely available as much of what is in the public domain as possible. In addition, the archive will not be restricted to users of Yahoo. David Mandelbrot, Yahoo's vice president for search content, said the texts will be online in such a way that other search engines will be able to locate them. Much of the scanning for the OCA will be done by the Internet Archive, which has already been working with the University of Toronto on scanning several thousand books in its collection. Chronicle of Higher Education, 3 October 2005

Category 4B1 *Copyrights*

2005-10-07 **Google intellectual property rights violation copyright infringement book scanning project**

EDUPAGE; http://chronicle.com/daily/2005/10/2005100701t.htm

AUTHOR AND PUBLISHER PULL BOOKS FROM GOOGLE

Google's controversial program to scan millions of books has run afoul of a very prolific author and his publisher. Jacob Neusner, a research professor of theology at Bard College, has written more than 900 books. Calling Google's book-scanning project a violation of copyright, Neusner requested that his books not be included in the database. Google's response was that Neusner must submit a separate form for each book he wanted excepted from the project. Siding with Neusner, the Rowman & Littlefield Publishing Group, which has published many of Neusner's titles, then told Google it wanted all of its titles excluded from the project as well. Calling the scanning project "unfair and arrogant," Jed Lyons, president of Rowman & Littlefield, said, "[W]e don't want to do business with an organization that thumbs its nose at publishers and authors." Lyons said representatives from Google are trying to persuade the publisher to change its decision. Chronicle of Higher Education, 7 October 2005 (sub. Req'd)

Category 4B1 *Copyrights*

2005-10-11 **intellectual property rights Copyright Clearance Center permissions Blackboard higher education**

EDUPAGE; http://www.insidehighered.com/news/2005/10/11/copyright

SECURING COPYRIGHT PERMISSIONS GETS EASIER

The Copyright Clearance Center is launching a program to link its services with the Blackboard course management system. The center was created by Congress in the late 1970s to help businesses and academics obtain appropriate permissions from copyright holders. The new Copyright Permissions Building Block will allow users of Blackboard, which is implemented on about 1,200 campuses, to tie directly into the Copyright Clearance Center when creating a course. Many faculty are unsure about when permissions are needed to use copyrighted material in a course and when they are not, exposing themselves and their universities to possible copyright violations. The new tool will protect faculty and their institutions from such risks while ensuring that the rights of copyright holders are respected. Officials from the Copyright Clearance Center said they hope to add the functionality to other vendors' course management systems. Inside Higher Ed, 11 October 2005

Category 4B1 *Copyrights*

2005-10-25 **Microsoft Yahoo book project Internet archive intellectual property rights copyright Open Source Alliance**

EDUPAGE; http://news.zdnet.com/2100-9588_22-5913711.html

MICROSOFT JOINS YAHOO BOOK PROJECT

Microsoft has said it will participate in a recently announced book-scanning project led by Yahoo and the Internet Archive. Unlike Google's much-maligned project, the Yahoo initiative, called the Open Content Alliance, will only scan books that are in the public domain or for which explicit permission has been granted by the copyright holder. In contrast, Google will scan copyrighted books unless copyright holders specifically request that their books be excluded, though only small portions of copyrighted books will be available online. For its part, Microsoft will finance the scanning of about 150,000 books, while Yahoo will pay for about 18,000 books to be digitized. The Open Content Alliance also differs from Google's project in that all of the content from the alliance will be available from a database to any search engine; Google will be the only means to access the content of its project. Microsoft will create an MSN Book Search service next year, though the business model for particular services and fees has not been set, according to Danielle Tiedt, general manager of search content acquisition at MSN. ZDNet, 25 October 2005

Category 4B1 *Copyrights*

2005-10-29 **intellectual property rights violation copyright infringement Google book scanning project lawsuit litigation court damages**

EDUPAGE; http://news.bbc.co.uk/2/hi/business/4358768.stm

MORE SUITS TARGET GOOGLE'S BOOK SCANNING PROJECT

After failing to reach an agreement during several months of negotiations, a group of five publishers has filed a lawsuit against Google over its book-scanning project. The project has come under fire since it was announced, with publishers and copyright holders arguing that scanning their texts constitutes a violation of their copyright, regardless of whether the digital copy is made available online in its entirety. Penguin, McGraw-Hill, Pearson Education, Simon and Schuster, and John Wiley and Sons have sued Google, seeking to have the project cancelled. The publishers are asking for Google to pay court costs but not damages. All five are members of the Association of American Publishers, which had been in talks with Google for months. Last month, an organization representing writers sued Google over the book-scanning project. Google continues to maintain that it respects the rights of publishers and copyright holders and that the project will bring wider exposure for the scanned text. BBC, 19 October 2005

Category 4B1 *Copyrights*

2005-11-07 **peer-to-peer P2P illegal file movie sharing downloading intellectual property rights violation copyright infringement jail Hong Kong BitTorrent**

EDUPAGE; http://www.iht.com/articles/2005/11/07/business/bit.php

BITTORRENT USER SENTENCED FOR TRADING MOVIES

A court in Hong Kong has sentenced a citizen there to three months in prison for illegally distributing movies online. Chan Nai-ming was found guilty of making three movies available on his computer with BitTorrent tools and then, under the name Big Crook, of notifying Internet users that the movies were available for download. The case is the first in which a user of the BitTorrent technology has been found guilty of copyright infringement, and the case also represents Hong Kong's stepped up efforts to prosecute file-sharing crimes. The country is seen by many as a haven for intellectual-property crimes, a reputation the Hong Kong government hopes to shed. Government officials applauded the verdict and the sentence, saying they would deter others from committing similar crimes. Chan's lawyer said his client would appeal the verdict. Chan remains free on bail while the legal action continues. International Herald Tribune, 7 November 2005

Category 4B1 *Copyrights*

2005-11-07 **peer-to-peer P2P illegal file sharing downloading intellectual property rights violation copyright infringement Grokster Supreme Court ruling shut down RAA MPAA**

EDUPAGE; http://www.macworld.com/news/2005/11/07/grokster/index.php

GROKSTER REACHES THE END OF THE LINE

Following the U.S. Supreme Court's ruling this summer against Grokster, the company has agreed to a settlement that requires it to shut down its operations. The Supreme Court unanimously ruled that despite the possibility of noninfringing uses of Grokster's technology, the company could be held liable for violations that took place using its tools because it did not adequately discourage or deter users from such violations. According to the Recording Industry Association of America (RIAA) and the Motion Picture Association of American (MPAA), in the settlement Grokster agreed to end its operations and to permanently cease contributing to copyright infringement, either directly or indirectly. The Grokster site no longer includes links to download the company's software, instead featuring a message noting that copyright violations are illegal and will be prosecuted. The company said it plans to launch a legal service, called Grokster3G, in the near future. Macworld, 7 November 2005

Category 4B1 *Copyrights*

2005-11-10 **intellectual property rights violation copyright infringement protection Attorney General Alberto Gonzalez BSA RIAA**

EDUPAGE; http://news.com.com/2100-1028_3-5944612.html

FEDS PUSH FOR STRICTER COPYRIGHT PROTECTIONS

According to Attorney General Alberto Gonzales, the Justice Department recently submitted a package of legislative proposals to Congress that would broaden the scope of laws to protect copyright and would strengthen law enforcement powers to investigate such crimes. Among the proposals are recommendations to allow enforcement of copyrights, regardless of whether they are registered; to hold those found guilty of infringement liable for compensation to the victims; and to allow the seizure and destruction of counterfeit goods, equipment used to make such goods, and property acquired with the profits from such goods. The proposals would also make it a crime to "attempt to infringe copyright." Groups such as the Business Software Alliance and the Recording Industry Association of America welcomed the proposed changes to copyright law, while those concerned about fair use rights expressed reservations. An organization called Public Knowledge said in a statement that it is "concerned that the Justice Department's proposal attempts to enforce copyright law in ways it has never before been enforced." CNET, 10 November 2005

Category 4B1 *Copyrights*

2005-11-15 **illegal downloading intellectual property rights violation copyright infringement program initiative**

EDUPAGE; http://news.com.com/2100-1029_3-5954668.html

PROGRAM WILL SHED LIGHT ON DOWNLOADS

A new initiative is designed to give computer users the information they need to avoid downloading software that includes ad programs or other pieces of code that they do not want. The Trusted Download Program, created by America Online, Yahoo, CNET Networks, Verizon, and Computer Associates, will offer a certification program for companies that offer downloads. Rather than determining what should or should not be allowed in a download, however, the certifications simply require vendors to disclose exactly what the products do and what other components, such as adware or spyware, are included. Users are then given the opportunity before downloading any software to see that information. Before the software can be downloaded, users must explicitly agree to the indicated components of the download. Consent is then required again before the software can be installed. Clear instructions for uninstalling the software must also be provided. CNET, 15 November 2005

Category 4B1 *Copyrights*

2005-11-22 **movie piracy BitTorrent peer-to-peer P2P file sharing MPAA Bram Cohen deal copyright infringement intellectual property right protection**

EDUPAGE; http://news.com.com/2100-1032_3-5967750.html

MPAA AND BITTORRENT MAKE NICE

The Motion Picture Association of America (MPAA) and the creator of BitTorrent technology have announced an agreement that will keep many BitTorrent users from finding copyrighted movie files with the technology. In May, Bram Cohen added a service to his site, BitTorrent.com, that allowed users to search the Web for file downloads that use the popular technology. Under the new agreement, Cohen will remove copyrighted content from search results on his site. Although his technology has become a favorite for many traders in copyrighted material, Cohen does not offer services targeted at such users and has previously discouraged using the technology for illegal file trading. The entertainment industry has not targeted Cohen for prosecution for copyright violations, but a number of individual BitTorrent users have been sued for such violations. Despite the agreement, however, several other sites that search the Web for BitTorrent downloads remain operational. CNET, 22 November 2005

Category 4B1 *Copyrights*

2005-11-22 **Internet Web plagiarism copyright infringement intellectual property rights violations UK British government parents teachers children**

EDUPAGE; http://news.bbc.co.uk/2/hi/uk_news/education/4460702.stm

THE INTERSECTION OF TECHNOLOGY AND CHEATING

An expert in the impact of technology on teaching and learning has told the British government that parents and teachers--not technology tools--can effectively address the problem of Internet cheating. Following a report from the Qualifications and Curriculum Authority that identified widespread cheating, government officials sought advice from Jean Underwood, professor at Nottingham Trent University, about solutions to students' using technology to cheat. Underwood acknowledged that the line between providing appropriate assistance to a student and facilitating cheating is not always clearly defined, and she noted that some technologies can help examiners easily identify instances of plagiarism. But students, she said, will forever be able to find ways to circumvent technology that screens for cheating. The real solution will be to change student attitudes toward their work, making them understand the value of doing it themselves and genuinely learning the material. BBC, 22 November 2005

Category 4B1 *Copyrights*

2005-11-30 **Free Software Foundation FSF General Public License GPL open-source Richard Stallman license revision intellectual property rights copyright**

EDUPAGE; http://www.nytimes.com/2005/11/30/technology/30license.html

OPEN SOURCE LICENSE UP FOR REVISION

The Free Software Foundation has announced plans to revise the General Public License (GPL), which covers many open source applications including the Linux operating system. The license has not been revised since 1991, long before Linux and other open source applications had been implemented widely. Now, according to Eben Moglen, the foundation's general counsel, "The big boys, corporations and governments, have far more reason to be interested and concerned." The GPL and the Free Software Foundation are the creations of Richard Stallman, an unwavering critic of proprietary software and the author of much of the source code that led to the Linux operating system. Stallman has used the license and the foundation to foster what he says are the four principles of software: the ability to use, study, copy, and modify it. Stallman acknowledged that with the success of open source applications in recent years, the task of revising the GPL is complicated by patent issues, which must allow open source and proprietary software to run on the same systems. A first draft of the new GPL will be presented at MIT in mid-January. The revision process is expected to be completed by the end of 2006, with the Free Software Foundation making final decisions about changes. New York Times, 30 November 2005 (registration req'd)

Category 4B1 *Copyrights*

2005-12-12 **intellectual property rights copyright violation infringement Music Publishers' Association MPA scores lyrics downloading illegal**

EDUPAGE; http://news.bbc.co.uk/2/hi/entertainment/4508158.stm

SONG SITES UNDER THE GUN FOR COPYRIGHT VIOLATIONS

An organization representing U.S. sheet music publishers has said that in 2006 it will begin an effort to rein in the illegal online distribution of music scores and lyrics. The Music Publishers'
Association (MPA) said that such material is widely available on the Internet and suggested that, in addition to forcing sites to shut down and fining site operators, sentencing those responsible to jail time would be an effective deterrent. Lauren Keiser, president of the MPA, said the effort would initially focus on "very big sites that people would think are legitimate and very, very popular." David Israelite, president of the National Music Publishers' Association, echoed Keiser's comments, saying sites that publish guitar "tabs" and lyrics are stealing from songwriters and that "all tools under the law" will be used to curb the practice. Recently, music publishing company Warner Chappell forced PearLyrics to shut down its Internet site for unauthorized presentation of song lyrics. Walter Ritter, developer at PearLyrics, complained about the action from Warner Chappell, saying that his company provided a service that users want but that is otherwise unavailable. BBC, 12 December 2005

Category 4B1 *Copyrights*

2005-12-12 **intellectual property rights copyrights HarperCollins book publisher digitize Google Internet search index service**

EDUPAGE; http://online.wsj.com/article/SB113435527609919890.html

HARPERCOLLINS TO DIGITIZE BOOKS

HarperCollins has announced plans to digitize its own books and make those files available through search services, marking the latest development in the rapidly changing landscape of electronic access to books. Google is working on its hotly contested service to scan vast numbers of texts and make them available online, while other companies have begun their own programs to digitize books. The move by HarperCollins is that company's attempt to be a part of new technologies while retaining control over its content. The company will pay to have an estimated 20,000 backlisted books digitized, as well as about 3,500 new titles each year. Those electronic files will be open to search engines to make indexes but not to download images of the pages. According to Brian Murray, group president of HarperCollins, "We'll own the file, and we'll control the terms of any sale." Jane Friedman, chief executive of the publisher, said, "We want to be the best collaborator, but we also want to take charge of our future." The company said the effort would also allow it to keep certain titles available long after they are out of print. Wall Street Journal, 12 December 2005 (sub. req'd)

Category 4B1 *Copyrights*

2005-12-12 **music piracy illegal downloading intellectual property rights copyright violation RIAA lawsuit Cecilia Gonzalez ruling**

EDUPAGE; http://news.com.com/2100-1028_3-5991531.html

APPEALS COURT REJECTS SAMPLING DEFENSE

An appeals court has upheld a federal court ruling against a woman who had been sued by the Recording Industry Association of America (RIAA) for illegally trading music files. The RIAA initially offered Cecilia Gonzalez a settlement of about $3,500, which she rejected, and at her trial, a federal judge ruled in favor of the RIAA. In her appeal, Gonzalez argued that she had only downloaded songs with the intention of "sampling" them to decide if she wanted to purchase them and that this activity was protected under fair use. Gonzalez's computer contained at least 1,370 songs that she had downloaded. The three-judge appeals court rejected her argument and ordered Gonzalez to pay a fine of $22,500. In its opinion, the court compared her defense to a "thief's contention that he shoplifted 'only 30' compact discs, planning to listen to them at home and pay later for any he liked." The ruling gives the recording industry an appellate-court victory that--while only a formal precedent in Illinois, Indiana, and Wisconsin--is likely to bolster its legal efforts to curb illegal file trading. CNET, 12 December 2005

Category 4B1 *Copyrights*

2006-01-10 **Google online bookstore CES copyrights intellectual property rights issues**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4598478.stm 23

GOOGLE PONDERS STARTING AN ONLINE BOOKSTORE

At this year's Consumer Electronics Show (CES), officials from Google said they are considering launching an online bookstore, though they were quick to say such a venture would depend on permission from copyright holders. Google has been embroiled in ongoing legal disputes with publishers and other copyright holders over its effort to scan millions of texts, creating what CEO Eric Schmidt called "the world's largest card catalogue." Despite Google's contention that the scanning project does not violate copyright, many copyright holders disagree and have challenged the project in court. An online bookstore would be a fundamentally different proposition, according to Google officials, and such a plan would only go forward with the express permission of copyright holders. During the CES, Google unveiled an online video store, the company's first offering that allows consumers to pay for premium content.

Category 4B1 *Copyrights*

2006-02-06 **Google book scanning program University of Michigan president defense copyright intellectual property rights issues**

EDUPAGE; http://news.com.com/2100-1025_3-6035858.html 23

MICHIGAN PRESIDENT DEFENDS GOOGLE'S BOOK SCANNING

Speaking at the annual conference of the Professional/Scholarly Publishing division of the Association of American Publishers, the president of the University of Michigan defended her institution's participation in Google's Book Search program. The program has upset many publishers and other copyright owners, who contend that the project violates their intellectual property rights. Mary Sue Coleman told conference attendees that the program "is about the social good of promoting and sharing knowledge" and argued that Thomas Jefferson would have loved it. Insisting that vast numbers of cultural artifacts are at risk of being lost due to insufficient efforts at conservation, particularly among libraries, Coleman characterized Google's project as one of preservation and her institution's participation as central to the university's mission. She noted that the University of Michigan had been "digitizing books long before Google knocked on our door, and we will continue our preservation efforts long after our contract with Google ends." Coleman's comment also included a clear defense of the rights of copyright holders. Her institution would not "ignore the law and distribute [protected material] to people to use in ways not authorized by copyright."

Category 4B1 *Copyrights*

2006-03-03 **European Commission EC European Digital Library intellectual property rights copyright issues**

EDUPAGE; http://www.theregister.com/2006/03/03/european_digital_library_goes_live/ 23

EC PUSHES FOR DIGITAL LIBRARY

The European Commission (EC) is supporting a plan to create a European Digital Library that may one day include as many as six million volumes from libraries around Europe. The commission acknowledged that opinions differ about intellectual property concerns for digitized works, noting that a study it conducted showed wide disagreement between rights holders and institutions such as libraries. Still, the EC said it will work to settle those differences and begin working on the project, which would involve collaboration among all of the national libraries in the European Union and potentially other organizations such as museums. The EC said that by 2008, two million books, photographs, and other materials will be available through the European Digital Library and that this total could rise to six million by 2010.

Category 4B1 *Copyrights*

2006-03-13 **online library e-publishing problems Questia Media copyright intellectual property rights issues**

EDUPAGE; http://news.com.com/2100-1025_3-6048801.html 23

ONLINE LIBRARY TRIES TO AVOID PROBLEMS OF E-PUBLISHING

Houston-based Questia Media is a digital-library company whose executives believe they have seen past the errors of e-publishing. CEO Troy Williams and Chairman Rod Canion, who founded Compaq, survived the fallout from failed electronic publishing efforts and now count about 150,000 subscribers to their company's academic offerings, which target high schools and their students. Questia continues, in part, because although users did not warm to the idea of reading a novel on a screen, they are much more willing to conduct academic research online, said Williams. Much of Questia's current library of 65,000 books consists of hard-to-find materials. Much of the library content is copyrighted, so Questia has worked out agreements with publishers and other copyright holders, most of whom are happy to have high school students exposed to their materials.

Category 4B1 *Copyrights*

2006-03-13 **Google service online book sales copyright intellectual property rights Book Search Library Project litigation**

EDUPAGE; http://news.zdnet.com/2100-9588_22-6049002.html 23

NEW GOOGLE SERVICE SELLS BOOKS ONLINE

Google has announced a new service by which it hopes to sell online access to copyrighted books on behalf of publishers, similar to a program announced last fall between Amazon.com and Random House. With Google's new service, users would be able to buy electronic access to the full text of a book, based on terms determined by the publisher, but not allowed to make or save copies of the book. Currently, users of Google's Book Search service can see small bits of books but cannot access the full texts. According to Google, the new program is intended to help publishers increase revenues. The announcement comes as Google's legal troubles continue over its Library Project, a program to scan millions of books, including copyrighted books and those in the public domain. Public domain materials would be available online in their entirety, while only selected portions of copyrighted books would be online. Publishers and other copyright holders have challenged Google in court, saying the company has no right to make digital copies of their books, regardless of how it limits access to those copies.

Category 4B1 *Copyrights*

2006-04-23 **copyright law intellectual property rights US Congress revision Digital Millennium Copyright Act DMCA stricter EFF Software and Information Industry Association**

EDUPAGE; http://news.com.com/2100-1028_3-6064016.html 23

COPYRIGHT LAW UPDATE FAVORS COPYRIGHT HOLDERS

Despite pressure from a number of quarters to introduce restrictions on the Digital Millennium Copyright Act, Congress appears to be headed the other direction. Drafts of the Intellectual Property Protection Act of 2006 are circulating among lawmakers, and a spokesperson for the House Judiciary Committee said the bill will likely be introduced soon. The bill adds a number of new layers to copyright law, including increasing fines for certain copyright crimes; criminalizing attempted copyright violations, even if they fail; and allowing copyright owners to impound "records documenting the manufacture, sale, or receipt of items involved in" violations. Jason Schultz, staff attorney at the Electronic Frontier Foundation, said of this last provision that the recording industry has long wanted the ability to obtain server logs that would indicate "every single person who's ever downloaded" certain files. Keith Kupferschmid, vice president for intellectual property and enforcement at the Software and Information Industry Association, welcomed the bill, saying that it gives government officials needed authority to prosecute intellectual property criminals.

Category 4B1 *Copyrights*

2006-04-27 **copyright infringement intellectual property rights issues RIAA MPAA LANs**

EDUPAGE; http://news.com.com/2100-1025_3-6066118.html 23

COPYRIGHT INFRINGEMENT LETTERS TARGET LANS

The Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA) have sent letters to presidents of 40 universities in 25 states asking that they investigate possible illegal file trading on campus local area networks (LANs). The letters suggest that many students might think that trading copyrighted files across LANs is either not illegal or sufficiently shielded from copyright owners that it's okay to do. The letters encourage recipients to see whether students are using applications such as Direct Connect (DC++), MyTunes, or OurTunes to swap files on LANs and, if so, to take actions to stop them. Fred von Lohmann, a senior staff attorney at the Electronic Frontier Foundation, faulted the RIAA and the MPAA for being out of step with the times. Music labels sent similar letters regarding Napster, he said. "Here we are, seven years later, and the problem from their perspective is bigger than ever." The entertainment industry should make licensing arrangements with colleges and universities, he said, and "let the students do what they're going to do anyway."

4B2 Patents

Category 4B2 *Patents*

1997-05-14 **intellectual property patent antivirus**

COMTEX Newswire

Trend Micro Inc. sued McAfee Associates and Symantec Corp. for patent infringement because the competitors offer antivirus products that scan inbound files from the Internet for viruses. Trend Micro's General Counsel, Robert Lowe, said, "The broadest set of claims basically addresses when you have a server intercepting data being sent from one computer to a second computer, when you perform certain types of virus scanning processes such as separating high risk data from low risk data, and having certain types of predetermined actions that occur when a virus is detected, such as deleting it or storing it in a quarantine area." Other antivirus manufacturers might face lawsuits from Trend Micro as well, said the lawyer.

Category 4B2 *Patents*

2000-02-28 **personalization intellectual property privacy**

NewsScan, Salon.com
http://www.salon.com/tech/feature/2000/02/28/geographic/index.html

iCraveTV founder Bill Craig says he's developing technology that will indicate a Web surfer's geographic location when he or she logs on to a site, enabling the site operator to send pages targeted to people in that region. "It would be a huge breakthrough for the Internet and for copyright holders," says Craig, who would also stand to benefit, because it would enable him to sidestep the current controversy over his business of streaming video of sports events and movies to which he doesn't own the rights. The service is legal in Canada, but has unleashed protests from broadcasters in the U.S., and in January a U.S. judge ordered iCraveTV to stop the streaming. Craig is hoping that his "geographic intelligence" technology will alleviate concerns over iCraveTV, and maybe grow into an even more lucrative business than streaming TV broadcasts. "We want to build a business where we can go to rights holders and say, 'You want it released only in Canada, you've got it; in the U.S., you've got it,'" says Craig. (Salon.com 28 Feb 2000)

Category 4B2 *Patents*

2000-03-10 **software patents**

NewsScan, USA Today http://www.usatoday.com/life/cyber/tech/cth529.htm

Amazon CEO Jeff Bezos says that even though his company has received two potentially profitable e-commerce technology patents, he believes the length of time that patents protect a piece of software code is too long. "Especially in the age of the Internet, a good software innovation can catch a lot of wind in three or five years," Bezos wrote in an open letter to customers and Internet users (http://www.amazon.com/exec/obidos/subst/misc/patents.html/102-6583935-10424 35). He proposes drastically shortening the current 17-year term, and instituting a one-month public comment period prior to issuing patents so that other companies with similar or superior technology could ensure their rights are protected. Bezos says his company will retain its 1-Click and Amazon Affiliate patents, but will enforce them only "when there are important business reasons for doing so." (AP/USA Today 10 Mar 2000)

Category 4B2 *Patents*

2000-03-29 **patent regulations law research revamp change alter improve**

NewsScan, Wall Street Journal
http://interactive.wsj.com/articles/SB954286078412266261.htm

The U.S. Patent and Trademark Office is overhauling the way it reviews applications for many online practices, and will now require a broader search of past practices and inventions before awarding patents. The change comes in response to critics who charge the Office with granting overly broad patents for basic Web techniques, such as Amazon's "1-Click" ordering process. Examiners reviewing applications in the business-method area will now have to follow new procedures, including searching online databases for similar technology ideas. "If you make these decisions without adequate data, you run the very real risk of issuing patents on things that were already invented, or patents that are far broader than they should be," says Roland Cole, executive director of the Software Patent Institute. (Wall Street Journal 29 Mar 2000)

Category 4B2 *Patents*

2000-06-01 **intellectual property lawsuit patent infringement privacy exhibitionism**

NewsScan, New York Times
http://www.nytimes.com/library/tech/00/06/biztech/articles/01voyeur-lawsuit.html

Entertainment Network Inc., which operates a Florida-based Web site that paid college tuition for a half dozen women who agreed to have cameras situated throughout their group house sending 24-hour-a-day live video feeds of all aspects of their daily lives, . . . [sued] CBS and Infinity Broadcasting for allegedly stealing the site's marketing strategies and technical expertise. CBS and Infinity, who . . . [were] developing a similar program called "Big Brother," . . . [said] the suit . . . [was] frivolous. (AP/New York Times 1 June 2000)

Category 4B2 *Patents*

2000-06-02 **intellectual property advertising Web lawsuit patent infringement**

NewsScan

Juno Online Services . . . [sued] NetZero and Qualcomm for alleged patent infringement. Juno . . . [said] that the two companies . . . unlawfully made use of a technology developed by Juno that downloads advertisements and other content and displays it on a user's PC following an online session. (Bloomberg/Los Angeles Times 2 Jun 2000)

Category 4B2 *Patents*

2000-09-13 **intellectual property IP software copyright patent international agreement**

NewsScan, Wall Street Journal
http://interactive.wsj.com/articles/SB968792884357682385.htm

An administrative board for the European Patents Office has voted 10-9 to allow patents for software in Europe, with a final decision coming in November at a conference of the all the countries represented by the Office. Software patents are available in the U.S. and Japan, and multinational companies have been arguing for unlimited patenting as part of a uniform global legal framework. Critics, however, fear that large companies will use the patenting process as a tool to squelch innovative technologies that threaten their standard products. Among the dissenting countries were Germany, the U.K. and France. The head of the German delegation expressed his reservations over the change: "We would have problems with the U.S. tendency to patent everything that can be patented. That would stifle innovation and cause a glut of litigation." (Wall Street Journal 13 Sep 2000)

Category 4B2 *Patents*

2000-09-30 **intellectual property patent hyperlink litigation royalties court lawsuit**

NewsScan, New Scientist
http://www.newscientist.com/news/news.jsp?id=ns225851

It turns out that British Telecom has owned a U.S. patent covering hyperlinks for the last 14 years, but up until . . . [June had] made no attempt to exploit the patent commercially. The patent, which expires in 2006, was buried among 15,000 other global patents owned by the telecom giant until it was rediscovered "a few years ago" during a routine review of the company's intellectual property. BT has now decided to commercialize the technology, which allows Web surfers to move between pages by clicking on pictures or text — a move that could earn BT hundreds of millions of pounds. "We are not trying to stop anybody using the Internet. We simply want some reasonable royalties based on the revenues that other organizations are enjoying from making use of this intellectual property," BT said in a statement Monday. "We are not trying to take anything away from Tim Berners-Lee, but [BT] did invent a way of structuring information to make it easily accessible." The company added that it has spent the last two years researching its claim to the technology to make sure it holds up in court. "It is not something you want to shoot from the hip on," it said. (Financial Times 20 Jun 2000)

[However,] British Telecom's claim that it patented Internet hyperlinking technology back in 1976 . . . hit a snag [in September]. The U.S.-based Internet Patent News Service . . . [pointed] patent lawyers to a Web site (http://sloan.stanford.edu/MouseSite/1968Demo.html) that hosts a 90-minute film shot by Stanford University in 1968 featuring Douglas Englebart demonstrating the first computer mouse — and using it to click on hyperlinks. (New Scientist 30 Sep 2000)

Category 4B2 *Patents*

2000-10-04 **patent business method legislation**

NewsScan, Computer
Userhttp://www.computeruser.com/news/00/10/04/news5.html

A new bill introduced by Reps. Rick Boucher (D-Va.) and Howard Berman (D-Calif.) seeks to strengthen the review process for companies wishing to patent a "business method." The U.S. Patent and Trademark Office has recently come under fire for issuing patents to Amazon.com for its "1-click" check-out model, and to Priceline.com for its "name your own price" e-commerce service. These overly broad patents have led to unnecessary lawsuits over common business practices, say critics. "Something is fundamentally wrong with a system that allows individuals to get patents for doing the seemingly obvious," said Boucher. The Business Method Patent Improvement Act would require the Patent Office to publish all business method patent applications after 18 months, and would offer an administrative "opposition" process to settle disputes without litigation. It would also discourage patents on processes whose only distinguishing factor is that they use a computer to accomplish the task. (Computer User 4 Oct 2000)

Category 4B2 *Patents*

2000-12-28 **patent infringement lawsuit**

NewsScan, Hollywood Reporter
http://www.hollywoodreporter.com/convergence/index.asp?ee

NetZero, a free Internet access provider, has filed a patent infringement lawsuit against rival Juno Online Services. The suit alleges that NetZero's patent covers the technology used to present an on-screen advertising window that pops up separately from an Internet browser. Juno has responded that "On the contrary, we believe that NetZero has been infringing on a key patent held by Juno, in connection with which Juno filed a lawsuit against NetZero in June of this year." (Hollywood Reporter 28 Dec 2000)

Category 4B2 *Patents*

2001-01-25 **Web index patent infringement claim lawsuit intellectual property**

NewsScan

ALTAVISTA SAYS IT OWNS WEB INDEXING TECHNOLOGY
AltaVista has claimed a patent on a method of indexing Web sites used by most search engines and company intranets, and is threatening to sue companies using these search techniques for patent infringement. "We believe that virtually everyone out there who indexes the Web is in violation of at least several of [AltaVista's] key patents," says David Wetherell, CEO of CMGI, AltaVista's parent company. AltaVista owns 38 patents, "many of which we think are fundamental to the search area," and has applications pending for another 30, says Wetherell. "If you index a distributed set of databases -- that's what the Internet is. And even within intranets, that's one of the patents." AltaVista's move will intensify the debate over to what extent companies should be allowed to claim monopolies over methods that have become building blocks of the Internet. "If nothing is done, the Web will become fenced in by competing patents, turning an open, free and transparent playing field into a proprietary wasteland littered with nonsensical and stifling legislation," says one critic, CEO of a Web design and development company. (Financial Times 25 Jan 2001)
http://news.ft.com/news/industries/infotechnology

Category 4B2 *Patents*

2001-05-10 **patent infringement lawsuit judgement fraud**

NewsScan

RAMBUS FOUND GUILTY OF FRAUD
In a back-and-forth legal battle with Infineon Technologies, memory chip maker Rambus has been found guilty of fraud and slapped with punitive damages of $3.5 million. The fine was later reduced to $350,000 because of limitations in the local Virginia law. The verdict was a shocking turnaround for Rambus, which had sued Infineon on 57 charges of patent infringement. The jury agreed with Infineon's claim that Rambus had committed fraud because it participated in a broad chip industry project to develop fast memory chips, but did not reveal it had patents on similar technology. The goal of the cooperative project was to develop chips that would be royalty-free. (Financial Times 10 May 2001)

Category 4B2 *Patents*

2001-08-07 **patent Internet software update delivery subscription**

NewsScan

MCAFEE PATENT COVERS SUBSCRIPTION-BASED SOFTWARE
A new patent awarded to security software maker McAfee.com covers its system for delivering software and services over the Internet, giving it a potential advantage in the emerging trend of subscription-based software. "This doesn't close the door for competitors, it simply sets some boundaries for them," says market research executive Harry Fenik. Microsoft and other software vendors are already testing the concept of selling ongoing Web-based subscriptions to their products rather than collecting one-time fees for packaged goods, and now these companies "will have to tread carefully" to avoid infringing on McAfee's patent, or agree to pay licensing fees, says Fenik. Meanwhile, McAfee CEO Srivats Sampath says it's too early to say whether his company will sue potential violators, but "we will be sensitive to someone willfully flaunting the technology," he warns. (AP 7 Aug 2001)
http://news.excite.com/news/ap/010806/23/mcafee-patent

Category 4B2 *Patents*

2001-08-28 **patent infringement lawsuit digital television TV**

NewsScan

MIT SUES SONY OVER DIGITAL TV [28 Aug 2001]
The Massachusetts Institute of Technology is suing Sony Electronics, alleging that Sony's digital television business is infringing on four patents owned by MIT. The lawsuit says the technology was contributed by MIT scientists to the so-called "Grand Alliance" set up by the FCC in 1993, in which corporations and researchers collaborated to set a uniform U.S. standard for digital TV. Earlier, MIT won concessions by taking similar action against Sharp and Toshiba America, which also sell digital TVs. The digital sets cost anywhere from $800 to $12,000 or more, and MIT says it is entitled to a share of the profits. (AP 28 Aug 2001) http://news.excite.com/news/ap/010828/11/mit-sony

---

Category 4B2 *Patents*

2001-12-21 **patent infringement handwriting recognition lawsuit judgement court ruling**

NewsScan

PALM JUDGED GUILTY OF INFRINGING ON XEROX PATENT [21 Dec 2001]
A federal judge in Rochester, NY, has found handheld computer maker Palm Inc. and 3Com (Palm's former parent company) guilty of violating a Xerox's patent on handwriting recognition software called Unistrokes, which takes a simplified version of the alphabet that can be entered on a tablet with pen strokes. Palm will apparently have to decide whether to pay royalties to Xerox or discontinue using the software; in any event, it will have to pay Xerox damages for past infringement. Palm's sales were down 44% this quarter compared to the same quarter a year ago, and industry analyst Dylan Brooks of Jupiter Media Metrix comments: "With Palm reporting enormous losses and with some of the problems they've had in the market lately, this is the last thing they need." (Washington Post 21 Dec 2001)
http://www.washingtonpost.com/wp-dyn/articles/A9556-2001Dec20.html

---

Category 4B2 *Patents*

2002-03-15 **intellectual property patent law claim litigation judgement**

NewsScan

U.S. JUDGE NARROWS BT PATENT CLAIM
British Telecom suffered a setback in its attempt to enforce a patent filed in the 1970s, which it says covers the concept of hyperlinking, when U.S. Judge Colleen McMahon issued an opinion that cast doubts on the relevance of some of the patent's concepts to the modern-day Internet. British Telecom is attempting to extract royalty payments from Prodigy in a first test of its ability to enforce the patent, but critics say the inventions claimed by the company were detailed in previous work by British and U.S. scientists in the 1960s and have long since entered the public domain. (Reuters 14 Mar 2002)
http://story.news.yahoo.com/news?tmpl=story&cid=581&u=/nm/20020315/tc_nm/tech_hyperlinks_patent_dc_2

Category 4B2 *Patents*

2002-05-28 **intellectual property patent law infringement SCOTUS ruling**

FindLaw Download This 87

PATENT PROTECTIONS UPHELD BY SUPREME COURT
A unanimous U.S. Supreme Court on Tuesday set aside a ruling on copycat products that critics have charged would have seriously undermined the protections under the nation's patent system. The justices said a U.S. appeals court was wrong in its ruling that reinterpreted a major, long-standing doctrine of patent law in a way that makes it tougher for inventors to prove patent infringement.
http://news.findlaw.com/news/s/20020528/courtpatentsdc.html

Read The Opinion (FESTO CORP. v. SHOKETSU KINZOKU KOGYO KABUSHIKI CO.)
http://laws.lp.findlaw.com/us/000/001543.html

Category 4B2 *Patents*

2002-06-04 **fair use intellectual property digital rights copyright policy**

NewsScan

TECHNOLOGY IS EASY, POLICY IS HARD: CERF WANTS RULE CHANGES
Internet pioneer and WorldCom senior VP Vint Cerf thinks government policies are impeding the advancement of the Internet, but acknowledges: "Policy problems are harder to solve, and probably more important than the technology ones. Policy doesn't have a simple answer. Sometimes it has to do with attitude, sometimes it has to do with culture, sometimes it has to do with the legal framework." He would like to see the government require phone and cable network companies to share those networks with Internet service providers at a fair price, and he would like to see strong support for the extension of "fair use" principles of copyright law extended to the digital world: "Even though there will be some people in the publishing industry who think fair use isn't fair, I believe it has served reasonably well. We don't have a good definition of fair use for online, digital material." If policy issues were worked out properly, technologists would be able to create a new communications environment that would have enormous impact. For example, people "could download a one-hour HDTV movie in 16 seconds. This changes your whole view of video on demand." And with new views like that will come a renaissance of communication, entertainment, and learning, because "most of the creative uses don't come from the people who design the network, they come from the people who use it. That's what happened with the World Wide Web and Java." (KRT/San Jose Mercury-News 3 Jun 2002)
http://www.siliconvalley.com/mld/siliconvalley/3392998.htm

Category 4B2 *Patents*

2002-06-27 **intellectual property competition proprietary information codes embedded microcomputers diagnostic systems competition information warfare infowar**

RISKS, http://www.cnn.com/2002/TECH/ptech/06/24/diagnosing.cars.ap/ 22 13

Monty Solomon contributed this tid-bit about the consequences of secrecy:
At least a couple of times a week, mechanic Ernie Pride tells customers at his independent repair shop he can't fix their cars because he doesn't know what's wrong with them. Go to the dealer, he advises. He has the experience and knowledge to service vehicles but lacks the closely guarded information needed to diagnose problems with today's high-tech cars. Automakers refuse to make much of it available to independent shops that compete with higher-priced dealerships. The practice is raising hackles in Congress and a vigorous defense by the industry. ... [AP, June 24, 2002]

Category 4B2 *Patents*

2002-07-19 **intellectual patent compression algorithm images**

NewsScan

PICTURE THIS: COMPANY CLAIMS JPEG PATENT
Forgent Networks, based in Austin, Texas, is claiming that a patent it holds covering a "coding system for reducing redundancy" directly applies to the compression technique used in the creation of JPEG images. The patent originally was granted to Compression Labs in 1986 and later acquired by Forgent, which says it will now seek licensing revenue from companies that use JPEG "in all fields of use," with the sole exception of the satellite broadcast business. Last month, Forgent sealed a licensing deal with Sony, and a company spokeswoman says it's in discussions with several other companies, but did not disclose names. In a statement published last week, Forgent said the patent could apply to companies that make "devices used to compress, store, manipulate, print or transmit digital images." The licensing plan has sparked concern among many users of digital imaging technology. "It's sort of an ambushing kind of thing," says one digital photography hobbyist. (Wired.com 19 Jul 2002)
http://www.wired.com/news/business/0,1367,53981,00.html

Category 4B2 *Patents*

2002-08-23 **patent litigation lawsuit royalties hyperlinking Web**

NewsScan

CLICK-AND-PAY: BT ASSERTS PATENT CLAIM FOR HYPERLINKS [7 Feb 2002]
The BT Group in the U.K. is targeting Prodigy in the first of a series of planned lawsuits aimed at enforcing its claim to have a copyright covering hypertext links. The claim, which is supported by a U.S. patent obtained in 1984 (before the creation of the World Wide Web), would allow BT to demand royalty payments from Internet service providers who offered their users the ability to surf the Web by using hyperlinks. A company spokesman argues: "We believe we have a duty to protect our intellectual property and we would expect companies to pay a reasonable royalty based on the revenues that they have enjoyed through the use of that intellectual property." Various critics of the BT lawsuit maintain that hyperlinking was conceived all the way back in the 1960s, and promoted by such well-known Internet luminaries as Ted Nelson and Doug Engelbart. (Retuers/USA Today 7 Feb 2002)
http://www.usatoday.com/life/cyber/tech/2002/02/07/patent-suit.htm

DOUBTS ARISE OVER BT'S CASE FOR HYPERLINK PATENT [13 Feb 2002]
Judge Colleen McMahon, the judge assigned to British Telecom's case defending its right to collect royalties from a 26-year-old patent covering hyperlinking, has raised doubts over the validity of the case. She noted that it would be difficult to prove that a patent first filed in 1976 -- long before the Web was created -- would apply to today's technology, and that comparing a 1976 computer to a 2002 computer was like comparing a mastodon with a jet. If BT prevails, its first likely target for royalty collection is Prodigy Communications, and if that attempt is successful, BT will notify other ISPs in the U.S. that they must pay up. (The U.S. is the only country where the patent has not yet expired.) Some analysts say the royalties could total tens of millions of dollars if the patent is upheld. (Financial Times 13 Feb 2002)
http://news.ft.com/news/industries/internet&e-commerce

BT LOSES BATTLE TO CLAIM HYPERLINK ROYALTIES
In a test case for British Telecom's claim that it owns a patent on hyperlinking technology, U.S. Judge Colleen McMahon has dismissed BT's claims, saying that Prodigy's use of the technology did not infringe on BT's 25-year-old patent. McMahon found several flaws in BT's argument, most notably that the Internet has no "central computer" as described in the original patent filing. As part of its defense, Prodigy offered a 1968 video by Stanford University computer scientist Douglas Engelbart apparently demonstrating hypertext technology, eight years before BT filed its patent application in the U.S. (BBC News 23 Aug 2002)
http://news.bbc.co.uk/1/hi/technology/2212203.stm

Category 4B2 *Patents*

2002-10-11 **patent law court ruling appeal intellectual property**

NewsScan

COURT RULES INTEL IN VIOLATION OF INTERGRAPH PATENTS
A U.S. federal court has concluded that Intel violated Huntsville, Alabama-based Intergraph's patents on the parallel-instruction computing (PIC) technology used in Intel's high-end 64-bit Itanium microprocessors. Intel plans to appeal. A loss will cost the company as much as $250 million in fines and new licensing fees. (Reuters/San Jose Mercury News 11 Oct 2002)

Category 4B2 *Patents*

2002-11-11 **patent infringement lawsuit settlement intellectual property**

NewsScan

SONICBLUE AND TIVO CALL A TRUCE
Sonicblue and TiVo are dismissing their patent infringement claims against each other and plan to devote their energies to building the market for digital video recorders (DVRs) instead. "We believe our energies are better spent expanding the market for digital video recorders rather than fighting each other. Both sides believe in the merits of their respective positions, but the overall success of the DVR category is what is most important to the companies at this time," said the two companies in a joint statement. Sonicblue still faces a lawsuit, however, filed by major entertainment companies, including AOL Time Warner, MGM, Disney and the big three TV networks. The plaintiffs allege that the company's service, which allows viewers to strip out commercials and to send copies of recorded programs to other ReplayTV recorders via the Internet, amounts to copyright infringement. (CNet News.com 8 Nov 2002)
http://news.com.com/2100-1040-965166.html

Category 4B2 *Patents*

2002-12-19 **instant messaging patent intellectual property**

NewsScan

AOL PATENTS INSTANT MESSAGING TECHNOLOGY AOL
Time Warner has quietly won a U.S. patent for its ICQ instant messaging technology, representing a potential goldmine for the media giant. The broadly worded patent defines AOL's IM application as one that enables users to chat with and identify one another across a specific "communications network," opening up the possibility for AOL to collect royalties from rivals. ICQ, which was developed in the mid-1990s by a group of Israeli scientists at a company called Mirabilis, was the first breakthrough chat application. It filed a patent for its technology in 1997 and was acquired by AOL in 1998 for $287 million. (Reuters 19 Dec 2002)

Category 4B2 *Patents*

2003-01-23 **patent Web frame interface licensing**

NewsScan

SBC CLAIMS PATENT ON WEB INTERFACE
SBC Communications is enforcing its patents on what it claims is any use of frame-like user interfaces in Web sites. According to SBC's interpretation of its "Structured Document Browser" patents, hundreds of thousands of Web sites, including that of the U.S. Patent and Trademark Office, could be infringing on the telecom's intellectual property. "SBC Intellectual Property currently is working with several commercial Web site owners regarding patent licensing agreements related to specific techniques for enabling consistent navigation features from different pages of a Web site," SBC announced in a statement yesterday. At issue are Web sites that use an interface that remains on-screen while a user navigates the site. SBC so far has contacted only a few sites with requests for licensing fees, with suggested amounts ranging between $527 and $16.6 million per year, depending on the annual revenue of the company and what kind of license they sign up for. (The Register 23 Jan 2003)
http://www.theregister.co.uk/content/6/28985.html

Category 4B2 *Patents*

2003-02-06 **patent law streaming audio Web**

NewsScan

STREAMING PATENT HAS NET RADIO SITES STEAMED
A company that says it owns patents on the process of transmitting compressed audio or video online is flexing its muscle, demanding fees from a host of Internet multimedia companies. Acacia Media Technologies says its patents may even cover pay-per-view movies on cable TV and in hotel rooms. And while Acacia's move has outraged Internet entrepreneurs, many of them are reluctantly forking over the fees. "We did research on the claims and found that they were pretty clear — somewhat broad, but specific enough to cover us," says Zack Zalon, general manager of the Radio Free Virgin Web site. "We realized that they were tight enough that a license would be substantially less expensive in the long run than litigation." Meanwhile, the trend toward companies exercising ownership over what generally are viewed as overly broad patents has drawn the ire of many experts, but analysts admit it's a strategy that's likely to increase in popularity. "With the economy the way it is, you see a lot more people trying to leverage their intellectual property. It's one of the few ways left that people can actually make money," says Rich Belgard, an independent patent consultant. (CNet News.com 6 Feb 2003)
http://news.com.com/2100-1023-983552.html

Category 4B2 *Patents*

2003-02-20 **patent dispute lawsuit I&A identification authentication PKC public key cryptosystem PKI infrastructure**

NewsScan

PATENT DISPUTE ON AUTHENTICATION SOFTWARE
Inventor and retired electronics engineer Leon Stambler is suing VeriSign, RSA Security, and other companies for allegedly violating his patents on software used in electronic transactions to let one party be certain of another's true identity. Although Internet security experts generally believe that the inventor's patents merely imitate work previously done by Stanford and MIT cryptographers during the 1970s and 1980s, intellectual property lawyers predict that the retired engineer's effort may very well be successful. Attorney Jack Russo says: "Patent litigation is fairly expensive and you will see people settle for what seems to be large sums." (New York Times 20 Feb 2003)

Category 4B2 *Patents*

2003-02-25 **patent law overly broad software**

NewsScan

U.S. PATENT SYSTEM IS BROKEN, SAYS LESSIG
Stanford law professor Lawrence Lessig has warned Europeans not to follow the same path toward software patent protection as the U.S., saying "The system in America is broken — to the great detriment of software developers generally — and there is no reason to believe the Europeans could do any better." Critiquing the last 10 years' tendency toward granting overly broad patents, he notes that software developers — those whom patents ostensibly would protect — are actually some of the most vocal critics of the current system. "Developing software is [now] like crossing a minefield," says Richard Stallman, the originator of the free software movement that has developed the GNU/Linux operating system. "With each design decision, you might step on a patent that will blow up your project." Lessig says that Europeans should take pains to avoid a similar quagmire: "American software developers will continue to choke on software patents, especially as more and more get enforced in massively expensive litigation? Until software patents prove themselves safe and effective, Europe could gain a great deal by sparing its developers the same drug. Rather than copying a failed American policy, the Europeans could be exploring alternatives to patents that might provide protection without sinking the intended beneficiaries. No doctor would approve an untested drug for his or her patient. Nor should Europe inflict such a remedy on its already weakened software industry." (Financial Times 20 Feb 2003)

Category 4B2 *Patents*

2003-04-10 **video on demand patent infringement lawsuit movie studios**

NewsScan

MOVIELINK SLAPPED WITH PATENT INFRINGEMENT LAWSUIT
Movielink, a joint venture involving five Hollywood studios, has been sued for patent infringement by USA Video Technology in a case that could have an impact on other future video-on-demand endeavors. The USA Video lawsuit alleges that Movielink, which sells digital copies of films for downloading from the Internet, violates a patent called "Store and Forward System" that was awarded in July 1992. The patent broadly covers a method for Internet users to request and receive "a digitized video program for storage and viewing," according to the complaint. The plaintiff's attorney says the resolution of the case could affect many other VOD offerings. "This case is ripe now because the content is available and the legal landscape permits (an online movie rental service)," says Erik B. Cherdak, plaintiff attorney for the case. "The reality is this case has far-reaching effects on whether the corner video store will remain as a going concern in the future." Movielink, which launched last November, is a partnership of MGM, Paramount Pictures, Warner Brothers, Sony Pictures Entertainment and Universal Pictures. (CNet News.com 10 Apr 2003)

Category 4B2 *Patents*

2003-04-24 **intellectual property rights eBay patent violation defense**

NewsScan

EBAY DEFENDS ITSELF AGAINST PATENT-VIOLATION CHARGES
Online auction eBay is involved now in patent litigation involving in claims by MercExchange LLC that eBay stole from MercExchange founder Thomas G. Woolston his ideas for the programs and processes now used by eBay in the auctions it conducts on the Internet. Attorneys for eBay say the patent-violation charges are baseless. The judge presiding over the trial (estimated to last about three weeks) cautioned the two sides in the dispute: "It's going to be your responsibility to make sure this is something the average person can understand." (AP/San Jose Mercury News 24 Apr 2003)

Category 4B2 *Patents*

2003-04-27 **trade secret law violation University Chicago student**

NewsScan

STUDENT CONFESSES TO VIOLATION OF TRADE SECRET LAW
University of Chicago student Igor Serebreyany is pleading guilty to charges of putting secret documents about DirecTV's anti-piracy technology on the Internet, in violation of the federal Economic Espionage Act of 1996, which prohibits anyone from disclosing trade secrets for economic benefit. He theoretically faces penalties of up to 10 years in prison and a $250,000 fine, but has negotiated a deal under which his prison sentence would be no more than one year. The documents described details about the design and architecture of DirectTV cards. (AP/ContraCostaTimes 27 Apr 2003)

Category 4B2 *Patents*

2003-05-14 **SCO intellectual property infringement linux unix open software**

NewsScan

LINUX USERS WARNED OF INTELLECTUAL PROPERTY INFRINGEMENT
The SCO Group, which acquired control of Unix intellectual property from Novell after it bought the rights from AT&T back in 1992, has sent letters to Linux customers warning that commercial users may face legal liability for using Linux with a license from SCO. If SCO's tactic is successful, it could undermine one of the basic tenets of the open software movement, of which Linux has been the most successful example. Linux is a Unix derivative first developed in the 1990s, and has won a loyal following because of its low cost, reliability and ability to run on inexpensive computer hardware. Linux developer Linus Torvalds says he has not heard what parts of Linux might be infringing: "I'd dearly love to hear exactly *what* they think is infringing, but they haven't told anybody. Oh well. They seem to be more interested in FUD [fear, uncertainty and doubt] than anything else." The latest move follows a $1-billion lawsuit filed by SCO in March against IBM, alleging IBM took parts of the Unix code and transferred them to Linux. IBM dismissed the lawsuit as unfounded. (AP 14 May 2003)

Category 4B2 *Patents*

2003-05-19 **Unix license Microsoft SCO Group part of code duplicative Darl McBride**

NewsScan

MICROSOFT SCOOPS UP UNIX LICENSE FROM SCO
Microsoft is buying the rights to SCO Group's Unix technology for an undisclosed amount, in a move that will bolster SCO's controversial campaign to demand royalties from users of the Linux operating software, which SCO claims infringes on its Unix patents. Linux supporters have demanded that SCO identify which parts of the code are duplicative, but SCO says that doing that would allow programmers to cover up their transgressions by rewriting the software. "That's like saying, 'show us the fingerprints on the gun so you can rub them off,'" says SCO CEO Darl McBride. Microsoft, which competes fiercely with both Linux and Unix, at the same time has been a long-time backer of SCO and some in the Linux community have speculated the software giant is secretly bankrolling SCO's litigation to reduce the Linux threat. A Microsoft spokeswoman denied that rumor. (Wall Street Journal 19 May 2003)

Category 4B2 *Patents*

2003-05-21 **patent W3C World Wide Web Consortium Patent Policy Working Group Daniel Weitzner**

NewsScan

W3C ADOPTS POLICY ON PATENTS
The World Wide Web Consortium (W3C) has approved a policy on patents that requires all those who participate in the development of a W3C recommendation must license essential claims on a royalty-free basis. It also requires W3C members to make disclosures on patents they own and requests that anyone else who sees technical drafts share their knowledge of patents which may be essential. At the same time, the policy suggests a process for handling unexpected patent claims that are inconsistent with the terms of the W3C Patent Policy. In that instance, the W3C will convene a Patent Advisory Group, which may then recommend: a legal analysis of the patent, the removal of the patented feature, or cessation of work in that area altogether. The W3C's efforts to create a patent policy have been contentious since it first released its Patent Policy Framework Draft in 2001, says Daniel Weitzner, chair of the Patent Policy Working Group, who cautioned technology companies against trying to exploit the patent exception process. "Anyone who thinks that's going to be an easy way to squeeze fees out of Web standards I think is mistaken," says Weitzner. (Internet News 21 May 2003)

Category 4B2 *Patents*

2003-05-28 **ebay patent MercExchange Buy it Now section half.com purchase auctions**

NewsScan

EBAY LOSES PATENT-INFRINGEMENT LAWSUIT
A federal jury in Virginia has concluded that online auction eBay and its Half.com unit intentionally infringed on patents belonging to MercExchange. MercExchange is also seeking an injunction prohibiting eBay from continuing its current "Buy it now" program, which allows eBay customers to make fixed-priced purchases rather than participating in auctions. EBay is asking the judge to reverse the $35-million judgment against it, whereas MercExchange is saying that the judgment should be tripled, because the jury's verdict was that the patent infringement was deliberate rather than accidental. (Bloomberg/New York Times 28 May 2003)

Category 4B2 *Patents*

2003-05-28 **software group linux SCO threatned proof of intellectual property rights**

NewsScan

GERMAN SOFTWARE GROUP THREATENS SCO OVER LINUX
German software alliance Linuxtag, which backs the Linux operating system, has issued an ultimatum to SCO Group: prove your claims that Linux infringes on your Unix technology patents by May 30 or we'll see you in court. "SCO is massively unsettling our members and the companies that are potential exhibitors at the fair with those claims," says a Linuxtag spokesman. "It they don't stop that, or present proof for the intellectual property rights they are claiming, we are going to apply for a preliminary injunction at the court on Friday." SCO's German unit says it's received Linuxtag's motion and is considering whether to respond before SCO's case against IBM, a major Linux promoter, goes to court. Some of Germany's largest companies, including Siemens AG, the Deutsche Bundesbahn and Volkswagen, have received letter from SCO notifying them their use of Linux may be in violation of its rights. (Reuters 28 May 2003)

Category 4B2 *Patents*

2003-08-25 **intellectual propery copyright DVD copy-protection California**

NewsScan

FREE SPEECH TRUMPED BY TRADE SECRETS
The California Supreme Court has ruled Monday that courts may block Internet users from posting computer code that could be used to illegally copy DVD movies if the code revealed legitimate trade secrets online. Justice Janice Rogers Brown, in reversing a lower court ruling on a 7-0 vote, said the California Supreme Court's action "does not violate the free speech clauses of the United States and California constitutions." Companies such as Boeing, Ford and AOL Time Warner filed briefs urging the justices to side with the plaintiff, which had argued that trade secret protections trump First Amendment speech protections. (AP/San Jose Mercury News 25 Aug 2003)

Category 4B2 *Patents*

2003-10-29 **patent Microsoft W3C Tim Berners-Lee**

NewsScan

BERNERS-LEE SIDES WITH MICROSOFT IN PATENT CASE
The World Wide Web Consortium (W3C) has come out on Microsoft's side in a patent-infringement lawsuit the company has on appeal. A lower court awarded $521 million to a researcher who holds a patent the Web consortium contends is based on "prior art" that was not considered when the patent was granted (nor was it considered in the Microsoft trial). W3C director Tim Berners-Lee has asked that the U.S. the patent office begin a review of the patent "to prevent substantial economic and technical damage to the operation of the World Wide Web."(New York Times 29 Oct 2003)

Category 4B2 *Patents*

2003-11-12 **patent office University Califronia web pages tim berners-lee microsoft interactive programs internet explorer**

NewsScan

PATENT OFFICE RECONSIDERS CONTROVERSIAL NET PATENT
The U.S. Patent and Trademark Office is taking the unusual step of reconsidering a patent awarded to three University of California researchers in 1998. Patent No. 5,838,906 covers technology used to build small interactive programs into Web pages, potentially affecting everything from banner ads to interactive customer service. The patent's validity was invoked by Eolas Technologies (which was founded by one of the inventors and has licensed the patent exclusively) in its lawsuit against Microsoft. That legal action resulted in a $520 million jury award in favor of Eolas and prompted Microsoft to pledge a redesign of its Internet Explorer browser to avoid further infringement, a move that Web creator Tim Berners-Lee says could "render millions of Web pages and many products of independent software developers incompatible." Deputy patent commissioner Stephen G. Kunin cited "a substantial outcry from a widespread segment of the affected industry" in his decision to reexamine the patent and noted that patent examiners may not have adequately considered "prior art" in their investigations. (AP 12 Nov 2003)

Category 4B2 *Patents*

2003-11-24 **system for managing intellectual property alain rossmann**

NewsScan

NEW SYSTEM FOR MANAGING INTELLECTUAL PROPERTY
French-born Silicon Valley entrepreneur Alain Rossmann is creating his fifth high-tech start-up, PSS Systems, to develop a product that will help companies keep their documents compliant with government and industry regulations. Rossman's past start-ups have included Phone.com (now Openwave Systems), C-Cube Microsystems, Radius, and EO; the first three went public and the fourth was sold to AT&T. The new PSS system will allow a company to manage its intellectual property by tracking even those documents that are used for R&D outsourcing. It will also help government agencies collaborate in the fight against terrorism. (San Jose Mercury News 24 Nov 2003)

Category 4B2 *Patents*

2003-12-04 **patent intellectual property agreements cooperation**

NYT
http://www.nytimes.com/2003/12/04/technology/04soft.html?th=&pagewanted=print&position=

In December 2003, Microsoft announced "that it would adopt a more liberal policy for licensing its intellectual property, opening the doors to its storehouse of patents and copyrights to outsiders." [Steve Lohr, New York Times]. The reporter continued with an analysis suggesting that Microsoft could be trying to demonstrate a better attitude to regulators in the United States and Europe who are investigating monopolistic practices of the enormous company.

Category 4B2 *Patents*

2004-01-12 **patent infringement lawsuit Rockwell automation customers**

RISKS; http://www.law.com/jsp/article.jsp?id=1039054478800 23 12

SUING THE CUSTOMERS

Joyce Scrivner writes about a patent infringement countersuit by Rockwell Automation Inc. Rockwell was suing "a law firm currently suing Rockwell's customers." Rockwell customers were being sued because they could potentially cough up more money than Rockwell itself. Rockwell feels that the law firm, Niro Scavone, sought to "'shakedown' manufacturers through threats of potential business interruption or catastrophic damages." In a follow-up article, contributor Paul Robinson comments that Rockwell automation "doesn't have a leg to stand on" in this case. According to patent law, he says, everyone in the chain of producer, distributor, and consumer is liable if they've been in contact with a product that infringes on someone else's patent. It doesn't matter who is actually sued. Robinson adds that Rockwell is wrong to call Niro Scavone's actions a 'shakedown' because the law firm was "using the courts." He explains: "If I threaten you if you don't pay me for something, that's extortion and a crime. If I threaten to sue you if you don't settle, that's legal. If I just sue you anyway, whether I have a case or not, that's also legal."

Category 4B2 *Patents*

2004-01-13 **US patent system obsolete**

NewsScan

PATENTLY ABSURD?

A number of industry and government officials have come to the conclusion that the U.S. patent system has become absurd — especially in fields such as computers, software and biotechnology. Intellectual property attorney Mark Banner says: "Very bad patents are getting through. It's draining millions of dollars that could be spent on finding a better mousetrap." Yet the current system has its defenders. Jon Dudas of the Patent Office insists that most patents are valid, and Jay Walker (whose company patented the "reverse auction") argues: "We as a nation are ahead of the rest of the world because we have strong property rights. Everybody said you couldn't have patents on electricity. Guess what? They were wrong." Others in the debate take the position that the problem with the patent system is not that it's unfair but that it's irrelevant: software executive Jordan Greenhall says: "If you didn't have any patents at all, people would still be doing the same stuff because of the speed of the marketplace." (USA Today 13 Jan 2004)

Category 4B2 *Patents*

2004-03-02 **Toshiba flash memory intellectual property rights issues patents licences**

NewsScan

TOSHIBA ENGINEER SUES FOR 20% OF FLASH MEMORY PROFITS

A former Toshiba engineer is suing his former employer, the Japanese electronics maker, alleging that he was insufficiently compensated for his work developing flash memory technology. That technology has made 20 billion yen (US$183.49 million) in profits for Toshiba, and the engineer, who now a university professor, is asserting that his fair share of those profits is 20%. Flash memory chips, which are able to retain data after power is switched off, are widely used in mobile phones, digital cameras and other portable electronics.(San Jose Mercury News 2 Mar 2004)

Category 4B2 *Patents*

2004-03-05 **intellectual property rights patents Internet Explorer browser Microsoft infringement**

NewsScan

PTO REJECTS EOLAS PATENT CLAIM

In a move that could cripple their lawsuit against Microsoft, the U.S. Patent and Trademark Office has reached a preliminary decision to invalidate Eolas Technologies' and the University of California's patent on Web browser technology. Eolas and UC had won a $521 million verdict against Microsoft last year for infringing on their patent in its Internet Explorer browser, a decision that was upheld last month by an Illinois federal judge. The software giant had already started to make changes to Internet Explorer to comply with the court's ruling, but suspended those changes last month in hope of a reprieve by the PTO. "We have maintained all along that, when scrutinized closely, this patent would be ruled invalid," said a Microsoft spokesman. Meanwhile, Eolas attorney Martin Lueck said it was not uncommon for the PTO to invalidate a patent claim as the first step in the review process and remained upbeat about the final outcome of the litigation. (Reuters/CNet News.com 5 Mar 2004)

Category 4B2 *Patents*

2004-03-17 **intellectual property rights ownership Kazaa source code**

NewsScan

KAZAA RHUMBA

Fabian Toader, a programmer in Redmond, Washington, claims he wrote the source code for the Kazaa file-sharing software while he was a freelancer in his native Romania, and he is now suing the program's distributor, Sharman Networks, for $25 million in compensation. Toader says, "Sharman has made millions using my software. I just want to be fairly compensated for my contribution." Sharma, whose home offices are in Sydney, Australia, says: "The work done by Fabian Toader on early versions of the Kazaa Media Desktop software was done under a work for hire agreement that expressly states that Kazaa B.V. owned all rights to any work related to the development of the software." A Sharman spokesman has called Toader's new lawsuit a "shakedown effort." (AP/USA Today 17 Mar 2004)

Category 4B2 *Patents*

2004-04-12 **intellectual property digital rights management patents lawsuit settlement**

NewsScan

MICROSOFT SETTLES INTERTRUST PATENT LAWSUIT

Microsoft has settled a lawsuit brought three years ago by InterTrust Technologies, which alleged that the software giant infringed on its digital rights management patents. Microsoft will pay $440 million to InterTrust, which is owned by a joint venture of Sony, Philips Electronics and investment banking firm Stephens Inc. The announcement comes on the heels of Microsoft's agreement last week to pay Sun Microsystems $1.6 million to settle an antitrust lawsuit and resolve patent claims. And last month, Microsoft settled a patent lawsuit filed by AT&T over voice-recognition technology. Terms of that settlement were not disclosed. (AP/Washington Post 12 Apr 2004)

Category 4B2 *Patents*

2004-08-09 **patent licensing demand Acacia academia intellectual property rights**

NewsScan

ACACIA PRESSURES ACADEMIA FOR PATENT PAYMENTS

Acacia Media Technologies, which last month suffered a setback in its efforts to force adult entertainment sites to make licensing payments for using its patented streaming video technology, has now turned its attention to higher education, whipping off dozens of letters to colleges claiming
the schools' use of streaming video for purposes such as distance learning violates its patents. Acacia's digital media patents were acquired from Greenwich Information Technologies in 2001 and since then Acacia has secured dozens of licensing deals with companies, including Walt Disney.
And while a handful of colleges and universities have agreed to pay up, most have resisted. The American Council on Education and the Electronic Frontier Foundation both are advising colleges not to pay, citing last month's legal ruling that several terms in Acacia's patents were indefinite
-- a verdict that could knock a hole in Acacia's case for demanding payments from other sectors. "Honestly, I think it's a sign of desperation," says EFF staff attorney Jason Schultz. "Acacia knows the hammer is coming down on its patents, and it's going to extract as much as it can before the apocalypse," adding that the company's tactics were "a threat to the future of education… I think that's despicable. Universities are under enough pressure in their budgets right now to try to pay for
everything. The last thing they need to do is give a pound of flesh to some tech company that doesn't even make a product." (AP 9 Aug 2004)

Category 4B2 *Patents*

2004-10-01 **patents Microsoft open source FAT file allocation table appeal**

NewsScan; http://www.usatoday.com/tech/news/techpolicy/2004-10-01-fat-patent-rejected

MICROSOFT LOSES PATENT BATTLE

In a victory for "open source" advocates, the U.S. Patent and Trademark Office has rejected a Microsoft application for a patent on a system called File Allocation Table (FAT), which lets people create and find files on a computer using easy-to-remember names. The reason for the rejection is that the technology in question is already widely used throughout the industry. Independent patent expert Greg Aharonian comments: "It's like getting a patent on cheesecake." Microsoft plans to file an appeal.

Category 4B2 *Patents*

2004-11-03 **video games patent Electronic Arts Atari Sega McKool Smith**

NewsScan; http://www.theregister.com/2004/11/03/game_cos_3d_lawsuit/

GAME MAKERS THREATENED BY PATENT LAWSUIT

Computer game makers, including such big names as Electronic Arts, Atari and Sega, have been sued by Texas-based McKool Smith, which claims the makers' games violate a 1987 patent that covers a way to display 3D objects realistically in a 2D space, such as a computer monitor. The technique is used by almost every game that uses 3D modeling, including older games such as Quake and Doom. The companies are now frantically researching prior art, citing games such as The Colony and Spectre, which may have been released before the 1987 patent was granted. (The Register 3 Nov 2004)

Category 4B2 *Patents*

2004-11-15 **Microsoft Xbox modification cheating live multiuser games fraud**

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/10189248.htm

MICROSOFT CRACKS DOWN ON XBOX MODIFICATIONS

Cameron Ferroni, Microsoft's general manager for the Xbox software platform, says the company's not planning to sue individual users but that it does want to stop users of the Xbox Live online service from modifying their machines to improve their performance at games. Ferroni believes it's important that Microsoft prevent cheating on Xbox Live (where multiple players can take part in games) and says that the company's goal is to make sure there's a level playing field for game players. (AP/San Jose Mercury News 15 Nov 2004)

Category 4B2 *Patents*

2005-01-11 **IBM patents source projects licensing fees property patents Matsushita Electric Industrial**

EDUPAGE; http://www.nytimes.com/2005/01/11/technology/11soft.html

IBM OFFERS PATENTS TO OPEN SOURCE PROJECTS

IBM will begin allowing the use of 500 technologies covered by patents it holds by developers working on open source projects. While IBM will not forfeit the patents, it will seek no licensing fees from groups that use them on projects that meet a definition by the Open Source Initiative. Despite past donations of intellectual property to open source groups, the new program is seen as a fundamental shift in the company's approach because unlike those donations, this one does not hold the potential to harm IBM's competitors. The 500 patents that will be available involve 14 categories of technology and do not target any specific open source project. IBM said it hopes to create a "patent commons," including the initial 500 as well as other patents, that other companies could join. IBM's new approach to managing its intellectual property, however, has not diminished its pursuit of new patents. IBM, which is the world's largest patent holder, collected 3,248 new patents in 2004, 1,300 more than Matsushita Electric Industrial, which had the second-highest tally for the year.

Category 4B2 *Patents*

2005-03-02 **University of California Microsoft patenet infringement intellectual property rights violation Eolas Internet Explorer Web browser**

EDUPAGE; http://news.com.com/2100-1032_3-5596500.html

EOLAS CASE SET TO GO AROUND AGAIN

Both sides claimed partial victory from an appeals court ruling in the patent infringement case between Microsoft and the University of California (UC). The case focuses on technology patented by Mike Doyle, a researcher at the university, which has been incorporated into most Web browsers, including Microsoft's Internet Explorer (IE). Eolas Technologies, a company that was spun off of the university and which holds a patent on the technology, has claimed patent infringement by Microsoft. A lower court found for Eolas and awarded it $565 million in damages, but an appeals court this week sent the case back to a lower court to be tried again. The appeals court ruled that Viola, a browser written before UC applied for its patent, should have been considered by the jury. If Viola is determined to be "prior art," UC's patent could be invalidated. Microsoft has also argued that Doyle misled the U.S. Patent and Trademark Office, a charge that the appeals court decision brings back to the table. In UC's favor, the appeals court said the patent, if valid, covers a wider range of applications than attorneys for Microsoft had argued. The court also upheld the finding that copies of IE shipped abroad would be covered by a U.S. patent and would be considered in determining damages if the patent is upheld. CNET, 2 March 2005

Category 4B2 *Patents*

2005-09-30 **intellectual property rights patent infringement lawsuit litigation Eolas University of California Web browser launch technology Microsoft WWC**

EDUPAGE; http://chronicle.com/daily/2005/09/2005093001t.htm

EOLAS RULING SWINGS BACK TO UNIVERSITY OF CALIFORNIA

The U.S. Patent and Trademark Office has issued its final ruling in favor of the University of California in its patent dispute with Microsoft. At issue is a technology used for launching certain applications in Web browsers. The technology was developed at the University of California at San Francisco and licensed to a company called Eolas Technologies. Eolas and the university had earlier won a $521 million judgment against Microsoft for violating the patent in its software, but that ruling was appealed on the grounds that the patent was not valid. Despite a preliminary ruling in which the Patent and Trademark Office indicated its leaning toward Microsoft's position on the Eolas patent, the final ruling upholds all of the university's claims. The ruling rejects the assertions of both Microsoft and the World Wide Web Consortium that the patent relies on "prior art." The case now returns to district court for trial. Chronicle of Higher Education, 30 September 2005 (sub. req'd)

Category 4B2 *Patents*

2005-11-08 **intellectual property rights patent infringement ACE Acacia Research litigation lawsuit**

EDUPAGE; http://chronicle.com/daily/2005/11/2005110801t.htm

LEGAL DANCE WITH ACACIA CONTINUES

Not long after Acacia Research updated the terms of a licensing agreement it is offering to colleges and universities, officials at the American Council on Education (ACE) said they are continuing with efforts to challenge Acadia's patent claim. Acacia contends that it owns patents that cover streaming of audio and video files over the Web and that most higher education institutions use technology that violates those patents. After a backlash from the terms it initially offered, Acacia revised its offer, freeing small schools from any licensing fee but insisting that large schools owe as much as $5,000 per year. Although ACE was involved in the negotiations that led to the revised offer, David Ward, the organization's president, informed member campuses that ACE has not endorsed any agreement with Acacia and said institutions might benefit from waiting "until the broader legal negotiations are completed." Karlton Butts, vice president of licensing for Acacia, said he is not aware of any broader negotiations and contended that Acacia is "not trying to pull a fast one." Sheldon E. Steinbach, general counsel for ACE, said the communication from Ward was "a clarification that we felt was necessary." Many institutions remain cautious about signing a licensing agreement, pointing to ongoing debate over the legitimacy of Acacia's patent claims. Chronicle of Higher Education, 8 November 2005 (sub. req'd)

Category 4B2 *Patents*

2005-11-10 **intellectual property rights patent infringement issue share source code**

EDUPAGE; http://news.zdnet.com/2100-3513_22-5943781.html

NEW GROUP ADDRESSES OPEN SOURCE PATENT ISSUE

A new organization hopes to eliminate one of the major obstacles to adoption of open source technology: concern over patent and royalty disputes over shared code. The Open Invention Network (OIN), which includes IBM, Sony, Royal Philips Electronics, and Linux distributors Red Hat and Novell, will acquire and freely share patents that organizers hope will encourage broader adoption of open source tools, particularly Linux. Any organization that agrees not to assert its patents over those who have licenses with OIN will be permitted to use OIN patents for free. The business model for OIN represents a new arrangement in which patents are shared to promote the underlying Linux technology. Industry analyst Richard Doherty said, "A lot of lawyers are going to throw their hands up and ask, 'How do we make money from this?'" The answer, he said, is that they might not. ZDNet, 10 November 2005

Category 4B2 *Patents*

2005-11-15 **intellectual property rights patents Open Source Development Labs OSDL library database**

EDUPAGE; http://www.internetnews.com/dev-news/article.php/3564201

OSDL OPENS PATENT LIBRARY

The Open Source Development Labs (OSDL) has unveiled its public patent library (PatentCommons.org), which offers a free searchable database of patents donated to the open source community. The library is a catalogue of patents whose owners have agreed not to exert any control over the technologies as long as they are used to improve the open source community. The OSDL does not hold any of the patents but simply offers the site as a clearinghouse for information about patents, where they came from, what they do, and under what conditions they can be used. Officials from the OSDL said they expect more patents to be added to the database soon but that they wanted to launch the service now, ahead of patent pledges they expect later. The site should free open source developers from much of the uncertainty they have when using patented technologies in their development efforts. Internet News, 15 November 2005

Category 4B2 *Patents*

2005-11-28 **intellectual property rights violation patent infringement US Supreme Court Hearing eBay case MercExchange**

EDUPAGE; http://online.wsj.com/article/SB113319064690608067.html

U.S. SUPREME COURT TO HEAR E-BAY PATENT CASE

The U.S. Supreme Court will hear a patent-infringement lawsuit involving eBay and a patent holding company that eBay lost in 2003. MercExchange holds a patent over sales and purchasing methods used in online auctions. The appeal deals with whether the U.S. District Court that handled the case should have issued a permanent injunction against eBay. The Federal U.S. Circuit Court of Appeals, which handles patent lawsuits on appeal, ruled that the federal trial judge should have issued a permanent injunction against eBay, which said they believe the legal reasoning used will force district courts to issue more injunctions in patent lawsuits. Meanwhile, Congress is considering legislation that would change how patent injunctions are issued by federal courts. The U.S. Patent and Trademark Office is also exploring the issue. Wall Street Journal, 28 November 2005 (sub. req'd)

Category 4B2 *Patents*

2005-11-30 **intellectual property rights patent Blackberry litigation**

DHS IAIP Daily;
http://www.techweb.com/wire/ebiz/174403076;jsessionid=0GCQWZ
R4LYF22QSNDBGCKH0CJUMEKJVN

BLACKBERRY WORKAROUNDS READIED TO SIDESTEP PATENT PROBLEMS

Research In Motion Ltd. said Wednesday, November 30, it is preparing workarounds to keep Blackberry services in the U.S. up and running, in the event a court issues an injunction against the company as a result of ongoing patent litigation. A new chapter emerged in its dispute with NTP Inc., earlier Wednesday when a federal judge invalidated a $450 million settlement between RIM, maker of the Blackberry email device, and the Arlington, VA, patent holding company. The ruling was a victory for NTP, which had argued that the settlement was never finalized. As a result, U.S. District Judge James R. Spencer could next consider whether to re-issue an injunction preventing RIM, based in Canada, from offering Blackberry service in the U.S. In a statement, RIM said it was prepared to argue against the injunction, but also said it was ready to make changes to its technology to avoid the alleged patent infringement. "As a contingency, RIM has also been preparing software workaround designs, which it intends to implement if necessary to maintain the operation of Blackberry services in the United States," the company said.

Category 4B2 *Patents*

2005-12-02 **intellectual property rights violation patent infringement Microsoft Internet Explorer IE tweak Eolas Technologies applets ActiveX**

EDUPAGE; http://www.internetnews.com/xSP/article.php/3568286

MICROSOFT TWEAKS IE TO SIDESTEP EOLAS PATENT

Microsoft has made a change to its Internet Explorer browser to avoid infringing on a patent held by Eolas Technologies, though Microsoft continues to dispute the validity of that patent. Eolas was granted a patent in 1998 for a technology that allows certain programs, such as applets or ActiveX controls, to be launched automatically from Web pages. Eolas sued Microsoft in 1999 and in 2003 was awarded $521 million for infringement of its intellectual property. That case has been working its way through appeals courts and is set for a retrial. In the meantime, Microsoft has opted to modify its browser so that users must manually accept the launching of ActiveX controls on Web pages. Unlike an earlier proposal, the one implemented will not require users to accept each such control on a Web page but simply to accept them all at once. Microsoft's Michael Wallent said this solution is less intrusive and that for most users, it will be "an almost invisible change." Microsoft is working with developers to rewrite Web pages in a way to minimize the effects of the change. Internet News, 2 December 2005

Category 4B2 *Patents*

2005-12-04 **intellectual property rights violation patent infringement BlackBerry lawsuit**

RISKS; http://tinyurl.com/dtkra 24 11

BLACKBERRY PATENT INFRINGEMENT LAWSUIT

A "long-running patent infringement battle between the maker of BlackBerry, Research In Motion, and NTP, a tiny patent holding company, might cause a service shutdown, perhaps within a month. … R.I.M., which is based in Waterloo, Ontario, promises it has a solution that will keep its beloved BlackBerries humming even in the face of an injunction. While most analysts view the prospects of a shutdown as unlikely, they have little faith in the proposed solution, which has potential legal pitfalls of its own. What's more, the history of the struggle between the companies means that no outcome is certain."

[Abstract by Peter G. Neumann]

Category 4B2 *Patents*

2005-12-15 **intellectual property rights violation patent infringement mobile mail Visto lawsuit Microsoft**

EDUPAGE;
http://www.siliconvalley.com/mld/siliconvalley/business/technology/13415305.htm

MOBILE MAIL PATENT SUIT FILED AGAINST MICROSOFT

Visto Corporation of Redwood Shores, California, a start-up company dedicated to mobile e-mail, has sued Microsoft Corporation for infringement of three patents. The suit targets methods for handling information between servers and handheld devices. Microsoft bundles its Windows Mobile operating system with its Exchange e-mail server. According to a Visto release, "This method of bundling software … potentially increases the rate and manner in which their infringement on Visto's patents occurs." Microsoft representatives declined to comment until the company had seen and evaluated the suit. San Jose Mercury News, 15 December 2005

Category 4B2 *Patents*

2005-12-19 **NTP RIM Blackberry patent review infringement lawsuit court case e-mail rejection**

EDUPAGE; http://www.nytimes.com/2005/12/20/technology/20rim.html

PATENT OFFICE EXPECTED TO REJECT NTP PATENTS

The U.S. Patent and Trademark Office notified NTP, a patent holding company, and Research in Motion (RIM), maker of the BlackBerry wireless e-mail device, that it expects to reject the five patents held by NTP. The two companies are involved in a patent infringement lawsuit brought by NTP. The patent office had issued preliminary rejections of the e-mail patents in the past, but speeded its review process in response to a request by RIM. The patent review is separate from the patent infringement lawsuit, which could potentially stop most BlackBerry service in the United States. NTP expects to appeal the final patent rulings, a process that could take several years.

Category 4B2 *Patents*

2006-01-30 **Microsoft Office forced upgrade corporate business users legal setback**

DHS IAIP Daily; http://news.zdnet.com/2100−3513_22−6032870.html 23

MICROSOFT PATENT SPAT FORCES BUSINESSES TO UPGRADE OFFICE.

Microsoft has begun e-mailing its corporate customers worldwide, letting them know that they may need to start using a different version of Office as a result of a recent legal setback. The software maker said Monday, January 30, that it has been forced to issue new versions of Office 2003 and Office XP, which change the way Microsoft's Access database interacts with its Excel spreadsheet. The move follows a verdict last year by a jury in Orange County, CA, which found in favor of a patent claim by Guatemalan inventor Carlos Armando Amado. Microsoft was ordered to pay $8.9 million in damages for infringing Amado's 1994 patent. That award covered sales of Office between March 1997 and July 2003. Although existing customers can keep using older versions on current machines, any new installations of Office 2003 will require Service Pack 2, released by Microsoft in September. Office XP will need to be put into use with a special patch applied. The software maker started notifying customers this month, in an e-mail sent via its sales channel. All those affected will have been informed by next month, Microsoft said. The company said the necessary downloads are available from its Website.

Category 4B2 *Patents*

2006-03-03 **Blackberry patent litigation completed RIM NTP**

DHS IAIP Daily; http://www.eweek.com/article2/0,1895,1933824,00.asp 23

RIM, NTP SETTLE CASE: BLACKBERRY SERVICE IS SAFE.

BlackBerry maker Research In Motion (RIM) and patent-holding company NTP on Friday, March 3, announced that both parties have entered into a settlement agreement and a license that will end the patent litigation that had been threatening to shut down BlackBerry service in the United States. Under the terms of the settlement, RIM will make a one-time payment to NTP of $612.5 million. In return, NTP has granted RIM a license that will let RIM continue its BlackBerry-related wireless business, according to officials at both companies. The license covers all the current wireless e-mail patents involved in the litigation as well as any future NTP patents, officials said. The resolution also protects all the wireless carriers and channel partners who sell BlackBerry products, as well as any other hardware makers who have licensed BlackBerry software for use in their own devices.

Category 4B2 *Patents*

2006-03-28 **patent campus technology threat campus card money transfer JSA Technologies intellectual property rights issues**

EDUPAGE; http://chronicle.com/daily/2006/03/2006032802n.htm 23

ANOTHER PATENT THREATENS CAMPUS TECHNOLOGY

Another company has contacted a number of colleges and universities about a technology patent they might be infringing, this time for systems that transfer money across the Internet to campus cards. in 1998, JSA Technologies applied for a patent, which was granted in 2005, that covers such transfers. Many institutions use campus cards for student expenses such as books, food in snack bars, or campus fees. Jon Gear, vice president of JSA, said the company has no intention of forcing institutions to discontinue their funds-transfer systems. The company, he said, is simply enforcing a patent that protects its intellectual property. Gear said JSA contacted a number of schools, though he declined to say how many or to name them, and will negotiate licensing fees, which he said would be "negligible." Lowell Adkins, executive director of the National Association of Campus Card Users, said his organization is working to clarify the issue. "It's still really unclear what the scope of the patent is," he said. "We need to understand how they're going to exercise their rights."

Category 4B2 *Patents*

2006-04-06 **Electronic Frontier Foundation EFF US Patent and Trademark Office online test-taking patent intellectual property rights**

EDUPAGE; http://chronicle.com/daily/2006/04/2006040601t.htm 23

EFF CALLS FOR PATENT TO BE INVALIDATED

The Electronic Frontier Foundation (EFF) has called on the U.S. Patent and Trademark Office (USPTO) to invalidate a patent that broadly covers technologies that allow tests to be posted and taken online. In 2003, the USPTO granted the patent to Test.com, which has since contacted a number of colleges and universities, as well as businesses, that conduct online testing, saying those services violate the patent. Many of those approached by Test.com believe that the idea of putting tests on the Web is too obvious to warrant a patent. Now, the EFF says it has evidence that, even if the idea justifies a patent, Test.com was not the first to develop the technology to make it happen. According to the EFF, the IntraLearn Software Corporation began selling products with online testing capabilities in 1997, two years before Test.com applied for its patent. Jason Schultz, staff lawyer for the EFF, said that the USPTO would address the validity of the patent, which could take as long as a year or more. If the office determines that a patent is appropriate, said Schultz, it will "a tiny insignificant patent" rather than the very broad patent granted to Test.com.

4B3 Reverse engineering

Category 4B3 *Reverse engineering*

2000-03-16 **Internet content filtering censorware reverse engineering hacking civil lawsuit restraining order**

AP, NewsScan, USA Today 20 85
http://www.usatoday.com/life/cyber/tech/cth570.htm; RISKS

Microsystems Software Inc. (Framingham, MA) filed a civil lawsuit in mid March 2000 against two software experts who reverse engineered their Cyber Patrol software. Eddy L. O. Jansson (thought to live in Sweden) and Matthew Skala (a graduate student in computer science at University of Victoria in British Columbia, Canada) posted a utility called "cphack" on the Web to allow kids to determine their parents' password for the program's administration functions and thus bypass Cyber Patrol filters. The software was instantly posted around the world, making it impossible to stop the spread of the anti-censorware regardless of what the authors do.

Bear Giles, a frequent and always lucid commentator in RISKS, wrote that the entire question of encrypting the blacklists should be examined. Are these lists of forbidden sites concealed to protect children? Against what? "[H]ow would knowing that a site is on the blacklist permit a kid to access the blocked site? How many kids have the technical knowledge to edit the blacklist?" Giles asked whether such lists are encrypted as an anticompetitive measure and to prevent users and analysts from determining the rate of false positives (exclusion of sites on spurious grounds).

A federal judge in Boston . . . [ordered] a halt to distribution of the "cphack" software created by two computer hackers by reverse-engineering the commercially distributed "Cyber Patrol" program that allows parents to shield their children from pornography on the Internet. The judge's order also applies to any mirror Web sites where the program has been made available. Peter Junger, a law professor and free speech advocate, calls the ruling "a rather horrifying challenge to people's right to write software" and to figure out how it works by taking it apart and examining it. (USA Today 17 Mar 2000)

Category 4B3 *Reverse engineering*

2000-03-24 **Internet content filtering censorware reverse engineering hacking civil lawsuit restraining order subpoena court documents e-mail forgery delivery reliability**

NewsScan

In the MicroSystems case against two hackers who reverse-engineered that company's "Cyber Patrol" filtering software in order to create a "cphack" program to thwart its effectiveness, MicroSystems attorney Irvin B. Schwartz prevailed on U.S. District Judge Edward Harrington to allow him to send e-mail copies of the restraining order to anyone who is distributing a copy of cphack. Schwartz says, "It makes sense. You want to put people who might conceivably be in violation of a court order that they're on notice... It provides a medium to serve the court's order at Internet speed as opposed to snail mail or even worse, by courier." But Wired magazine columnist Declan McCullagh charges that the e-mails are "subpoena spam" and says: "E-mail is easy to forge. I can't even be certain it really did come from a real lawyer." (AP/San Jose Mercury News 24 Mar 2000)

http://www.sjmercury.com/svtech/news/breaking/merc/docs/079231.htm

---

Category 4B3 *Reverse engineering*

2000-03-28 **Internet content filtering censorware reverse engineering hacking civil lawsuit restraining order copyright**

POLITECH, Wired

The Mattel suit trying to stop distribution of cphack moved to the next stage on March 28, 200 when Judge Edward Harrington of the US District Court in Boston ruled that all mirror sites must remove copies of cphack or face legal consequences. In an interesting twist, Mattel declared in court that it now owned the copyright for cphack and therefore could control its distribution. However, Declan McCullagh pointed out that the original software was released under the GNU General Public License, apparently permitting anyone to distribute the code for free regardless of later copyright claims.

In early April, the ACLU filed suit for a stay of Judge Harrington's order while they appealed his ruling.

Category 4B3 *Reverse engineering*

2000-04-15 **legislation software license back door denial of service DoS**

Crypto-gram http://www.counterpane.com/crypto-gram-0004.html 00 04

Bruce Schneier of Counterpane Internet Security < http://www.counterpane.com/index.html> analyzed the disastrous Uniform Computer Information Transactions Act (UCITA) which was signed into law in Virginia and Maryland. Specifically, he pointed out that the Act allows software makers to include a back door so they can remotely disable software if users fail to abide by the terms of their license. As Schneier wrote, "The naive conceit here is that only the manufacturer will ever know this disable code, and that hackers will never figure the codes out and post them on the Internet. This is, of course, ridiculous. Such tools will be written and will be disseminated. Once these tools are, it will be easy for malicious hackers to disable peoples' computers, just for fun. This kind of hacking will make Back Orifice look mild." As for using public-key cryptography to ensure that only authorized instructions could be effective, Schneier commented that such assurances would depend upon perfect implementation of cryptography; however, "Given the industry's track record at implementing cryptography, I don't have high hopes."

Category 4B3 *Reverse engineering*

2000-10-20 **intellectual property lawsuit ruling copy protection fair use reverse engineering Digital Millennium Act copyright**

NewsScan

With a decision that represents a defeat for universities, libraries, and computer programmers but pleases media companies such as Sony and Time Warner, the U.S. Copyright Office . . . endorsed a provision of a new federal law making it illegal to use "reverse engineering" to learn how to evade the technological safeguards protecting copyrighted material. The provision in question is part of the 1998 Digital Millennium Act, and Congress had asked the Copyright Office to review it before it took effect. Academic and research institutions had argued that the restriction against reverse engineering was counter to the spirit of the "fair use" principle that allows limited kinds of free use to copyrighted materials under certain, specified conditions. (New York Times 30 Oct 2000) http://www.nytimes.com/2000/10/30/technology/30LIBE.html

---

Category 4B3 *Reverse engineering*

2000-11-26 **regulation software reverse engineering contract law**

Computer Professionals for Social Responsibility
http://www.cpsr.org/program/UCITA/ucita-fact.html

The Computer Professionals for Social Responsibility (CPSR) published a fact sheet about the Uniform Computer Information Transactions Act (UCITA) < http://www.cpsr.org/program/UCITA/ucita-fact.html >. Among other resources, the fact sheet includes a useful link that keeps track of developments in state legislatures. Another useful resource is the July 1999 essay by Cem Kaner and David Pels at < http://www.badsoftware.com/kaneropd.htm >.

Category 4B3 *Reverse engineering*

2001-01-24 **standards corruption sabotage lawsuit settlement ntellectual property reverse engineering license contract**

NewsScan

SUN CLAIMS VICTORY OVER MICROSOFT IN JAVA DISPUTE
Microsoft yesterday agreed to settle a long-running legal dispute with Sun Microsystems over Sun's Java programming language and related software development tools. Under the terms of the settlement, Microsoft will pay Sun $20 million and accept Sun's termination of its prior Java licensing agreement. In addition, Microsoft will relinquish use of the Java trademark. The lawsuit, originally filed in 1997, alleged that Microsoft had modified Java in order to optimize its performance with the Windows operating system. Microsoft said it decided to settle in order to avoid "costly litigation" and left open the possibility that it might now proceed to develop its own, independent version of Java. Meanwhile, Sun CEO Scott McNealy called the settlement "a victory for our licensees and consumers. The [software development] community wants one Java technology. This agreement further protects the authenticity and value of Sun's Java technology." (Financial Times 24 Jan 2001)
http://news.ft.com/news/industries/infotechnology

Category 4B3 *Reverse engineering*

2001-06-07 **reverse engineering intellectual property contract copyright research vulnerability weakness encryption watermarking steganography**

NewsScan

RECORDING INDUSTRY THREATENS RESEARCHER WITH LAWSUIT [24 Apr 2001]
The litigation department of the Recording Industry Association of America (RIAA) has threatened legal action against a Princeton University computer scientist if he and his colleagues give a conference presentation this week explaining how to get around a system developed by the industry to protect copyrighted music. The researcher, Dr. Edward W. Felton, works in the field of steganography, which develops techniques such as digital watermarking. The head of RIAA's litigation department insists: "There is a line that can get crossed, and if you go further than academic pursuit needs to go, you've crossed the line and it's bad for our entire community, not just for artists and content holders, it's everyone who loves art, and it's also bad for the scientific community." (New York Times 24 Apr 2001)
http://www.nytimes.com/2001/04/24/technology/24MUSI.html

COMPUTER RESEARCHERS YIELD TO THREAT OF LITIGATION [27 Apr 2001]
A group of computer scientists at Princeton and Rice universities has decided to withdraw an academic paper that was to be presented at a conference this week, because the Recording Industry Association of America said that public presentation of the work would violate the Digital Millennium Copyright Act of 1998, because it would describe how to evade the systems used to protect copyrighted music. Princeton computer scientist Edward W. Felton explained the group's decision by saying: "Litigation is costly, time-consuming, and uncertain, regardless of the merits of the other side's case. We remain committed to free speech and to the value of scientific debate to our country and the world." John McHugh of Software Engineering Institute at Carnegie Mellon University commented: "This was an excellent technical paper. This was pure and simple intimidation. This paper didn't do anything that a bright technical person couldn't easily reproduce." (New York Times 27 Apr 2001)
http://www.nytimes.com/2001/04/27/technology/27MUSI.html

COURT CASE TESTS ACADEMIC FREEDOM AND COPYRIGHT LAW [7 Jun 2001]
Princeton University computer scientist Edward W. Felton and colleagues at Princeton, Rice and Xerox, have asked a federal court for a declaratory judgment that would overturn a part of the 1998 Digital Millennium Copyright Act. The scientists say that the DMCA has constrained them from presenting their research results because the recording industry said the research, if made public, would undermine the industry's antipiracy technology, used to protect content on compact disks. Dr. Felton says that what is needed is "a broad principle that scientific investigation and publication is okay, that discussion of these technologies is okay. Publication is how scientists communicate with each other." (New York Times 7 Jun 2001)
http://www.nytimes.com/2001/06/07/technology/07CODE.html

Category 4B3 *Reverse engineering*

2001-11-05 **music piracy peer-to-peer encryption DMCA Digital Millennium Copyright Act lawsuits**

NewsScan

AIMSTER VS. RECORDING INDUSTRY [21 May 2001]
The recording industry may be hoist on its own petard if the Napster-like music swapping service called Aimster is successful in its legal strategy against the Recording Industry Association of America (RIAA). Unlike Napster, Aimster (which has no central servers to maintain and leaves users individually responsible for their actions) encrypts transmissions, and so there is no way for the RIAA or any other outside party to distinguish between files which are in compliance with copyright law and those that infringe on it. Of course, RIAA could simply decrypt the files -- but then it would be in violation of the Digital Millennium Copyright Act (DMCA), a law that it strongly supports, and that makes it a criminal offense to circumvent encryption protection of copyrighted material. (The New Republic 21 May 2001)
http://www.tnr.com/cyberlaw/babbitt051101.html

NOW IT'S AIMSTER'S TURN [25 May 2001]
"This is Napster all over again": Five major record companies, of which four are represented by the Recording Industry Association of America (RIAA), have filed a lawsuit against the Internet service Aimster, charging it with allowing users to illegally exchange copyrighted music. But Aimster insists that, unlike Napster, it's "not a music sharing service" but a service that delivers private messages and files (music or any other kinds of files) and is not authorized to examine the content of those communications. (New York Times 25 May 2001)
http://www.nytimes.com/2001/05/25/technology/25MUSI.html

AIMSTER TARGETED BY NEW LAWSUIT [5 Jul 2001]
Aimster, already being sued for copyright infringement by a long list of recording companies, is now being sued by the National Music Publishers Association (NMPA), whose chief executive says: "We are extremely disappointed that before the ink was even dry on Ninth Circuit Court of Appeals' opinion concluding that Napster was engaging in massive copyright infringement, another Internet music service would seek with impunity to supplant Napster and expect to get away with it." But the Aimster's chief executive charges that the publishers are in collision with the recording industry, and says that Aimster is quite different from Aimster. He insists that Aimster is not a music-swapping service like Napster, but rather an instant messaging system that, coincidentally, allows files of all kinds to be swapped confidentially through member "buddy lists." (Reuters/USA Today 5 Jul 2001)
http://www.usatoday.com/life/cyber/tech/2001-07-05-aimster.htm

NAPSTER ALTERNATIVE USE UP 20% [5 Nov 2001]
The use of Napster-like peer-to-peer music file-sharing sites like Kazaa, MusicCity and Grokster rose 20% during the month of October, signaling U.S. Internet users' insatiable demand for digital music and video downloads. All three sites use software licensed from FastTrack, an Amsterdam-based technology company, and share the same network. "The growth of the FastTrack network continues to be astounding," says a Webnoize analyst. "During the last four months the number of users typically logged on has risen by 480%, and in November will likely surpass the 1.57 million simultaneous users that Napster... enjoyed at its peak... As higher awareness translates into higher usage, the FastTrack network may ultimately become many times larger than Napster ever was." Meanwhile, a recent Jupiter Media Metrix survey shows that song-swapping has declined in Europe over the same period. According to the report, music downloads are down by 50% in Europe since February, the point at which Napster usage hit its zenith. (Reuters 5 Nov 2001)
http://news.excite.com/news/r/011105/14/net-tech-webnoize-dc

Category 4B3 *Reverse engineering*

2001-11-07 **copyright reverse engineering remote control lawsuit robot dog**

NewsScan

SONY TELLS AIBO HACKER "NO NEW TRICKS" [7 Nov 2001]
Sony has demanded that the owner of a Web site that distributes free software for enhancing the smarts of the cuddly robot pets, remove the software from its site on pain of prosecution for copyright infringement and altering its product without a license. The software could be used to teach Aibo new tricks, such as disco dance steps and additional vocabulary. "This is a legal issue," said a Sony Entertainment spokesman. "We don't support the development of software by manipulating the existing Aibo software code -- hacking it." The company's action has irked Aibo owners, who usually spend hundreds of dollars on software from Sony, and were thrilled to get the free enhancements. (AP 7 Nov 2001)
http://news.excite.com/news/ap/011107/14/sony-robot-hack

Category 4B3 *Reverse engineering*

2001-12-14 **Digital Millennium Copyright Act DMCA reverse engineering decryption electronic book copyright protection intellectual property lawsuit prosecution arrest**

NewsScan

CRYPTOGRAPHER ARRESTED FOR VIOLATING DIGITAL COPYRIGHT LAW [18 Jul 2001]
Law enforcement officials have arrested Dmitri Sklyarov, a 27-year-old Russian graduate student at Moscow State Technical University, on charges of unauthorized copying of digitized material that he obtained breaking the electronic book encryption code developed by Adobe Systems. Accused of violating the Digital Millennium Copyright Act of 1998, he will face up to five years in jail and a $500,000 fine if he is found guilty. (New York Times 18 Jul 2001)
http://partners.nytimes.com/2001/07/18/technology/18CRYP.html

IN DIGITAL AGE, SECURITY ISSUES PLAY LARGE ROLE [23 Jul 2001]
The Electronic Frontier Foundation, a civil liberties group, is helping to underwrite challenges against the Digital Millennium Copyright Act (DMCA) of 1998, which was used last week as grounds for arresting an encryption expert accused of violating its restrictions on circumventing security schemes for protecting electronic books. One critic of the law says, "It's distressing that if someone writes software they say is secure and you prove them wrong, you can go to jail." Those opposed to the DMCA argue that by allowing copyright-holders to protect their work by encryption and making it a crime to break that encryption, the law is taking away the "Fair Use" exceptions that have always allowed people to copy portions of copyrighted works for purposes such as scholarship, criticism, or parody. (New York Times 23 Jul 2001)
http://www.nytimes.com/2001/07/23/technology/23DIGI.html

ADOBE CHIMES IN, ASKS GOVERNMENT TO FREE DMITRY [24 Jul 2001]
Adobe Systems is asking the government to release Russian programmer Dmitry Skylarov, who was arrested last week in Las Vegas for violating the Digital Millennium Copyright Act (DMCA) by trafficking in code used to break the encryption used to protect Adobe's eBook Reader software. An international "Free Dmitry" movement has protested the government's action, which was taken at Adobe's urging. Adobe now says that although it strongly supports the DMCA and the enforcement of copyright protection of digital content, it believes that " the prosecution of this individual in this particular case is not conducive to the best interests of any of the parties involved or the industry." A lawyer for the Electronic Frontier Foundation, a civil liberties advocacy group, said: "We explained to Adobe, imagine how you would feel if one of your programmers was visiting in Russia and was arrested for making software that was considered illegal there? It sort of hit home with them that what they are doing here isn't right." However, a government attorney prosecuting the case says: "This is a criminal case brought by the United States against the defendant, and to that extent no one else is a party." (San Jose Mercury News 24 Jul 2001)
http://www.siliconvalley.com/docs/news/svfront/adobe072401.htm

"FREE DMITRY" PROTESTS CONTINUE [31 Jul 2001]
About a hundred protesters showed up yesterday in San Francisco to denounce the arrest of Russian programmer Dmitry Sklyarov, who the government has accused of violating the U.S. Digital Millennium Copyright Act (DMCA). The charge was based on Sklyarov's role in the development of software used to evade copyright protections used on Adobe eBook software. An attorney for the Electronic Freedom Foundation told the gathering of Sklyarov supporters that the long-standing "Fair Use" principle of copyright law "allows people to make use of things freely without the permission of the copyright holder." One protester said: "I'm interested in freedom of speech and trying to redress the balance between copyright holders to control information and the lack of the individual's right to challenge that." (Reuters/San Jose Mercury News 31 Jul 2001)
http://www.siliconvalley.com

BAIL FOR DMITRI [7 Aug 2001]
A federal district court in San Jose has released the 26-year-old Russian programmer and graduate student Dmitri Sklyarov on $50,000 bail. Arrested at a software conference in Las Vegas, he is charged with criminal violation of the Digital Millennium Copyright Act (DMCA) of 1998, and faces up to five years in prison and a half-million dollar fine for promoting a software product that evades the encryption algorithms used by Adobe Systems to protect e-books. Sklyarov is viewed by many as a martyr for the cause of freedom of information, and his lawyer says: "If there are constitutional questions out there, we're certainly going to be raising them. I see this as being an intellectual fight to the death. Either the criminal provisions of the DMCA are going to be killed, or we're in a position where some civil liberties are going to be killed." (New York Times 7 Aug 2001)
http://partners.nytimes.com/2001/08/07/technology/07HACK.html

DID DMITRI VIOLATE RUSSIAN LAW? NYET! [9 Aug 2001]
The Russian official responsible for fighting high-tech crimes in that country says that programmer Dmitri Sklyarov, arrested in Las Vegas for violating U.S. digital copyright laws, broke no Russian laws. "If this case was being reviewed in Russia, we would have nothing against Dmitri Sklyarov. No crime falling under current Russian law has been committed." Sklyarov, now out on $50,000 bail, is charged with having violated the 1998 Digital Millennium Copyright Act (DMCA) by promoting software capable of evading the encryption used by Adobe's eBook Reader. Adobe has dropped its support of the case. (AP/San Jose Mercury News 9 Aug 2001)
http://www.siliconvalley.com/docs/news/svfront/075617.htm

WHAT IS DMITRI THINKING? [3 Aug 2001]
Here's what Dmitri Skyarov -- the 26-year-old Russian cryptographer arrested in Las Vegas for violating the Digital Millennium Copyright Act -- has this to say about what has happened to him: "If someone will allow me to choose not to be famous in this case, I would prefer not to be famous. I'm not company chief. I'm just a programmer." The programs he developed are written in Russia and violate no Russian laws. He's anxious to return to his wife and two children in Moscow, where his hope is "to be as independent as possible. It's very hard to have real dreams in Russia. All things change very fast, and you never know what will happen tomorrow." (San Jose Mercury News 13 Aug 2001)
http://www.siliconvalley.com/docs/news/svfront/sklyar081101.htm

RELEASE OF RUSSIAN PROGRAMMER [14 Dec 2001]
Dmitry Sklyarov, the 27-year-old Russian programmer arrested in the U.S. for violating the Digital Millennium Copyright Act (DMCA) by writing and promoting code that could be used to evade the copy-protection features of the Adobe Acrobat eBook Reader, is being released, but the U.S. government will continue its prosecution of his employer, ElcomSoft of Moscow. Skylarov's cause was embraced by a worldwide collection of programmers, scientists, free-speech advocates and civil libertarians who organized "Free Dmitry" rallies. (San Jose Mercury News 14 Dec 2001)
http://www.siliconvalley.com/docs/news/svfront/hacker121401.htm

---

Category 4B3 *Reverse engineering*

2002-04-22 **intellectual property law reverse engineering chilling effect research publication science scientists engineering engineers**

Security Wire Digest 4 31

In early 2002, the IEEE began requiring authors of papers submitted to its scholarly publications to affirm that they were complying with all US laws, including the Digital Millennium Copyright Act (DMCA). In April 2002, the professional society decided to remove reference to compliance with the DMCA because so many scientists have complained that complying with this controversial law makes their normal work impossible.

Category 4B3 *Reverse engineering*

2002-05-21 **copyright intellectual property reverse engineering DMCA prosecution trial**

FindLaw Download This 86

COPYRIGHT TRIAL SET FOR RUSSIAN
Associated Press

The first criminal trial under the Digital Millennium Copyright Act will begin Aug. 26, a federal judge decided Monday. ElcomSoft Co. Ltd. of Moscow could be fined $500,000 if convicted of selling a program that let users circumvent copyright protections on electronic-book software made by Adobe Systems Inc. Such programs are legal in Russia but banned under the 1998 Digital Millennium Copyright Act. Attorneys for the company failed this month to convince a judge that the law is too broad, vague and unconstitutional.

http://news.findlaw.com/ap/ht/1700/5-20-2002/20020520204501_09.html

The Prosecutors
http://www.usdoj.gov/usao/can/index-2.html

Category 4B3 *Reverse engineering*

2002-06-06 **reverse engineering encryption decryption**

Security Wire Digest 4 44

*STUDENT CRACKS XBOX, OPENS GAME CONSOLE TO OTHER OSES
With three weeks of work and $50 in hardware, a graduate student at the Massachusetts Institute of Technology cracked the security protections of Microsoft's Xbox, making it possible to run competing software and operating systems on the popular video game console. In a paper posted on MIT's Web site last weekend, Andrew Huang described how he build hardware that read the Xbox's internal security system and crack the encrypted data exchanged between two chips that prevented the console from being exploited. Huang says he technique gives users the ability to turn the Xbox into a standalone computer that can run non-Microsoft software and OSes, including rival Linux. Huang says he also discovered a series of other vulnerabilities that could allow users to run the code of their choice on the box and identify users when the Xbox is connected to the Internet.
http://web.mit.edu/bunnie/www/proj/anatak/AIM-2002-008.pdf

Category 4B3 *Reverse engineering*

2002-12-17 **jurisdiction prosecution intellectual property reverse engineering e-commerce electronic books DMCA fair use free speech**

Security Wire Digest 4 26

JUDGE UPHOLDS U.S.'S RIGHT TO PROSECUTE ELCOMSOFT
A federal judge in California has ruled the United States has jurisdiction to prosecute a Russian software company that last year marketed a program on the Internet that allowed pirating of electronic books. Lawyers this week asked the same judge to dismiss copyright infringement charges leveled against ElcomSoft last year under the Digital Millennium Copyright Act (DMCA) on grounds the DMCA is too far-reaching and unconstitutional. ElcomSoft created a product that breaks the copyright protections in Adobe Systems' eBook Reader. One of its programmers, Dmitry Sklyarov, was arrested in July after speaking about the tool at the DefCon hacker conference in Las Vegas. In February, Sklyarov entered a plea-bargain deal, admitting to five DMCA violations. ElcomSoft argues the DMCA doesn't clearly define tools considered illegal, making all technologies suspect. This, they argued, violates fair-use and free speech rights. Prosecutors maintain the 1998 copyright law is broad, but clear on prohibiting tools that circumvent copyright protection controls.

RUSSIAN FIRM CLEARED IN U.S. COPYRIGHT CASE
ElcomSoft Co. Ltd., based in Moscow, has been found not guilty of criminal charges that it violated the 1998 U.S. Digital Millennium Copyright Act by selling a software program designed to circumvent the digital locks used to enforce copyright protections on Adobe Systems e-book software. The two-week trial was the first criminal prosecution under the controversial DCMA, which prohibits the sale of technology that can be used to break the code that "locks" digitally formatted movies, music and other software. The case hinged on whether ElcomSoft had "willfully" violated U.S. law, an intent the defendants denied. "They never intended to violate the law," said defense attorney Joseph Burton. ElcomSoft president Alexander Katalov pointed out that the program was legal in Russia and was not meant to be used for electronic books that had not been legally purchased. He said he didn't know that the software was illegal under U.S. law. (Reuters 17 Dec 2002)

Category 4B3 *Reverse engineering*

2003-01-06 **reverse engineering copyright infringement copy protection DVD**

NewsScan

SUPREME COURT BACKS OFF ON DVD DESCRAMBLING CODE
The U.S. Supreme Court has rescinded an emergency stay barring defendant Matthew Pavlovich from distributing DeCSS, a software utility that descrambles the digital lock on most DVDs to prevent copying them. Pavlovich is now free to distribute the code, but could be sued again if he decides to do so. "The entertainment companies need to stop pretending that DeCSS is a secret," says Cindy Cohn, legal director for the Electronic Frontier Foundation, which is assisting Pavlovich. "Justice O'Connor correctly saw that there was no need for emergency relief to keep DeCSS a secret. It doesn't pass the giggle test." The rescission is just the latest twist in a case that has been winding its way through the courts since 1999, when the DVD Copy Control Association — a coalition of movie studios and consumer electronics makers — filed a lawsuit against scores of people, alleging violations of California's trade secret laws. (CNet News.com 3 Jan 2003)
http://news.com.com/2100-1023-979197.html

Category 4B3 *Reverse engineering*

2003-04-09 **digital copyright act defended ACLU Harvard student reverse engineer**

NewsScan

JUDGE DISMISSES CHALLENGE TO DIGITAL COPYRIGHT ACT
U.S. District Judge Richard Stearns has dismissed a lawsuit by the American Civil Liberties Union on behalf of a Harvard student who sought proprietary information from software company N2H2 so that he could reverse-engineer its software filtering product. The student and the ACLU had argued that software filters violate constitutional free speech protections because such filters unintentionally block far more than just pornography, and thereby deny people access to information to which they have a right. But Judge Stearns ruled that "there is no plausible protected constitutional interest that Edelman can assert that outweighs N2H2's right to protect its copyrighted material from an invasive and destructive trespass." (AP/USA Today 9 Apr 2003)

Category 4B3 *Reverse engineering*

2003-04-16 **Digital Millenium Copyright Act Super DMCA privacy anonymizing restrictions bill law legislation offshore**

NIPC/DHS

April 14, SecurityFocus — 'Super-DMCA' fears suppress security research.

University of Michigan graduate student Niels Provos who is noted for his research into steganography and honeypots — techniques for concealing messages and detecting hackers, respectively — says he's been forced to move his research papers and software offshore and prohibit U.S. residents from accessing it, in response to a controversial new state law. At issue are the so-called "Super-DMCA" (Digital Millennium Copyright Act) bills under consideration in seven states, which have already become law in six others. The state measures appear to target those who would steal pay-per-view cable television shows or defraud broadband providers. The Michigan law, which took effect on March 31st, typifies the legislation: Among other things, residents of the Great Lakes State can no longer knowingly "assemble, develop, manufacture, possess, deliver, offer to deliver, or advertise" any device or software that conceals "the existence or place of origin or destination of any telecommunications service." It's also a crime to provide written instructions on creating such a device or program. Violators face up to four years in prison. Taken literally, the law would target businesses like Anonymizer.com and Hushmail — both services cater to privacy-conscious Internet users determined to conceal their place of origin from marketers, or to communicate anonymously. Critics say it would also ban firewalls and NAT boxes, dealing a blow to Internet security.

Category 4B3 *Reverse engineering*

2003-05-13 **DMCA copy protection Digital Millennim Copyright Act ACM Association Computing Machinery hackers ckrack security systems patents copyright**

NIPC/DHS

May 13, SecurityFocus — Security research exemption to DMCA considered.

Computer security researchers would be allowed to hack through copy protection schemes under a proposed exception to the Digital Millennium Copyright Act (DMCA) being debated in official hearings this week. The DMCA's anti-circumvention provision generally makes it unlawful for anyone to "circumvent a technological measure that effectively controls access" to DVD movies, digital music, electronic books, computer programs, or any other copyrighted work. However, the Association for Computing Machinery (ACM) would like an exemption permitting white hat hackers to crack copy protection schemes "that fail to permit access to recognize shortcomings in security systems, to defend patents and copyrights, to discover and fix dangerous bugs in code, or to conduct forms of desired educational activities."

Category 4B3 *Reverse engineering*

2003-09-16 **dmca verizon provacy information personal music piracy indentity**

NewsScan

CHALLENGE TO DMCA; 'TOO SOON TO CHANGE THE LAW' SAYS HATCH
Verizon is challenging the constitutionality of the subpoenas forcing Verizon to turn over names and addresses for at least four Internet subscribers. The Digital Millennium Copyright Act of 1998 permits music companies and others to force Internet providers to turn over the names of suspected pirates upon subpoena from any U.S. District Court clerk's office (and a judge's signature is not required). Sen. Orrin Hatch (R-Utah), chairman of the Senate Judiciary Committee, has said that it's too early to consider changing the 1998 law. "These issues have not ripened enough. I don't think we can yet determine if these subpoenas are being used responsibly to identify alleged infringers... As we start to hear more voices protesting the impact of these subpoenas, there may be more of a chance to reconsider their impact." (AP/San Jose Mercury News 16 Sep 2003)

Category 4B3 *Reverse engineering*

2004-10-04 **reverse engineering genome algorithms protocols computer science**

NewsScan; http://www.wired.com/news/infostructure/0

REVERSE ENGINEERING TAKES A LESSON FROM THE GENOME PROJECT

There's a lot more in common between reverse-engineering software and the algorithms used in bioinformatics research than you would expect, says security analyst Marshall Beddoe. In both cases, scientists must fill in a lot of blanks -- much of bioinformatics is devoted to finding DNA sequences separated by long gaps of unknown data, and the same is true in protocol reverse-engineering. Scientists attempting to reverse engineer software protocols find that network conversations are full of "junk" -- usually the actual data being sent -- which interferes with the analysis of the of the command sequences. Beddoe solved the problem by using bioinformatics algorithms to eliminate the junk data sandwiched between commands. Meanwhile, Avaya senior security consultant Dan Kaminsky says he's investigating using genomic pattern analysis for identifying and clustering "mutant" machines on a corporate network. "Generating an ordered, hierarchical breakdown of interrelationships from huge piles of information is a problem that crops up everywhere. I'm not surprised to see bioinformatics solutions finally being applied to the rest of our poorly understood, oversized networks," says Kaminsky.

Category 4B3 *Reverse engineering*

2004-12-15 **iPod Apple RealNetworks Harmony music copy protection blocking information warfare reverse engineering**

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/10425219.htm

ANOTHER ROUND IN THE APPLE-VS.-REAL NETWORKS FIGHT

Apple has begun blocking the technology that RealNetworks created to evade the copy-protection shield used by Apple's iPod. When RealNetworks introduced its Harmony technology this summer, it hoped to dissolve some of the barriers created by incompatible, proprietary digital music standards, and said it had reverse-engineered Apple's copy-protection code to allow songs purchased from non-Apple online outlets to be playable on the iPod. To deal with Apple's new move, RealNetworks now says it "will look at the Apple upgrade and see how it'll make Harmony work once again with the iPod." (AP/San Jose Mercury News 15 Dec 2004)

Category 4B3 *Reverse engineering*

2005-12-29 **electronic voting machines legal challenges**

RISKS 24 14

DRUNKS MUST HAVE ACCESS TO BREATHALYZER INNARDS BUT VOTERS MUST TRUST E-VOTING MACHINES

Tanner Andrews pointed out the irony of US state law, in which drunk drivers have been ruled to have full access to the internals of breath-analysis devices used by police whereas voters have no legal right to examine the internals of electronic voting machines.

Category 4B3 *Reverse engineering*

2006-01-05 **Electronic Frontier Foundation EFF computer security researchers protection reverse engineering DMCA violation**

EDUPAGE; http://www.internetnews.com/security/article.php/3575441 23

EFF SEEKS PROTECTION FOR COMPUTER RESEARCHERS

The Electronic Frontier Foundation (EFF) has called on Sony EMI to pledge not to pursue prosecution of computer researchers who investigate the security of the company's products. Last fall, the company was caught in a public outcry over technology included in music CDs. The technology installed itself on users' computers and scanned them for potentially illegal activities. The company has removed those tools from CDs, but security researchers believe they have reason to reverse engineer copy protections on EMI CDs, a practice which would violate not only the Digital Millennium Copyright Act but also EMI's end user license agreement. Fred von Lohmann, senior staff attorney with EFF, said, "When it comes to computer security, it pays to have as many independent experts kick the tires as possible, and that can only happen if EMI assures those experts that they won't be sued for their trouble."

Category 4B3 *Reverse engineering*

2006-04-14 **EFF Digital Millennium Copyright Act DMCA consequences list piracy anti-piracy**

EDUPAGE; http://www.internetnews.com/bus-news/article.php/3599026 23

EFF LISTS CONSEQUENCES OF DMCA

The Electronic Frontier Foundation (EFF) has issued a report detailing what it said are the unintended effects of the Digital Millennium Copyright Act (DMCA). The law was enacted seven years ago to address intellectual property issues that arose with the development of the Internet and other technologies. Among other provisions, the law includes a prohibition on circumventing antipiracy measures, even if such circumvention was done for reasons that reasonable people would see as legitimate, according to the EFF. In a number of cases, the DMCA has been invoked to suppress information obtained by researchers about security weaknesses. The EFF's report said that the law has been used not so much to limit piracy as to "threaten and sue legitimate consumers, scientists, publishers, and competitors." The Cato Institute recently released a report on the DMCA with similar findings.

Category 4B3 *Reverse engineering*

2006-04-24 **DMCA Digital Millennium Copyright Act revisions law bill restrictions proposal**

RISKS; CNET news.com http://tinyurl.com/k5ebw 24 26

CONGRESS PROPOSING TO STRENGTHEN DMCA

For the last few years, a coalition of technology companies, academics and computer programmers has been trying to persuade Congress to scale back the Digital Millennium Copyright Act.

Now Congress is preparing to do precisely the opposite. A proposed copyright law seen by CNET News.com would expand the DMCA's restrictions on software that can bypass copy protections and grant federal police more wiretapping and enforcement powers.

The draft legislation, created by the Bush administration and backed by Rep. Lamar Smith, already enjoys the support of large copyright holders such as the Recording Industry Association of America. Smith, a Texas Republican, is the chairman of the U.S. House of Representatives subcommittee that oversees intellectual property law.

[Excerpt by Declan McCullagh for RISKS]

4B4 EULA (End-user license agreements)

Category 4B4 *EULA (End-user license agreements)*

2001-03-30 **copyright e-mail Web office software .NET intellectual property appropriation theft contract**

RISKS 21 32

RISKS correspondent Michael Sinz reported on astounding claims in the end-user license agreement (EULA) for .NET and HailStorm PassPort services. He summarized the situation as follows: "If you send source code or business plans or a chapter of your first novel or anything else of any value (or of no value), Microsoft has the right to use, exploit, and sublicense any and or all of it without any payment to the copyright holder. It also has the right to any trademark, service mark, or patent that you might use in such communications or documents that are used/stored/transmitted via their service!" Mr Sinz bolstered his reaction with quotations from the LICENSE TO MICROSOFT section of the EULA for the Passport site, which included the following text:

"By posting messages, uploading files, inputting data, submitting any feedback or suggestions, or engaging in any other form of communication with or through the Passport Web Site, you warrant and represent that you own or otherwise control the rights necessary to do so and you are granting Microsoft and its affiliated companies permission to:

1. Use, modify, copy, distribute, transmit, publicly display, publicly perform, reproduce, publish, sublicense, create derivative works from, transfer, or sell any such communication.

2. Sublicense to third parties the unrestricted right to exercise any of the foregoing rights granted with respect to the communication.

3. Publish your name in connection with any such communication.

The foregoing grants shall include the right to exploit any proprietary rights in such communication, including but not limited to rights under copyright, trademark, service mark or patent laws under any relevant jurisdiction. No compensation will be paid with respect to Microsoft's use of the materials contained within such communication. Microsoft is under no obligation to post or use any materials you may provide and may remove such materials at any time in Microsoft's sole discretion."

Category 4B4 *EULA (End-user license agreements)*

2001-07-13 **contract law end-user license agreement EULA**

NewsScan

USER AGREEMENTS REQUIRE USER CONSENT
A federal judge in New York has ruled that individuals who downloaded free software from Netscape's Web site are not bound by a "conditions of use" statement they hadn't read. The reason? The site had not required them to take positive action -- prior to the download -- to show they agreed to Netscape's conditions. A lawyer who represented the plaintiffs against Netscape praised the court's decision: "It applies an ancient and fundamental principle in a novel context. That is, you can't be bound to that which you don't agree to." (New York Times 13 Jul 2001)
http://www.nytimes.com/2001/07/13/technology/13CYBERLAW.html

Category 4B4 *EULA (End-user license agreements)*

2001-09-21 **UCITA EULA end-user license agreement**

RISKS 21 68

Alistair McDonald noted in RISKS that "the latest MS Front Page licence agreement prevents you from any anti-microsoft Web content with it." The quoted text from the EULA is "You may not use the Software in connection with any site that disparages Microsoft, MSN, MSNBC, Expedia, or their products or services . . . ."

http://slashdot.org/article.pl?sid=01/09/20/1443226 reports that

---

Category 4B4 *EULA (End-user license agreements)*

2002-02-08 **end-user license agreement EULA lawsuit antivirus censorship contract**

NewsScan

SOFTWARE REVIEW PROHIBITION CHALLENGED BY LAWSUIT [8 Feb 2002]
The State of New York is suing Network Associates, a company that makes McAfee Virus Scan and other software products, over a Network Associates prohibition which specifies: "The customer will not publish reviews of this product without prior consent from Network Associates Inc." New York says that the company is guilty of censoring consumers in order to shield itself "from criticism and commentary that is the essence of the free market." Network Associates argues that its use of the restriction is nothing more than an attempt by the firm to exercise its right "to set the terms of its license," which is a matter between the consumer and the company. In its response to the lawsuit, the company has also explained that its only motivation for the restriction was to make sure that customers did not publish reviews of outdated versions of products. (New York Times 8 Feb 2002)
http://partners.nytimes.com/2002/02/08/technology/08VIRU.html

4B5 Trademarks

Category 4B5 *Trademarks*

2001-12-20 **trademark infringement lawsuit emulator monopoly**

NewsScan

MICROSOFT SUES LINDOWS FOR TRADEMARK INFRINGEMENT [20 Dec 2001]
Microsoft has sued a small startup called Lindows, charging that the name infringes on its Windows trademark. Lindows software is based on the Linux operating system and is capable of running programs made for Windows. "The similarity between the Lindows and Windows marks is likely to lead consumers to mistakenly conclude that the Lindows product was exclusively or jointly developed by, licensed or certified by, or otherwise sponsored or approved by Microsoft," said the software giant in its complaint. Microsoft is hoping to settle the dispute out of court, says a company spokesman. (Reuters 20 Dec 2001)
http://www1.excite.com/home/technology/tech_article/0,2109,196677|technology!12-20-2001::19:45|reuters,00.html

---

Category 4B5 *Trademarks*

2002-04-05 **intellectual property trademark proper name parody satire humor complaint**

NewsScan

CAN FALWELL'S NAME BE TRADEMARKED TO PROTECT HIM AGAINST PARODY?
The Reverend Jerry Falwell has lodged a complaint with the World Intellectual Property Organization (WIPO) charging that a Web site that parodies him is violating his "common-law" trademark of his name. The operator of the parody Web site says Falwell's name is not entitled to trademark protection because he hasn't used it for the purpose of identifying goods and services. WIPO is headquartered in Geneva, Switzerland. (AP/San Jose Mercury News 4 Apr 2002)
http://www.siliconvalley.com/mld/siliconvalley/3000509.htm

Category 4B5 *Trademarks*

2002-12-30 **trademark infringement lawsuit**

NewsScan

WINDOWS, LINDOWS: WHAT'S IN A NAME? A LAWSUIT
When a company focused on the Linux operating system named itself Lindows, Microsoft got mad and sued, charging that the new company had infringed on Microsoft's trademark ownership of the term Windows. Nonsense, said Lindows, and sued back, challenging the legality of that trademark. An attorney representing Lindows maintains that "no company, no matter how powerful, no matter how much money it has spent, should be able to gain a commercial monopoly on words in the English language." Funny he should mention money. Microsoft's response is that Lindows should not be allowed a "free ride on the investments we have made in building Windows into one of the most recognizable brands in the world over the last 20 years." The dispute will be decided in a Seattle courtroom in the spring. (New York Times 30 Dec 2002)

Category 4B5 *Trademarks*

2004-06-22 **Apple loses trademark appeal China logo clothing hats shoes**

NewsScan

APPLE LOSES APPEAL AGAINST TRADEMARK PANEL DECISION

Apple has lost a court appeal against a decision that rejected its request to have its trademark logo extended to cover clothing and other items in China. The verdict by the Beijing No.1 Intermediate People's Court means that Apple cannot claim that its logo is protected under law for those goods. The trademark appraisal committee of China's State Administration for Industry and Commerce had previously rejected Apple's application from April 2000 to have its trademark logo extended to cover clothing, hats and shoes. Guangdong Apples Industrial Co, a Chinese maker of leather goods, had registered a similar trademark with an entire apple, while Apple Computer's
trademark has an apple with a bite taken out of it. (The Age 22 Jun 2004)

Category 4B5 *Trademarks*

2004-07-19 **Lindows Microsoft Windowd trademark copyright out-of-court settlement**

NewsScan

LINDOWS INSPIRED TO CHANGE ITS NAME FOR $20 MILLION

Microsoft has settled its trademark infringement lawsuits against Lindows with a $20 million payment to that Linux operating system company -- which will now change its name to Linspire. Microsoft says, "We are pleased that Lindows will now compete in the market place with a name distinctly its own." Lindows has four years to continue using two of its Web addresses ‹ www.lindows.com and www.lindowsinc.com › for the purpose of redirecting visitors to its new Web sites. (AP/USA Today 19 Jul 2004)

Category 4B5 *Trademarks*

2004-08-15 **USPS personalized individualized stamps Stamps.com order**

NewsScan

USPS AUTHORIZES INDIVIDUALIZED STAMPS

The U.S. Postal Service has put its stamp of approval on Stamps.com's plans to test a new service (www.photo.stamps.com) that enables users to design their own legally valid stamps using digitized photos of their pets, children or almost anything else that strikes their fancy. (Stamps.com says
it will screen each photo submission to weed out objectionable material such as nudity, obscenity, politics, violence and trademark infringements.) The personalized stamps don't come cheap -- at $16.99 for a minimum order of 20 37-cent stamps they cost 85 cents apiece -- but Stamps.com CEO Ken McBride reports that more than 2,000 sheets of personal stamps were ordered in the first two days and he anticipates the trial will win approval from the USPS and will be extended. (Washington Post 15 Aug 2004)

Category 4B5 *Trademarks*

2004-12-15 **Geico Google law dismissed trademark search engines advertising paid links**

NewsScan; http://www.nytimes.com/2004/12/15/technology/15cnd-google.html?oref=login

GEICO CASE AGAINST GOOGLE DISMISSED BY JUDGE

A federal district court judge in Virginia has dismissed a key claim in the trademark infringement suit brought against Google by Geico, the auto insurance company. Geico had argued that the Google practice that allows Geico's competitors to buy ads linked to searches for "Geico" and "Geico Direct" confuses Web surfers who are looking specifically for Geico, but the judge ruled that there was not enough evidence the Google practice actually confuses consumers. One intellectual property attorney not involved in the case predicts: "It will not be binding precedent. That's how cases get to the Supreme Court."(New York Times 15 Dec 2004)

4C Security paradigms, risk management, site-security certification, professional certification

Category 4C *Security paradigms, risk management, site-security certification, professional cer*

1997-08-05 **security awareness UK certification**

Universal News Services

The British Department of Trade and Industry, the U.K. Accredited Certification Service, and the British Standards Institution are developing a new Code of Practice for Information Security Management (BS 7799). To achieve this level of certification, organizations will have to implement minimal standards of security. This new certification scheme would be complementary to the ICSA's Web Certification program.

Category 4C *Security paradigms, risk management, site-security certification, professional cer*

1997-09-06 **infowar critical infrastructure**

AP

The President's Commission on Critical Infrastructure Protection continued its work as its October deadline for a final report drew nearer. Chairman Robert T. Marsh emphasized that although there have been no disasters due to attacks on the American infrastructure, it is important to prevent any such damage. He specifically named the Internet as an increasingly vital component of the infrastructure.

Category 4C *Security paradigms, risk management, site-security certification, professional cer*

1998-01-04 **NIST NSA certification Orange Book TCSEC Common Criteria**

Federal Computer Week

The National Security Agency (NSA) and the National Institute of Standards and Technology (NIST) announced their intention to accredit commercial laboratories for evaluation and certification of information security products. Using the Common Criteria instead of the outdated criteria of the TCSEC (Trusted Computer Security Evaluation Criteria, or "Orange Book"), the NIST-based laboratory will concentrate on developing a network of commercial facilities where vendors could have their products certified for use in government applications and, by extension, in the commercial sphere as well.

Category 4C *Security paradigms, risk management, site-security certification, professional cer*

1998-01-05 **cyberstalkers hate pedophiles cults safety Internet Web**

C|Net http://www.news.com/News/Item/Textonly/0,25,12590,00.html?pfv

CNET published an excellent resource page for information on threats to security in cyberspace. The article, a special feature written by several CNET staff writers, included information about cyberstalkers, hatemongers, child predators, cultists, and kooks with many hot links for further study and action. See <http://www.news.com/News/Item/Textonly/0,25,12590,00.html?pfv>.

Category 4C *Security paradigms, risk management, site-security certification, professional cer*

1998-03-09 **deception defense hacker scanner probe**

RISKS 19 62

Fred Cohen invented The Deception ToolKit to send false information back to hackers who probe a system, thus helping to waste the attackers' time and discourage their depredations. See <http://all.net/dtk/dtk.html> for an overview and the latest version.

Category 4C *Security paradigms, risk management, site-security certification, professional cer*

1998-04-09 **Web security book advice reference guide help**

RISKS 19 66

Rob Slade gave top marks to a new Web security book*, writing in RISKS, "The writing is clear and accurate, giving the reader both concepts and practical tasks in minimum time with maximum comprehension. Although the bulk of the book is for Webmasters, the casual user can not only read it but get a great deal of value from it. Any ISP that does not have it on their customer support bookshelf should held criminally negligent."

* Stein, L. D. (1998). Web Security: A Step-by-Step Reference Guide. Addison-Wesley (Don Mills, ON). ISBN 0-201-62489-9. 448 pp.

Category 4C *Security paradigms, risk management, site-security certification, professional cer*

1998-04-26 **insurance virus hacking penetration e-commerce**

EDUPAGE

Several companies, including the famous Lloyds of London, announced insurance policies to cover some of the measurable costs of computer intrusions, sabotage and malicious code.

Category 4C *Security paradigms, risk management, site-security certification, professional cer*

1998-05-16 **penetration testing tiger team**

RISKS 19 74

After a macro-virus infection reportedly interfered with NASA communications with the MIR space station, NASA asked the DoD Tiger Team to test for vulnerabilities in its computer networks.

Category 4C *Security paradigms, risk management, site-security certification, professional cer*

1998-06-15 **TruSecure insurance guarantee evaluation standards Internet**

Reuters

ICSA's inclusion of up to $250,000 in penalties from successful penetration for certified sites subscribing to the TruSecure service caused quite a reaction in the industry. Some commentators expressed disbelief, but others were positive about the initiative.

Category 4C *Security paradigms, risk management, site-security certification, professional cer*

1998-07-05 **WebTrust certification business privacy encryption**

EDUPAGE

CPA WebTrust, a new certification of proper business practice for Web sites, was announced by the American Institute of Certified Public Accountants. The seal is a mark of verified business integrity, proper notification of how personal data are to be used, and assurance that comunications between browser and server are encrypted.

Category 4C *Security paradigms, risk management, site-security certification, professional cer*

1998-08-06 **theft laptop costs insurance**

EDUPAGE

Safeware Insurance Agency (Columbus, OH), a firm specializing in insuring firms against, among other dangers, the loss of laptop computers, reported a 28% jump (to about $1B) in the amount of claims for stolen laptops since 1996. It was unclear from the news summaries whether this increase represented a rise in the risk per computer or merely an overall increase in the absolute number and value of claims as the number of clients rose.

Category 4C *Security paradigms, risk management, site-security certification, professional cer*

1998-08-13 **password cracking UNIX DES brute force**

RISKS 19 91

Chiaki Ishikawa pointed out in RISKS that the availability of the Deep Crack parallel-processing array implies that UNIX password files are no longer secure. Peter Neumann added, "RISKS readers must be tired of my saying that fixed reusable passwords are a menace, irrespectively of how long they are, how full of funny characters, how often they are changed (of course, sniffing catches all changes), how they are managed, etc. It is time to retire them."

Category 4C *Security paradigms, risk management, site-security certification, professional cer*

1998-10-29 **criminal hackers employees inside threat vulnerability**

BBC http://news.bbc.co.uk/hi/english/sci/tech/newsid_203000/203547.stm

Stephen Cobb was the keynote speaker at the conference organized in London by Diligence Information Security in October. The BBC reported that "ethical" hacking has been increasing in popularity as security experts test the strength of barriers to unauthorized access.

Category 4C *Security paradigms, risk management, site-security certification, professional cer*

1998-10-29 **e-mail policy privacy monitoring audit trail log supervision**

http://www.internet-magazine.co.uk/news/oct/29d.htm

In Britain, a survey of 50 large businesses suggested that although about 40% can monitor their employees' e-mail, only 18% of the total can register their e-mail destinations.

Category 4C *Security paradigms, risk management, site-security certification, professional cer*

1998-10-30 **international computer crime law enforcement police network**

Rule of Law Foundation

The United Nations Expert Group Meeting on Computer Crime selected the World Justice Information Network to distribute information worldwide to law enforcement officials in the fight against cybercrime. For more information, see <http://www.justinfo.net>.

Category 4C *Security paradigms, risk management, site-security certification, professional cer*

1998-10-30 **e-mail archives retention policy shredding destroy delete**

Inter@ctive Week Online
http://www.zdnet.com/zdnn/stories/zdnn_rc_display2/0,3733,2157779,00.html

Tom Steinert-Threlkeld wrote an interesting column in Inter@ctive Week urging companies to delete e-mail rather than archiving everything. He pointed out how the Microsoft trial was being influenced by the availability of archived e-mail.

Category 4C *Security paradigms, risk management, site-security certification, professional cer*

1998-11-05 **security architecture standard**

CNN DigitalJam http://cnnfn.com/digitaljam/wires/9811/05/ibm_wg/

IBM and Intel announced an industry-wide effort to build a common framework for interoperability of security products. The Common Data Security Architecture (CDSA) should provide for security products that could run on a wide variety of platforms and operating systems.

Category 4C *Security paradigms, risk management, site-security certification, professional cer*

1999-01-05 **computer emergency response team CERT**

South China Morning Post

The Hong Kong Internet Service Providers Association (HKISPA) and the Hong Kong Productivity Council (HKPC) began seeking government funding to create a local branch of the Computer Emergency Response Team (CERT).

Category 4C *Security paradigms, risk management, site-security certification, professional cer*

1999-02-12 **text book overview introduction paradigm model management**

RISKS 20 21

Rob Slade reviewed Donn B. Parker's new (1998) book, _Fighting Computer Crime_ (John Wiley & Sons, ISBN 0-471-16378-3). He wrote, "Parker's stance on security in general definitely puts him in the camp of the professional paranoids. However, absent the first and last chapters, there is a lot of good, solid knowledge here to help educate any security practitioner."

Category 4C *Security paradigms, risk management, site-security certification, professional cer*

1999-02-20 **site-security certification information warfare consultants**

National Post (Canada)

James Adams of IDefense Corp (Washington, DC) announced a site-security certification seal. He said, "We are Dun & Bradstreet meets the CIA meets the stamp of Good Housekeeping approval. We the only one in the world like it. There will be others but that's okay. Competition is good." [Yes, especially since the TruSecure seal from ICSA.net was on the market in 1998.]

Category 4C *Security paradigms, risk management, site-security certification, professional cer*

1999-04-24 **certification standards Internet perimeter scan**

BSI PR

In April, the British Standards Institute announced the release of a new version of its successful BS 7799 standards and of the C:CURE security certification scheme. The update cost £94 (£47 to BSI members), and could be ordered from BSI Customer Services, 389 Chiswick High Road, London W4 4AL, England. Phone: 0181 996 9001, fax: 0181 996 7001, email: <info@bsi.org.uk>, website: <www.bsi.org.uk>. The C:CURE certification scheme information was available from BSI DISC, 389 Chiswick High Road, London W4 4AL, England. Phone: 0181 996 7799, fax: 0181 996 6411, email: <c-cure@bsi.org.uk>, website: <www.c-cure.org>.

Category 4C *Security paradigms, risk management, site-security certification, professional cer*

1999-04-26 **theft law enforcement deterrence detection forensics**

JOURNAL OF COMMERCE

Computer crime and theft of high-tech components cost a lot not only to the victims but also to law enforcement agencies forced into expensive and lengthy investigations and court cases. The San Jose Police Department decided to use a bit of outreach in a bid to reduce vulnerability to high-tech crime. A four-person squad operates a computer forensics laboratory that helps in investigations of all sorts where computer data are part of the evidence; the members also visit local industries to point out vulnerabilities and encourage tighter physical and computer security. The officers encourage insurers to push prevention as an important tool: "We don't have all the answers," Lieut. Stephen Ronco, commander of the unit, said. "But if underwriters can go back to their respective clients and simply ask them, how are you preventing such crimes, are your inventory audits tight, do you have security measures and other anti-theft policies in place to give guidance to supervisors and employees, it would help enormously."

Category 4C *Security paradigms, risk management, site-security certification, professional cer*

1999-04-29 **vulnerability analysis certification BS7799**

Accountancy Age (UK)

Accountancy Age (UK) published an interesting article on the value of security standards such as the newly revised BS 7799 and independent vulnerability assessments such as the British Standards Institute's C:CURE in April. Experts insisted that security policy is a necessary prerequisite for any kind of certification and that policy is not a "techie" issue but a business management issue.

Category 4C *Security paradigms, risk management, site-security certification, professional cer*

1999-05-06 **information warfare critical infrastructure certification**

Computing (UK)

In Britain, national security officials suggested that experts from the private sector ought to help protect the critical infrastructure of the UK. In August, the Communications Electronic Security Group (CESG) security agency launched a security audit called "IT Health Check." Companies approved by CESG and the Defence Evaluation Research Agency (DERA) would test computers and networks in the private sector for vulnerabilities and then provide recommendations for improvements.

Category 4C *Security paradigms, risk management, site-security certification, professional cer*

1999-07-20 **telecommuting data communications encryption authentication digital signatures**

Washington Post

If Rep. Frank Wolf's (R-VA) proposed bill encouraging telecommuting were to become law, companies would earn pollution credits for the person-miles eliminated by allowing workers to stay at home while doing their jobs. These credits would be traded openly. In addition, if the 40% of 133M workers who could do their jobs from home offices did stay there, businesses could save millions in reduced office leasing, maintenance, heating, air-conditioning and lighting costs. [Yes, and if this actually does happen, we had better have really good security in place to protect data communications from breaches of confidentiality, integrity and authenticity. Virtual private networks and digital signatures, anyone?]

Category 4C *Security paradigms, risk management, site-security certification, professional cer*

1999-10-01 **cybercops cyberpolice investigators**

Wall Street Journal

Dean Takahashi of the Wall Street Journal wrote an interesting and laudatory article about Dave Kennedy and his IS/RECON team, who scour the Net looking for criminal hacker activity. Full-time operatives also infiltrate criminal hacker groups and warn potential victims of pending attacks whenever possible.

Category 4C *Security paradigms, risk management, site-security certification, professional cer*

1999-10-02 **bank financial systems security network alerts warnings sharing cooperation private**

AP

The US banking industry responded to President Clinton's demand for improved resistance to fraud in the financial sector. The Financial Services Information Sharing and Analysis Center was announced by the Treasury Department; its physical location was secret. The network will facilitate information sharing with full anonymity. According to Ted Bridis, writing for Associated Press, "Similar centers are planned in the coming months for seven other industries, including telecommunications, oil and gas, electrical power, transportation and America's water supply system."

Category 4C *Security paradigms, risk management, site-security certification, professional cer*

1999-10-05 **security-enabled e-business SEE Entrust paradigm encryption keys banks**

Entrust http://www.entrust.com/news/1999/09_21_99.htm, American Banker

Entrust Technologies Inc.'s President and CEO, John Ryan, published a white paper on "security-enabled e-commerce" <http://www.entrust.com/downloads/see.htm>. The paper recommends that security be integrated into the business planning cycle for Internet-based commerce and provides a good management overview of some of the technical means for assuring security while enhancing competitive position and profitability.

Category 4C *Security paradigms, risk management, site-security certification, professional cer*

1999-10-11 **e-commerce security alliance group industry consortium**

New York Times

In October, Compaq Computer, Hewlett-Packard, IBM, Intel and Microsoft formed the Trusted Computing Platform Alliance to develop universal security standards for e-commerce and to improve the security of personal computers.

Category 4C *Security paradigms, risk management, site-security certification, professional cer*

1999-10-15 **taxonomy classification terminology vulnerabilities database**

http://www.mitre.org/news/articles_99/cve_release.shtml

MITRE Corporation announced the Common Vulnerabilities and Exposures (CVE) database, in which over 300 vulnerabilities are cross-indexed so that security experts and security-product developers can figure out which vulnerabilities and exposures they are talking about.

Category 4C *Security paradigms, risk management, site-security certification, professional cer*

1999-10-18 **conference data sharing information pooling computer crime defense vulnerability database**

San Jose Mercury News Online

At the 22nd National Information Systems Security Conference organized in Arlington, VA by the NIST (National Institute of Standards and Technology) and the NCSC (National Computer Security Center), panelists urged industry and government to pool knowledge about security threats and vulnerabilities to strengthen the Good Guys' hands against computer criminals.

Category 4C *Security paradigms, risk management, site-security certification, professional cer*

2006-04-27 **law legislation Georgia USA private investigator forensic specialist licensing**

RISKS; The Register 24 27
http://www.theregister.co.uk/2006/04/26/law_change_for_pis

GEORGIA LAW REQUIRES LICENSING FOR DIGITAL FORENSICS SPECIALISTS?

Some computer professionals will need to get a Private Investigator license just to continue doing their computer work. I imagine this will also apply to accountants and auditors, in fact anyone who analyses data that is on computer systems, on behalf of some other company, and perhaps people who work at software houses, computer retailers, whoever does repairs to computers, installations of new stuff. We will have to be asking suppliers of firewall, anti-virus, anti-spam, anti-spyware etc. if they have a PI license, otherwise it might be illegal to buy their products, and if there are no such suppliers, then it may be illegal to be protected against the cyber-criminals.

Companies will need to get an opinion from their lawyers, with respect to filing annual reports with the state and with government regulators. We are supposed to swear this data is correct under penalty of perjury, but it was derived by accounting and computer experts, not Private Investigators, but now it is illegal to get such data from people who are not Private Investigators? Does this also mean that Police Department personnel need to get a PI license before they may testify in court?

[Summary and analysis by Al Macintyre]

4C1 Paradigms, security standards

Category 4C1 *Paradigms, security standards*

2000-05-11 **software quality assurance QA liability pressure**

NewsScan

In testimony provided to the Congressional subcommittee holding hearings on the love bug virus, noted computer security expert Peter G. Neumann of SRI International warned that the software industry is not doing what it should to keep the Internet safe: "Vastly many more people are now relying on the Internet, and most of them are oblivious to the risks... Overall, the situation is grave. The commercial marketplace is not leading. The government is not exerting enough driving forces. This is a really ridiculous predicament, and would be a very bad joke if it were not so serious... Until software developers and system purveyors are liable for the failures of their products, there will be no real motivation to develop robust systems... The mass-marketplace is overly concerned with features; it tends to be long on fancy features and to ignore critical requirements such as rudimentary robustness. However, robust features can be achieved with good design and good programming practice, rather than the business-as-usual practices of sloppy development and a rush-to-market mentality. If automobiles were recalled as often as computer system flaws are detected, we would still have horses and buggies." (New York Times 11 May 2000)

Category 4C1 *Paradigms, security standards*

2000-07-17 **web of trust confidence paradigm system ratings vulnerabilities**

NewsScan, Wall Street Journal
http://interactive.wsj.com/articles/SB963786024674216913.htm

With cyberfraud proliferating at Internet speed, the question of trust on the Internet is prompting some netizens to develop new systems known as "reputation managers" that attempt to "computerize" a trust function for wary Web surfers. One of the most sophisticated examples is Epinions.com, which solicits and compiles people's reviews of a variety of products and services. As you read the writeups, you tell Epinions which were most "trustworthy" and helpful, and the next time you return, Epinions prioritizes them based on who has earned your trust. The Google search engine works on a similar system, with each Web page in its database ranked by how many other sites link to it. Each link is counted as a "vote" for the trustworthiness of that site. In contrast, eBay's feedback system, in which every buyer who successfully completes a transaction gets to rate the seller, is fraught with potential for fraud. Jakob Nielsen, a Web design specialist who studies reputation systems, says "The eBay system actually works perfectly if everyone is completely honest. But if you can put in your own rating, it falls apart." (Wall Street Journal 17 2000)

Category 4C1 *Paradigms, security standards*

2000-09-25 **policy punishment unexpected consequences zeal overreaction incident response**

RISKS, Christian Science Monitor 21 07
http://www.christiansciencemonitor.com/durable/2000/09/26/fp2s2-csm.shtml

In the wake of the prosecution of Wen Ho Lee, staff at the Los Alamos National Laboratory of the U.S. Department of Energy became wary of reporting any security violations. This is an example of the law of unintended consequences and illustrates the foolishness of using punishment as the sole mechanism for encouraging secure behavior.

Category 4C1 *Paradigms, security standards*

2000-12-06 **conference paradigm social relations trust community**

NewsScan;http://www.code.uni-wuppertal.de/uk/trust/welcome.html

Dr. Mihai Nadin, professor of computational design at the University of Wuppertal in Germany says, "Our age is characterized by shorter cycles of innovation, faster processes, decentralization, and discontinuity. Permanence is at best a nostalgic desideratum connected to a past that for certain intervals had an appearance of stability. Our time is one of instability, higher speeds, and a human scale of pragmatic activity that has reached globality. Behind these loaded words is the simple realization, by each and every one of us, of a state of flux. After all is said and done: Is trust still possible today?" To answer that question, the University of Wuppertal will convene an international colloquium on "TRUST" on 16-17 January 2001.

Category 4C1 *Paradigms, security standards*

2000-12-12 **security alerts publication details Web link URL controversy discussion debate completeness**

RISKS 21 16

Chris Adams summarized a debate over new, more limited forms of bug alerts. Some companies, including Microsoft, are publishing their alerts with much less technical information and referring interested readers to their Web site for full details. Adams criticized this practice, arguing that (quoting him verbatim):
* Access for people with marginal Internet connections or browsers other than IE/Netscape is less convenient.
* Information is unavailable if the Web server is down or overloaded, as might happen with an important advisory. It seems counterproductive to put important, time-sensitive material behind a single point of failure, particularly when the decision is to deliberately avoid using a free distributed, fault-tolerant distribution channel.
* It makes it much easier for a vendor to change an advisory without notifying anyone, especially since changed or removed advisories won't be archived in anywhere near as many places as a mailing list such as BUGTRAQ. In addition to covering up bad work, this would also make it easier to remove or tone-down past advisories about companies the author is now aligned with.
* It opens the prospect of tailoring content to the reader. This could be as simple (and annoying) as charging for access to some content or as complex as determining what to show based on where the request came from (e.g. competitors, vendors or journalists). While this would probably be caught for something major, particularly at first, it would not surprise me to find at least subtle tampering happening regularly if this becomes commonplace.

In a follow-up posting, a report by Richard M. Smith on BUGTRAQ stated that the new Microsoft security bulletins include Web bugs, presumably to track how many people read the bulletins.

Category 4C1 *Paradigms, security standards*

2001-07-22 **privacy risk management false positives power of a test suspicion reporting law enforcement police notification postal service**

RISKS 21 54

Alan Wexelblat noted in RISKS a report by "Insight Magazine . . . [1] that since 1997, the US Postal Service has been reporting innocent activity it deems 'suspicious' to federal law enforcement officials. Evidence includes a training video with this chilling instruction: 'It's better to report 10 legal transactions than to let one illegal transaction get by.'

The risks of a system that presumes guilt until innocence is proven are too numerous to list here. Not least of them is the impossibility of proving a negative (I did not intend this cash to be used for illegal purposes). A similar reporting system in the banking arena is known to generate ratio of 99,999 false positives for every true positive. Yes, I do mean a ratio of 10^5:1 errors to correct results. I can't imagine any other system in which that error rate would be acceptable.

The information on suspicious activities is, of course, kept in a database controlled in secret and used for purposes no one is willing to discuss. The Post Office will not discuss the parameters used to flag 'suspicious' activity, though the video states that unwillingness to give out personal information such as date of birth and/or produce identification papers is automatically suspicious.

Someone help me verify that I'm still living in America, please?

[1] http://www.moreprivacy.com/editorials/postaleye.htm"

Category 4C1 *Paradigms, security standards*

2002-05-21 **anonymizer bug quality assurance QA policy**

NewsScan; FindLaw Download This 86

TRYING TO DENY SECURITY FLAWS 'IS ALWAYS THE WRONG ANSWER' The Web site Anonymizer.com, which offers a service that protects people's anonymity when they use the Internet, has acknowledged that it has had to fix several security flaws that had been identified by a friendly user, Bennett Haselton. Anonymizer president Lance Cottrell says that Haselton "came up with a new way of exploiting standards. They're pretty subtle." The company has awarded Haselton a prize for his effort, which is given to anyone who can find security holes in the Anonymizer service. "We are always actively soliciting people to attack it. Trying to hide and keeping your head down is always the wrong answer." (AP/San Jose Mercury News 21 May 2002)
http://www.siliconvalley.com/mld/siliconvalley/3306644.htm

SECURITY HOLES IN WEB PRIVACY PROGRAM
A popular Internet privacy service that lets Web surfers visit sites anonymously has fixed several serious flaws, and now the service's founder is offering a reward to the finder of the bugs. Bennett Haselton, an Internet filtering activist who runs the Peacefire Web site, found the problems with Anonymizer.com, a five-year-old service that shields users from tracking by Web sites and their Internet providers. . . Many major commercial sites cringe when security researchers find a hole. But Anonymizer actually encourages it through a "bug bounty."
http://news.findlaw.com/ap/ht/1700/5-21-2002/20020521004501_09.html

---

Category 4C1 *Paradigms, security standards*

2002-06-06 **security by obscurity open-source software homeland critical infrastructure protection**

Security Wire Digest 4 44

Edited version of an excerpt from Cheryl Balian's report in Security Wire Digest:

>A white paper released in June 2002 by the Alexis de Toqueville Institution (ADTI) in Washington, D.C., says that open-source software is inherently less secure and more likely to exploited by terrorists and other wrongdoers than closed-source, proprietary software.

The report, "Opening the Open Source Debate," suggests that the federal government's adoption of open-source software could compromise the safety of U.S. air traffic, e-commerce and surveillance systems. In a statement, ADTI says, "Terrorists trying to hack or disrupt U.S. computer networks might find it easier if the federal government attempts to switch to 'open source' as some groups propose."<

The ADTI's contention was met with incredulity by the security community, which cited Kerkhoff's principle that the security of a system should not reside in its obscurity.

Category 4C1 *Paradigms, security standards*

2003-01-31 **worm vulnerability analysis homeland defense infrastructure protection network vulnerabilities management**

NewsScan

SAFE & SOUND IN THE CYBER AGE: INTERNET GRAND SLAM
Could your company survive without the Internet? This is not a rhetorical question. In the wake of last weekend's "Slammer" attack, corporations may have to contemplate getting by without the Internet. That sounds like hyperbole until realize how much trouble was caused by just 376 bytes of worm code. The basic facts have been widely reported. Late last Friday, or early Saturday in Asia, a worm was released onto the Internet targeting a vulnerability in Microsoft Corp's SQL Server 2000. Activity generated by the worm's probing for systems to infect brought Internet traffic to its knees, at least in parts of Asia. Weekend Web surfers in North America experienced everything from momentary delays to complete lack of access. American Express customers couldn't check their accounts online. Web operations were paralyzed for two days at Countrywide, the country's biggest residential mortgage provider. The Atlanta Journal-Constitution couldn't print Sunday's first edition on time. Some 911 emergency services were forced to revert to manual dispatching. On top of that, some weekend shoppers found their Bank of America cash cards couldn't produce "cash back" at supermarkets. For some, even plain old cash at ATM machines was unavailable.

A lot of technical staff at companies that rely on SQL Server and related code spent the weekend at work, removing the worm from infected systems and patching them to prevent reinfection. Even so, some employees couldn't get to their data on Monday morning, including some employees at Microsoft itself. An internal memo, issued over the weekend and leaked to the press on Tuesday, made it clear that Microsoft had failed to apply to many of its own systems the very patches it had urged customers to install to avoid this problem in the first place.

Unfortunately, all the talk about Microsoft and SQL Server has tended to obscure two of the scariest parts of the story:
1. Our society is a lot more dependent on the Internet and "immature" systems than anyone has so far been prepared to admit.
2. The Internet exists at the whim of those who know how to destroy it.
In this column and the next we will address these points in the above order, starting with the issue of dependency.

Over the last few months, Bank of America has spent millions of dollars on a television advertising campaign touting the ubiquity of its ATM machines. Imagine that you just switched your account to Bank of America because of those ads, only to find that access to your money is denied, by 376 bytes of rogue computer code released onto the Internet. In our admittedly unscientific sampling of consumer opinion at the coffee shop we found universal disbelief that such a thing could happen. Sadly, it comes as no surprise to us. As security experts, we have made it our business to know a lot about network infrastructure (after all, that's where a lot of data is most vulnerable). People who know more than we do about that infrastructure have been warning us for years about excessive inter-dependencies, lack of redundancy, single points of failure, and so on (they have also pointed out that 90% of all military communications are handled by commercial carriers, but that's another column). There have also been plenty of warnings about excessive reliance on immature code, i.e. software which is not deployed through a production process that includes thorough pre-production testing and a proper maintenance cycle (companies that had installed the patches for SQL Server before the weekend were not infected, although they may still have been affected by the traffic overload which the worm created). Now the public has very concrete proof that the experts were right.

Now we know we cannot rely on our bank to provide 24/7 access to our money. Hopefully, companies will now set about beefing up their networks, providing redundant channels and managing their code (funded by some of the huge costs savings they reaped by shifting data and voice from private lines to the Internet). Fortunately, the advice of network experts can also help the consumer. Redundancy is the best strategy to avoid being denied access to your cash by an ATM system failure. Just make sure you have debit card accounts at more than one bank!

In the next column we will explain why we think the Internet exists at the whim of those who know how to destroy it.

[Chey Cobb, the author of "Network Security for Dummies," is an independent consultant (www.cheycobb.com) and a former senior technical security advisor to the NRO. Her email address, chey@patriot.net, is heavily spam-filtered... Stephen Cobb, the author of "Privacy for Business: Web Sites and Email," is Senior VP of Research and Education for ePrivacy Group (www.eprivacygroup.com). He can be reached at scobb@cobb.com.]

Category 4C1 *Paradigms, security standards*

2003-03-03 **Department of Defense DoD security policy release update information assurance controls standards**

NIPC/DHS

February 27, Government Computer News — DoD releases second half of security policy.

Directive 8500.2, an information assurance policy that sets specific controls and standards for how users should secure Department of Defense (DoD) networks, was released by the Pentagon on Thursday. While 8500.1, which was released last October, supplied a framework for DoD to follow to protect its information systems, 8500.2 tells users how to secure their networks, said Robert F. Lentz, director of information assurance for the Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence. The 8500.2 policy instructs Defense agency leaders to provide security training to all military and civilian personnel, including contractors, that meets an employee's job level of responsibility for working with DoD information systems. The policy establishes information assurance (IA) managers and officers to ensure that DoD systems meet IA specifications. According to 8500.2, information transmitted on Defense networks is shared across the Global Information Grid and is becoming more vulnerable to attacks and denial of service. The vulnerabilities stem from "increased reliance on commercial information technology and services; increased complexity and risk propagation through interconnection; the extremely rapid pace of technological change; a distributed and nonstandard management structure; and the relatively low cost of entry for adversaries."

Category 4C1 *Paradigms, security standards*

2003-03-26 **security specifications standards base requirements**

NIPC/DHS

March 24, eWEEK — Security specs in the works.

The CEO Cybersecurity Task Force by the end of this year will release a set of network security best practices for enterprises to adopt as a minimum standard. The task force plans to challenge executives to have their companies meet these base-line requirements by a certain date, which has yet to be determined. The hope is that peer pressure and a walk-before-you-run approach will entice laggard enterprises into shoring up their security. The task force, formed last week, is a subset of TechNet- a national organization of technology industry CEOs, somewhat akin to a lobbying group, that works with legislators to help shape policy. In addition to developing the base-line security guidelines, the task force plans to work with government security officials to develop an efficient, workable plan for public and private information sharing of attack and threat data. This is a hot topic both in Washington and in Silicon Valley, where corporate IT staffs see little to gain by divulging such sensitive data.

Category 4C1 *Paradigms, security standards*

2003-04-09 **corporate security single entity holistic**

NIPC/DHS

April 07, Computerworld — Handle corporate security as single entity, users say.

Companies can improve their ability to detect and respond to both cyber and physical threats by tying their IT security to other aspects of corporate security. But the cultural and business-process changes involved in implementing such a holistic view of security can be daunting for most corporations, users said here last week at a conference organized by ASIS International, an organization of security professionals. Lew Wagner of the MD Anderson Cancer Center at the University of Texas in Houston, said coordinating IT security functions with areas such as physical protection, facilities management, human resources and legal and audit functions has helped enhance overall threat-detection and incident-response capabilities at the hospital. A holistic view of enterprise security can help plug gaps that might otherwise be missed, said James Litchko, of Litchko & Associates Inc., a security consultancy in Kensington, MD. For instance, the majority of IT-related security threats still stem from procedural and process flaws-such as failure to secure access to crucial systems, inadequate backups and lack of auditing-rather than from technology glitches, Litchko said.

Category 4C1 *Paradigms, security standards*

2003-04-09 **cyber terrorism cyberspace attack Australia risk threat open door**

NIPC/DHS

April 08, Next — Australia leaves the hack door open to cyber sabotage.

Australia's critical information infrastructure is at risk because of the Federal Government's focus on physical infrastructure and terrorism, the head of Australia's Computer Emergency Response Team (AusCERT) says. AusCERT general manager Graham Ingram says that Malaysia, South Korea and Japan are spending enormous amounts of money on protecting information infrastructure - things such as government, banking, public utility, telecommunications and emergency networks. In Australia, many of these assets are in private hands. AusCERT has been contracted by the Federal Government to provide a free service to the general public and business about new threats to networked computer systems as part of the Trusted Information Sharing Network (TISN). TISN is a voluntary forum for owners of critical infrastructure to exchange information on security issues announced last November. But Kate Lundy, IT spokeswoman for Australia's Labor Party, says laws are needed to force the private sector to comply with minimum standards of protection for critical information infrastructure.

Category 4C1 *Paradigms, security standards*

2003-04-18 **Federal Information Processing Standard FIPS crypto cryptography international Canada Britain UK**

NIPC/DHS

April 15, Government Computer News — FIPS-140 gains international acceptance.

The Federal Information Processing Standard for cryptographic modules, FIPS-140, has become the de facto international standard for cryptography, with 300 products validated by independent laboratories. It is moving toward becoming an official international standard as well. In October, the International Standards Organization began considering a proposal to make FIPS-140-2 an international standard, and Britain in November accepted it as the standard for protecting personal information submitted to the government. The National Institute of Standards and Technology (NIST) and its Canadian equivalent, the Communications Security Establishment, jointly run the validation program, which certifies product compliance with FIPS-140-2. "I have heard that many states are recognizing FIPS-140," said Ray Snouffer, manager of NIST's Security Management and Testing Group. The standard is also required by many private-sector organizations, including banks in Europe and U.S. companies such as Visa International Service Association and Boeing Co. But the United Kingdom is the first country other than the United States to adopt the standard.

Category 4C1 *Paradigms, security standards*

2003-04-28 **Peter Neuman software testing quality assurance manufacturer reponsibility**

NewsScan

SOFTWARE MAKERS DON'T DO ENOUGH TESTING, SAYS NEUMANN
Peter Neumann, principal scientist at SRI International's Computer Science Laboratory in Menlo Park, California, says that most software is released without undergoing a sufficient amount of testing, and adds: "The idea that we depend on something that's inherently untrustworthy is very frightening." Last year a study commissioned by the National Institute of Standards and Technology found that software errors cost the U.S. economy about $59.5 billion a year, or 0.6% of the country's entire GDP. Should software makers be held responsible for shoddy code? Barbara Simmons, former president of the Association for Computing Machinery, thinks they certainly should: "Software is being treated in a way that no other consumer products are. We all know that you can't produce 100% bug-free software. But to go to the other extreme and say that software makers should have no liability whatsoever strikes me as absurd." (AP/USA Today 28 Apr 2003)

Category 4C1 *Paradigms, security standards*

2003-05-16 **NIST National Institute Standards Technology FISMA FIPS security risk categorize national confidentiality integrity availability information**

NIPC/DHS

May 16, Federal Computer Week — NIST releases draft security standard.

The National Institute of Standards and Technology's (NIST) Computer Security Division Friday released the draft of a new Federal Information Processing Standard, FIPS 199, which dictates how agencies should categorize their systems based on the security risk faced by each. The standard is the first step in several requirements generated by NIST under the Federal Information Security Management Act (FISMA) of 2002, all aimed at setting minimum security requirements for all government systems not related to national security. The draft outlines three categories of risk, which are based on the potential impact of a breach in three areas: the confidentiality, integrity and availability of the information in the system. Comments on the draft are due within 90 days. The draft is available on the NIST Website:
http://csrc.nist.gov/publications/drafts.html

Category 4C1 *Paradigms, security standards*

2003-07-25 **cybersecurity DoD COTs monoculture vulnerability**

NewsScan

CYBERSECURITY AT THE DEFENSE DEPARTMENT
Purdue University computer science professor Eugene Spafford says there is too much reliance in the Defense Department on off-the-shelf commercial software: "Most of those products are not written to be used in an environment where there is a significant threat. We have attacks being committed by hackers, by anarchists, by criminals, probably by foreign intelligence services. The products have not been designed to be reliable or robust under those kinds of circumstances." There's also a "near mono-culture" resulting from the use of common products across many different DOD systems: "When a new attack is found that has affected any one of these products, it seeps through the entire network. Operators of systems may be in the position of applying three to five security critical patches per week for every system under their control. That really is unacceptable for us to be in a state of high readiness." Microsoft chief security strategist Scott Charney offers an perspective on the issue: "Reasonable minds are debating whether a homogeneous environment or a heterogeneous environment is better for decreasing risk. The advantage of a homogeneous environment, or more of a mono-culture, is it's much easier to manage. You train your people in a particular system, and they manage that system, they know all the security settings, you run tools to make sure they lock it down." (IDG News/Infoworld 25 Jul 2003)

Category 4C1 *Paradigms, security standards*

2003-11-04 **NIST security control proposal standards federal information systems FIPS**

NIPC/DHS

November 03, Federal Computer Week — NIST releases security controls proposal.

The National Institute for Standards and Technology (NIST) released the first draft of a publication describing mandated security controls for federal information systems on Monday, November 3. NIST officials want agencies to experiment with the initial public draft, "Special Publication 800-53: Recommended Security Controls for Federal Information Systems." It outlines electronic and physical controls for systems categorized under three levels of potential impacts, such as what would happen if someone steals information from a federal system and modifies the data or disrupts a government service. NIST's Computer Security Division plans to use agencies' comments from the initial draft and an open workshop in March to develop final security controls that would become the new "FIPS 200: Minimum Security Controls for Federal Information Systems." FIPS 200 is required under the Federal Information Security Management Act of 2002. NIST expects to publish FIPS 200 in the fall of 2005, when its controls will become mandatory for all federal agencies.

Category 4C1 *Paradigms, security standards*

2003-11-06 **microsoft virus writers reward anti-virus money program information arrest**

NewsScan

MICROSOFT PUTS A PRICE ON THE HEADS OF VIRUS WRITERS
Microsoft is using an old-fashioned tactic to fight new-fangled viruses — it's created a $5-million Anti-Virus Reward Program and is offering $250,000 bounties for information leading to the arrest and conviction of the people behind last summer's Blaster worm and Sobig virus. Together, those attacks are blamed for $2 billion in losses by businesses and consumers, according to consulting firm Computer Economics Inc. Security experts are split on whether the new initiative will prove successful, but Microsoft senior security strategist Philip Reitinger says, "What we hope to accomplish is to give people an incentive to do the right thing." (Los Angeles Times 6 Nov 2003)

Category 4C1 *Paradigms, security standards*

2003-11-18 **NIST security guidelines posted draft federal information systems protection**

NIPC/DHS

November 14, Government Computer News — NIST posts security control guidelines for comment.

The National Institute of Standards and Technology (NIST) released an initial public draft of recommended security controls for federal information systems Thursday, November 13. The guidelines for mandatory controls are expected to go into effect in two years. The Special Publication 800-53 was drafted under the Federal Information Security Management Act. SP 800-53 is one of seven NIST publications to be completed over the next two years as a security framework. Federal Information Processing Standard Publication 200, "Minimum Security Controls for Federal Information Systems," will replace SP800-53 in late 2005 and will be mandatory for government systems not involved in national security. Controls include management, operational and technical safeguards and countermeasures that ensure the confidentiality, integrity and availability of government systems. The current 238-page report is preliminary and covers only guidelines for low and moderate security baselines. NIST's Computer Security Division will accept comments on the initial draft of SP 800-53 until January 31, 2004. The draft is available online:
http://csrc.nist.gov/publications/drafts.html

Category 4C1 *Paradigms, security standards*

2003-11-25 **worms msblast slammer code red carnegie mellon software information systems security**

NewsScan

NEW STUDY TARGETS IT MONOCULTURE
The National Science Foundation is funding two universities — Carnegie Mellon and the University of New Mexico — to investigate ways to diversify software and information systems in an effort to fend off cyberattacks. "We are looking at computers the way a physician would look at genetically related patients, each susceptible to the same disorder," says Carnegie Mellon engineering professor Mike Reiter. "In a more diverse population, one member may fall victim to a pathogen or disorder while another might not have the same vulnerability." The $750,000 grant comes in response to massive digital epidemics caused by the Code Red, Slammer and MSBlast worms, which disabled hundreds of thousands of computers over the past year. The researchers hope to create an application that could generate diversity in key aspects of software programs without hampering their utility. The result could prove a boon for Microsoft by helping it to break up its monoculture without losing market share. (CNet News.com 25 Nov 2003)

Category 4C1 *Paradigms, security standards*

2003-12-24 **NIST security guidance standards FISMA FIPS**

NIPC/DHS

December 22, Federal Computer Week — NIST releases security level guidance. The National Institute of Standards and Technology (NIST) released a draft of the last piece of guidance for agencies to determine the proper level of security on information systems last week. The "Special Publication 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories" provides the middle step for guidance and standards required under the Federal Information Security Management Act (FISMA) of 2002. NIST's categories of security impact are based on draft Federal Information Processing Standard (FIPS) 199, which the division released in September. The goal of the guidance is to have agencies assign impact levels without considering potential security controls and countermeasures, but in October, NIST released another draft guide outlining minimum-security controls for each category. NIST also released a draft interagency report on smart card technology development and adoption within agencies. The draft report is in response to a January General Accounting Office report that recommended that NIST play a greater role in smart card implementation governmentwide. Additional information is available on the NIST Website:
http://csrc.nist.gov/publications/drafts.html

Category 4C1 *Paradigms, security standards*

2004-01-15 **monoculture SNMP virus worm network Internet parallel agriculture pest epidemic**

CNET News http://news.com.com/Seeds+of+destruction/2009-7349_3-5140971.html

AGRICULTURE EPIDEMICS MAY HOLD CLUES TO NET VIRUSES

Computer scientists and biologists have been thinking about the parallels between computer viruses and biological viruses for years. Robert Lemos, a distinguished writer for CNET News, wrote a report on the growing collaboration in January 2004. One of the main ideas is that monoculture makes both agricultural fields and computer networks more susceptible to pathogens such as the Potato Blight that devastated Ireland in 1845 and the MSBlast worm that attacked Windows computers in August 2003. Many experts have pointed out that almost all of the major attacks on the Internet have been rooted in the Microsoft monoculture, including the Outlook e-mail client and the IIS (Internet Information Server) products. Another widespread technology at risk is SNMP, which could also be exploited by worms.

Category 4C1 *Paradigms, security standards*

2004-01-22 **Common Criteria CC certification standard Linux SUSE Enterprise Server 8 IBM eServer Access Protection Profile**

NIPC/DHS

LinuxWorld: SuSE, IBM gain higher security certification

Raising the security bar one notch higher, SuSE Linux AG and IBM Wednesday said they have achieved a more rigorous security certification for Linux operating system software running on Big Blue servers. With the higher-level security evaluation, the two companies hope to attract governments and organizations with critical operations to open source Linux software.

Category 4C1 *Paradigms, security standards*

2004-01-26 **NIST IT security draft report guidelines**

NIPC/DHS; ; http://www.fcw.com/fcw/articles/2004/0119/web−nist−01−23−04. asp

January 23, Federal Computer Week — NIST releases telnet, IT security drafts.

Federal agencies desiring to minimize work disruptions from outside intrusions can begin with simple safeguards, such as preventing unauthorized users from using the telnet protocol to gain access to a server, according to officials at the National Institute of Standards and Technology (NIST). Draft documents on computer security released Thursday, January 22, by the NIST give an example of how unauthorized telnet users simply identify themselves as a guest to gain access to sensitive government files. The Risk Management Guide for Information Technology Systems suggests that disabling telnet is about a 10-hour procedure. Practical advice in the 58-page document includes other ways that agencies can develop standards for safeguarding sensitive but unclassified information in federal computer systems. As applied to information systems, the guide says, risk management is a responsibility of executive managers to be shared with technical managers, and not a technical manager's sole responsibility. Engineering Principles for Information Technology Security, a 33-page document also released this week, offers an overview of accepted principles and practices for security information technology systems. Additional information can be found on the NIST Website:
http://csrc.nist.gov/publications/drafts.html

Category 4C1 *Paradigms, security standards*

2004-02-14 **Common Criteria CC certification standard Pointsec Mobile Level 4 EAL5 PC hard disk encryption software**

NIPC/DHS

Pointsec Gains CC Certification For Encryption Software

Pointsec Mobile Technologies says it has gained Evaluation Level 4 (EAL4) Common Criteria certification for its Pointsec for PC hard disk encryption software
The SC Infosecurity Newswire, Feb 13, 2004.

Category 4C1 *Paradigms, security standards*

2004-02-23 **AVDL Application Vulnerability Description Language XML base standard security**

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml?articleID=18100080

February 23, Information Week — Application security standard edges forward.

An application security standard known as Application Vulnerability Description Language (AVDL), which was proposed last year, is moving closer to reality. AVDL is based on XML and is designed to provide a standard way for application vulnerabilities to be defined and classified so all security applications from different vendors that companies use to secure their apps will understand the same language when it comes to security threats. For example, when a new software vulnerability surfaces, a company's vulnerability scanner could scan systems to spot the new flaw. The scanner then could send information to firewalls and patch-management systems, which those applications could then use to automatically adjust to better protect against any potential attacks, such as a worm or a hacker attack. AVDL 1.0 standard is complete and is expected to receive final standards approval next month. Gartner VP and analyst John Pescatore says that because of the number of application vulnerabilities that surface each week -- sometimes more than 80 are announced -- standards such as AVDL can help companies reduce the threat they face from the moment a vulnerability is discovered to the time it takes them to respond and patch.

Category 4C1 *Paradigms, security standards*

2004-04-01 **NIST draft standards securing computer systems**

DHS IAIP Daily; Source: http://www.fcw.com/fcw/articles/2004/0329/web−nist−04−01−04. asp

April 01, Federal Computer Week — NIST releases drafts.

Officials at the National Institute of Standards and Technology (NIST) announced this week the draft release of two security documents that provide detailed guidelines to federal agencies and other organizations for securing computer information systems. Special Publication 800-60, "Guide to Mapping Types of Information and Information Systems to Security Categories," is the second draft of a document meant to help federal agencies meet the requirements of the Federal Information Security Management Act of 2002. It describes how to categorize types of information and information systems for assessing security risks. Both documents are available at http://csrc.nist.gov/publications/drafts.html. The publications complement previous technical works from NIST.

Category 4C1 *Paradigms, security standards*

2004-04-06 **NIST security standards guidelines draft online**

DHS IAIP Daily; http://fcw.com/fcw/articles/2004/0405/web−nist−04−06−04.asp

April 06, Federal Computer week — Last draft released for security guide.

The National Institute of Standards and Technology (NIST) on April 6 released a final draft of security guidelines for federal agencies that need to certify and accredit their information systems. With May as their target date for publication, NIST officials cited an urgent need to receive comments on the final draft document by April 21. The proposed guidelines are relevant to security requirements that all federal agencies must meet under the Federal Information Security Management Act of 2002. NIST officials incorporated several significant changes in the final draft based on earlier comments they received. Among them are newly defined roles for the chief information officer and senior agency information security officer in the certification and accreditation process. Also new are additional guidelines for low-impact information systems, a revised timetable for interim approval to operate information systems, and a summary table of tasks and subtasks for security certification and accreditation. Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, is available online.

Category 4C1 *Paradigms, security standards*

2004-04-13 **Common Criteria CC certification standard Apple Computer Mac OS X open-source government**

NewsScan

APPLE PUSHES FEDS TOWARD BROADER OPEN-SOURCE USE

Apple Computer Inc. is seeking Common Criteria evaluation of Mac OS X, which could open government doors wider to open-source software.

Category 4C1 *Paradigms, security standards*

2004-04-14 **Common Criteria CC certification standard Symantec Firewall componenet Level 4 EAL4**

SYMANTEC FIREWALL COMPONENT RECEIVES CERTIFICATION

The firewall engine of Symantec Corp.'s Gateway Security 5400 appliance has received Common Criteria Evaluation Assurance Level 4 certification.

Category 4C1 *Paradigms, security standards*

2004-04-19 **cyber security strategy federal government recommendations**

DHS IAIP Daily; http://fcw.com/fcw/articles/2004/0419/web−ncsp−04−19−04.asp

April 19, Federal Computer Week — Last part of security strategy released.

A cybersecurity task force organized by the National Cyber Security Partnership issued a 104-page report with recommendations for the federal government and industry on Monday, April 19. The report is the last of five documents prepared by industry and academic experts on the President's National Strategy to Secure Cyberspace, a general blueprint for improving the nation's cybersecurity readiness. The task force members called for what they said were needed improvements to the consumer- and vendor-oriented software security testing program operated by the National Institute of Standards and Technology and the National Security Agency. The report recommends that NIST receive an initial $12 million in new appropriations and $6 million in following years for developing security requirements for specific classes of products such as intrusion-detection systems and virtual private networks. Other steps outlined in the report include making vendors responsible for shipping software products with more of their security features enabled and having the federal government mandate software-vulnerability analysis as a condition of procurement. The group also recommended that industry groups work together to develop a well-defined set of technical standards for designing secure IP networks. The report is available online: http://www.cyberpartnership.org/TF4TechReport.pdf

---

Category 4C1 *Paradigms, security standards*

2004-04-29 **security needs protecting company information assets Network Applications Consortium**

DHS IAIP Daily; http://www.nwfusion.com/news/2004/0426nac.html

April 26, Network World — User group defines security needs.

The Network Applications Consortium (NAC) plans to publish a document this summer that outlines the principle, policies, standards, technologies and processes necessary to protect a company's information assets. NAC's Enterprise Security Architecture addresses hot topics in cybersecurity such as governance, technology architecture and operations. The document will affect how several major corporations--including Bechtel, Boeing, GlaxoSmithKline and State Farm Insurance--make network hardware and software purchases in the future, network executives at these companies say. NAC members also plan to use the document to influence how key network vendors such as Cisco, Entrust, Microsoft and Symantec create security products. The consortium plans to embrace several security standards--selections have not been finalized--and urge vendors to adopt these standards. The document's goal is to create a framework that lets companies mix and match security products from different vendors while assuring interoperability and manageability. Additional information is available on the NAC Website: http://www.netapps.org/

Category 4C1 *Paradigms, security standards*

2004-05-09 **Sasser german teenager $250000 microsoft sabotage computer**

NewsScan

SASSER CREATOR TURNED IN FOR THE REWARD

The German teenager who created the computer worm Sasser was identified by acquaintances seeking a $250,000 reward from Microsoft. The young man was arrested in the village of Waffensen, near Bremen, and appeared shaken by the extent of the damage his program had caused around the world. He faces charges of computer sabotage, which under German law could mean his imprisonment for five years. If the teenager is convicted, Microsoft will make good on its pledge for the full $250,000 reward. (Washington Post 9 May 2004)

Category 4C1 *Paradigms, security standards*

2004-05-13 **NIST Standards Documentation FISMA**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/25881−1.html

May 13, Government Computer News — NIST releases computer security documents.

The National Institute of Standards and Technology (NIST) has published final versions of three computer security documents and released one draft document for public comment. Special Publication 800-38C, Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality, specifies an authenticated encryption mode of the Advanced Encryption Standard. The Guide for the Security Certification and Accreditation of Federal Information Systems (Special Publication 800-37), is one of a series of guidelines to help agencies comply with the Federal Information Security Management Act (FISMA). FISMA requires that all IT systems be certified and accredited for operation. The new guidelines provide a standardized approach for assessing the effectiveness of security controls determining the risks posed by threats to the system. A draft of An Introductory Resource Guide for Implementation of the Health Insurance Portability and Accountability Act Security Rule (Special Publication 800-66), provides help for agencies subject to both HIPPA and FISMA. The document identifies NIST resources for addressing HIPPA requirements, and provides cross-mapping between HIPPA and FISMA requirements to help agencies avoid redundant work. Additional information is available on the NIST Website: http://www.nist.gov/

Category 4C1 *Paradigms, security standards*

2004-05-24 **cybersecurity corporate executives threats outside hackers inside jobs CSO Carnegie Mellon CERT**

NewsScan

CORPORATE EXECS SHIFT THEIR FOCUS TO OUTSIDE CYBERTHREATS

A greater percentage of corporate executives are worried about cybersecurity threats from outside hackers than inside jobs by disgruntled or recently fired workers, according to a recent survey conducted by CSO (Chief Security Officer) magazine in cooperation with the Secret Service and Carnegie Mellon's CERT (Computer Emergency Response Team). The shift in focus marks a change in corporate attitudes toward security, says CSO publisher Robert Bragdon: "Historically, businesses have always focused on internal threats being the biggest dangers to their organization." But despite the change, 36% of the 500 executives polled said they still managed to keep a close eye on employees' Web activities and e-mail to prevent internal sabotage and leaks. Meanwhile, the costs of computer crime are going up. The study estimates that cybercrime attacks against businesses and government agencies cost $666 million last year. (Washington Post 24 May 2004)

Category 4C1 *Paradigms, security standards*

2004-05-25 **vulnerability reporting OIS guidelines**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/26045−1.html

May 25, Government Computer News — Group wants input on vulnerability reporting guidelines.

The Organization for Internet Safety (OIS) is soliciting comments on its guidelines for reporting and responding to software security vulnerabilities. OIS, a consortium of software vendors, researchers and security consultants, released the guidelines in July 2003, hoping to bring some order to the continual struggle between code makers and code breakers. The second version is expected to be available in mid-July. OIS hopes to address some issues in the second release that were sidestepped in the first edition, such as what role—if any—the government should play in vulnerability reporting. The voluntary guidelines are an effort to balance the public's right to know about possible software problems against the need for vendors to correct those problems before they are made public. Comments are being accepted through June 24 at feedback@oisafety.org. Details for the comment process are available at www.oisafety.org/review-1.5.html

---

Category 4C1 *Paradigms, security standards*

2004-08-24 **Microsoft leaves UN standards group Center Trade Facilitation Electronic Business intellectual property open source proprietary software**

NewsScan

MICROSOFT BUGS OUT OF U.N. STANDARDS GROUP

Microsoft has withdrawn from a U.N. software standards group focused on automating buying and selling through networks of computers. The diverse membership of the group -- known as the United Nations Center for Trade Facilitation and Electronic Business (U.N./Cefact) -- includes advocates of both proprietary and open-source approaches to software technology standards; however, Microsoft-watchers believe that the company's decision to withdraw from the group can be traced not to the open-source vs. proprietary standards debate but rather to issues concerning control of the intellectual property being contributed to the standards-setting effort. (New York Times 24 Aug 2004)

Category 4C1 *Paradigms, security standards*

2004-10-27 **National Information Assurance Partnership NAIP Common Criteria CC praise certification**

DHS IAIP Daily; http://www.fcw.com/fcw/articles/2004/1025/web−niap−10−27 −04. asp

October 27, Federal Computer Week — NIAP chief touts Common Criteria.

Officials at the National Information Assurance Partnership (NAIP) have effectively raised the level of security in many information technology products used by the government, the security group's director said Wednesday, October 27. NIAP, an initiative of the National Institute of Standards and Technology and the National Security Agency, is responsible for implementing the Common Criteria Evaluation and Validation Scheme, a rigorous set of security tests that adhere to international standards. The testing directly improved 30 percent of the products tested by eliminating security flaws that could have been exploited by attackers, said Jean Schaffer, director of NIAP. Critics say Common Criteria testing costs too much and takes too long, but Schaffer argued that these claims are made by those who do not have firsthand knowledge about the testing.

Category 4C1 *Paradigms, security standards*

2005-02-08 **Office Management Budget OMB cybersecurity standardization increase security reduce spending task force Homeland Security DHS**

DHS IAIP Daily; http://www.govexec.com/dailyfed/0205/020805p1.htm

OFFICE OF MANAGEMENT AND BUDGET CONSIDERING CYBERSECURITY STANDARDIZATION

Office of Management and Budget (OMB) officials are considering standardizing the cybersecurity business processes of agencies in order to save money, increase security and help those with small information technology budgets. A task force led by the Homeland Security Department and OMB officials will meet in March to consider whether the consolidation of common processes, services and technologies regarding security could improve performance while reducing costs. About $4 billion is spent each year securing federal information technology; an OMB official speculated that 40 percent of that is spent on processes that are common among agencies. The task force would examine how much of the $4 billion is spent on actual security improvements rather than duplicative administrative functions.

Category 4C1 *Paradigms, security standards*

2005-02-20 **software quality assurance QA systems engineering failure rates programming errors design flaws process modular construction paradigm shift expectations**

RISKS 23 73

BUY VS BUILD -- OR ELSE

Paul Robinson wrote an essay for RISKS that pointed out how unusual it is in our society for us to build tools or other products from scratch in our normal lives. We buy bread, cutlery, peanut butter, kitchen sinks, stoves, tiles … almost everything we need is created by specialists and used by others.

So why do we think it is still normal to build software from scratch? Why aren't we insisting on building software from well-tried-and-tested modules that we can use to put together the desired functionality?

And how come other products, such as wrenches, refrigerators and washing machines, have warranties -- some of them lifetime warranties -- but software generally does not? Why are we tolerating this degree of shoddy engineering and production in such critical tools in our current lives?

The question that should be asked is, "why this is allowed to continue?"

Robinson writes:

Software as it is currently being developed provides so much value relative to its costs that we as practitioners of this medieval-class craft (in terms of our level of automation and sophistication of production methods) can get away with practices that would not be tolerated by a Taiwanese manufacturer of toasters.

And this is the reason we are seeing programming jobs being outsourced to low wage countries. If you're going to get crappy software there's no reason to pay premium prices for it. It is exactly the sort of situation that befell the American automobile manufacturers back in the 1970s and 1980s. And unless we start to make changes we will see exactly the same thing happening.

Actually some of the software development places that are used for outshoring have formal practices in place for reducing defects. So it is entirely possible what we are getting is the exact equivalent of what I stated above. The overseas "manufacturers" produce better quality at a lower cost than we do.

I think that a basis of component architecture is the direction that we need to go in the development of software. That we need to make more software to be designed as a series of reusable components that can be used in other contexts. It also means we need to develop at least an engineering discipline in a way of making software of higher quality and eventually to reduce the risks of development.

And this is why I now understand more clearly why I knew that there was something right about this concept even though I didn't know exactly why at the time. In a book I once wrote, the main character explains about realizing the validity of a concept even if you're not sure why:

>I know how that is; more than once I've had gut feelings about things where I couldn't put my finger on it, but I knew something wasn't right. Later I would discover why I had that feeling, and, more importantly, why I was right, but at the time I did not have the evidence or knowledge to know why I felt that way.<

- George Green, "In the Matter of: The Gatekeeper: The Gate Contracts"

We can continue on the same path of disaster-ridden bugware or we can choose to change. We can change because the current methods do not work very well, they spell disaster in terms of cost, reliability, future employment potential, and the possibility of seeing our craft ruined by heavy-handed government mandates for licensing. We can choose to change because if we do not, the choice on how to make the changes may be made for us, and in a manner we will not appreciate.

The process will not be easy, but the benefits to us will more than outweigh the short-term losses by having to re-learn a new way of working, and thinking. If we want to continue to have fun in this craft without being placed into a bad position because of our own arrogance in failing to acknowledge the incompetence, sloth and waste our current practices contain, we need to change. And we need to do it before we are forced to do so because the customers decide they can't stand it any more, before we do.

* * *

This essay provoked a flurry of interesting contributions in RISKS 23.74 < http://catless.ncl.ac.uk/Risks/23.74.html#subj2 >. Highlights include these points [with authors in square brackets so you can find their full comments easily]:

* The same issues were raised in 1968 by Doug McIlroy in a NATO conference on software engineering; see < http://homepages.cs.ncl.ac.uk/brian.randell/NATO/>. [Jim Horning]

* Problems in components spread throughout the industry; e.g., "the buffer overflow in the commonly-used JPEG decoding algorithm." [Rick Russell]

* Software is much more complicated than manufactured goods. [Rick Russell]

* Describing software is much more difficult than describing physical objects or tools and therefore reusability is difficult to engineer or attain. [Kurt Fredriksson]

* Even when reusable components are part of a software project, there is still lots of work because of dependencies that may break the code when components are poorly upgraded. [Jay R. Ashworth]

* Object-oriented programming has resulted in aborted development of more advanced programming languages. [Kurt Fredriksson]

* It may not be possible to write perfect code using the specifications of existing code because new situations may impose unexpected constraints that lead to unexpected behavior of the systems. [Ray Blaak]

* Work by Jef Raskin, the architect of the Macintosh project at Apple, may lead to error-free user interfaces. See his text "The Humane Interface: New Directions for Designing Interactive Systems." [Richard Karpinski] [MK looked up the ISBN: 0-201-37937-6 & the AMAZON URL: http://tinyurl.com/abt7a]

* "…[T]he problem isn't a lack of components, it's that we're building much larger systems in relation to the power of those components." [Geoff Kuenning]

* "… [O]ther people's components will only work for you if those people's domain model is sufficiently close to yours -- otherwise they are be too generic to be of any use to anybody, all they are is overhead." [Dimitri Maziuk]

* "Software is not constrained by the laws of nature (until or unless it comes to controlling a real system)…. Thus while traditional manufacture is bounded by well-established physical parameters which lend themselves to repeatable solutions, requirements for software systems are not so bounded. This tends to mean that the requirements for each system are unique. And because of the perception that software can do anything, the requirements tend to be complex too: arguably excessively so. Working this down into the details of implementation, this means that the components needed tend to be unique for each system - thus limiting the possibilities of reuse." [Stephen Bull]

Category 4C1 *Paradigms, security standards*

2005-02-28 **National Institute of Standards and Technology NIST security guidelines release Federal Information Security Management Act FISA**

DHS IAIP Daily;
http://news.com.com/NIST+releases+final+security+guidelines/ 2100−7348_3−5593256.html?tag=nefd.top

NIST RELEASES FINAL SECURITY GUIDELINES.

A final version of security guidelines designed to protect federal computer systems and the information they hold was released Monday, February 28, by the National Institute of Standards and Technology (NIST). The guidelines will serve as a road map for federal agencies in meeting mandates set by the Federal Information Security Management Act (FISA). Government agencies will be required to have certain security controls, policies and procedures in place. At the heart of the initiative is an effort to protect the confidentiality, integrity and availability of all federal information systems that are not part of the national security system. The security controls in the new NIST guidelines span 17 key areas, ranging from user identification to authentication to risk assessment. Guidelines: http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.p df

---

Category 4C1 *Paradigms, security standards*

2005-06-09 **NIST feds control security computer systems FISMA**

EDUPAGE; http://www.fcw.com/article89154-06-09-05-Web

FEDS LOOK TO ADD CONTROLS TO COMPUTER SYSTEMS

The National Institute of Standards and Technology (NIST) is developing a set of controls that federal agencies will be compelled to adopt to increase the security of their computer systems. The controls are part of an effort to bring agencies into compliance with the Federal Information Security Management Act (FISMA). FISMA Implementation Project Leader Ron Ross said that agencies will be required to add 17 safety controls to their systems, noting that stronger controls will be required for more important systems. When finalized, the controls will become mandatory in January 2006. Agencies will have one year to implement the controls on existing systems; for new systems, the controls will be required immediately. Ross stressed that although it will not be "easy to put in all these controls and get them working," the government must make every effort "to establish a federal level of due diligence" for its computer systems. Federal Computer Week, 9 June 2005

Category 4C1 *Paradigms, security standards*

2005-12-15 **IT costs laws compliance budgets corporate governance study Sarbanes-Oxley SOX**

EDUPAGE; http://news.zdnet.com/2100-9595_22-5996670.html

MEETING COMPLIANCE LAWS RAISES IT COSTS

According to a recent Gartner study, laws on corporate governance and compliance, such as the U.S. Sarbanes-Oxley Act, force businesses to spend more on information technology. The report predicts increases in IT budgets from 10 to 15 percent in 2006, up from roughly 5 percent in 2004. The survey included 326 audit, finance, and IT professionals in North America and Western Europe. Gartner recommended solutions that can support multiple regulations across a business to maximize effectiveness on spending for compliance.

Category 4C1 *Paradigms, security standards*

2006-02-15 **vulnerability exploit code Microsoft product challenge Security Bulletin critical rating iDefense auction sale**

DHS IAIP Daily; 23
http://www.windowsitpro.com/windowspaulthurrott/Article/ArticleID/49416/windowspaulthurrott_49416.html

IDEFENSE OFFERS $10,000 BOUNTY FOR CRITICAL BUG BY 31 MARCH 2006

iDefense announced that it will pay $10,000 to anyone who discovers a bug in a Microsoft product that results in a new Microsoft Security Bulletin with a severity rating of critical. But there's one slight catch: The bug must be reported by midnight March 31, 2006, EST. The company has paid for vulnerability reports for some time now. However iDefense is changing its tactics to some extent. A spokesperson for iDefense said, "Going forward, on a quarterly basis, we will select a new focus for the challenge and outline the rules for vulnerability discoveries that will qualify for the monetary rewards." iDefense competes against a growing underground market for vulnerability reports and exploit code, where reports and code are sometimes sold the highest bidder and other times sold to everyone who can pay the asking price.

Category 4C1 *Paradigms, security standards*

2006-03-06 **open source bug hunt results posted DHS funding Coverity Stanford Symantec team**

DHS IAIP Daily; http://www.gcn.com/online/vol1_no1/40053−1.html 23

OPEN-SOURCE BUG HUNT RESULTS POSTED.

Coverity Inc. of San Francisco, CA, has released the results of a Department of Homeland Security (DHS)-funded bug hunt that ranged across 40 popular open-source programs. The company found less than one-half of one bug per thousand lines of code on average, and found even fewer defects in the most widely used code, such as the Linux kernel and the Apache Web server. To test the programs, Coverity deployed analysis software first developed by Stanford's computer science department. Ben Chelf, chief technology officer of Coverity, warned that this automated bug scan is not definitive, but it can point to bugs traditional in-house code review techniques can miss. The results are the first deliverable of a $1.2 million, three-year grant DHS awarded to a team consisting of Coverity, Stanford University and Symantec Corp. of Cupertino, CA. DHS wants to reinforce the quality of open-source programs supporting the U.S. infrastructure.

4C2 Risk management methodology & tools

Category 4C2 *Risk management methodology & tools*

1999-01-04 **enterprise security data integration tool**

Business Wire

Internet Security Systems introduced SAFEsuite(R) Decisions to automate the collection, integration, analysis and reporting of enterprise-wide security information from multiple sources and locations including not only integrated data from ISS' intrusion and vulnerability detection systems, but also third-party security safeguards such as firewalls.

Category 4C2 *Risk management methodology & tools*

2000-01-17 **cybercrime insurance risk management**

National Underwriter Property and Casualty

Several insurance companies began providing insurance to pay for damages resulting from illegal penetration of computer systems and networks and even against extortion. For example, in May 1999, the F&D/Zurich company in Baltimore announced policies with up to $25M in compensation for damages to e-businesses. Some policies cover insider damage such as logic bombs or destruction of critical data by enraged employees; Brad Gow of ACE USA in Philadelphia reported on one case where an employee at a Massachusetts defense contractor "destroyed all their critical databases and project data. The company identified direct costs of rebuilding data at about $2.4 million." Daniel Hays, writing for the _National Underwriter Property and Casualty_ publication, said that estimated total loss from missed sales and other opportunities and other setbacks to that business were projected to be $10 million.

Category 4C2 *Risk management methodology & tools*

2000-04-02 **Internet security monitoring log files audit trails intrusion-detection**

NewsScan, San Jose Mercury News
http://www.sjmercury.com/svtech/news/breaking/merc/docs/006917.htm

A new Internet security company called Counterpane Internet Security Inc., organized by well-known author and consultant Bruce Schneier, will use teams of analysts continuously scrutinizing activity logs from customer Internet sites and sound the alert when there are signs of an intrusion. Schneier says, "Computer security without monitoring is kind of like having a car alarm go off in the inner city. It might make a lot of noise, but everyone ignores it." An executive of Computer Associates, the current industry leader in computer security, insists his company will continue following a different approach: "We have seen in this industry that throwing more people at a problem actually doesn't solve it. Our approach is to apply technology solutions to solve problems rather than throwing more warm bodies at them." (AP/San Jose Mercury News 2 Apr 2000)

Category 4C2 *Risk management methodology & tools*

2000-06-08 **backup failure e-mail loss destruction documentation**

RISKS 20 91

In April 1998, the Office of the Vice President migrated the e-mail server to Windows NT 4 and moved the e-mail files to a new partition which was not added to the backup schedule. In May 1999, staffers discovered that there were therefore no backups at all of any of the e-mail for the office over more than a year. [MORAL: documentation and proper procedures really DO matter.]

Category 4C2 *Risk management methodology & tools*

2000-06-14 **government operations outsourcing quality assurance QA**

NewsScan, TechWeb http://www.techweb.com/wire/story/TWB20000613S0012

Prompted by results from its 15-month Project Groundbreaker feasibility study, the National Security Agency plans to use private sector sources to develop and maintain the bulk of its unclassified information technology infrastructure. This dramatic change in NSA's long-standing IT operations is intended to ensure the agency's agility and adaptability in the Information Age. The move to abandon the traditional policy of developing spy technology in-house in favor of procurement from the rapidly expanding encryption and fiber-optic technology available off-the-shelf was inspired in part by last January's massive computer failure that crippled NSA's global spy network for several days. The IT modernization will cover NSA's distributed computing, its enterprise/security management, networks and telephony. It is expected to save the government as much as $1 billion over 10 years. (TechWeb 14 Jun 2000)

Category 4C2 *Risk management methodology & tools*

2000-07-10 **criminal hacker attack insurance penetration vandalism outsourcing monitoring intrusion detection**

NewsScan, USA Today http://www.usatoday.com/life/cyber/tech/cti199.htm

Lloyds of London and two other insurance companies will offer up to $100 million in insurance coverage to the clients of the computer security management firm Counterpane Security against losses resulting from attacks by network vandals. A Counterpane executive says, "This is not for your home user, this is for Yahoo!, this is for CDUniverse... It's threat-avoidance. This, along with monitoring, is just another arrow in your quiver." A recent study by Reality Research has predicted that businesses worldwide will lose an estimated $1.5 trillion this year due just to computer viruses spread through the Internet. (USA Today 10 Jul 2000)

Category 4C2 *Risk management methodology & tools*

2001-07-01 **Digital Millennium Copyright Act DMCA video bootleg copyright infringement intellectual property ISP Internet Service Provider liability lawsuit judgement**

NewsScan

EBAY GRANTED VICTORY IN COPYRIGHT LAWSUIT
EBay won what it called a precedent-setting lawsuit Thursday when a federal judge ruled that the online auction company was not liable for copyright infringement under the Digital Millennium Copyright Act in the case of bootlegged copies of a Charles Manson documentary that were sold on the site. The case was touted as the first to test whether a Web site has a "safe harbor" if people who use the site sell items that infringe on copyrights. In his ruling the judge agreed with eBay's position that it is not like a real-world auctioneer that vouches for the items on sale, but rather is more like a provider of stalls at a flea market. (AP/Silicon Valley Sep 7 2001)
http://www.siliconvalley.com/docs/news/svfront/000051.htm(-20-)

Category 4C2 *Risk management methodology & tools*

2001-08-24 **downstream liability negligence standard due care Web vandalism denial of service DoS**

NewsScan

BLAME THE VICTIM: VANDALIZED WEB SITES MAY BE LIABLE FOR DAMAGES
Some legal scholars are suggesting that a Web site vandalized by hacker attacks may itself be legally liable if its customers suffer damages and if the site was negligent in maintaining security. Law professor Margaret Jane Radin of Stanford University predicts: "A court is going to say it is negligent of you not to implement preventative measures if they are reasonably effective and affordable." No reported court decisions have dealt with the issue, but Radin says that lawsuits in the near future are highly likely to be lodged against companies and network providers targeted by "denial of service" attacks. (New York Times 24 Aug 2001)
http://partners.nytimes.com/2001/08/24/technology/24CYBERLAW.html

---

Category 4C2 *Risk management methodology & tools*

2001-10-19 **criminal hacker attack Web Internet disclosure reporting announcement proposed legislation confidentiality law enforcement investigation statistics**

NewsScan

WHITE HOUSE SUPPORTS LIMITED DISCLOSURE ON HACK ATTACKS
The Bush administration is backing bipartisan legislation aimed at limiting government disclosures about hack attacks. Congressional supporters of the proposed law include Senators Robert Bennett (R-UT) and John Kyl (R-AZ) and Representatives Tom Davis (R-VA) and James Moran (D-VA). Bennett told his Senate colleagues that if they didn't pass the bill -- which is designed to protect the confidentiality of information disclosed by companies about attempts to hack into their computers -- then companies will simply not provide all the details of such attacks to government security investigators. (AP/San Jose Mercury News 19 Oct 2001)
http://www.siliconvalley.com/docs/news/svfront/054790.htm

Category 4C2 *Risk management methodology & tools*

2001-10-31 **availability bugs repair artificial intelligence AI quality assurance**

NewsScan

IBM INTRODUCES SELF-HEALING BUSINESS SOFTWARE SYSTEMS
Adapting the same kind of "brute force" computing strategy of its chess-playing Deep Blue supercomputer, IBM's e-business Management Services is introducing "self-healing" business software that will allow machines to detect and work around failing parts and work overloads without requiring the intervention of onsite technicians. Irving Wladawsky-Berger, the company's vice president for technology and strategy, says: "This is really the essence of making systems behave in an intelligent manner... God knows if this means they are intelligent. But what we really like about this, and we learned a lot about this in Deep Blue, is the brute force techniques of having a lot of information and a lot of computer power is the most effective way of making systems behave in what we humans would call intelligence." (Reuters/San Jose Mercury News 31 Oct 2001)
http://www.siliconvalley.com/docs/news/svfront/076589.htm

Category 4C2 *Risk management methodology & tools*

2001-11-12 **national identity card terrorists reliance incorrect assumption risk management**

RISKS 21 75

Frequent RISKS contributor Adam Shostack pointed out a significant risk of national ID cards: mistaken reliance on identification as a substitute for trustworthiness. His cogent analysis follows:

"I believe that there is an important risk, that of reliance, that will accompany a high-tech national ID card. Every terrorist commits their first act of terrorism at some time in their life, and before that time, they cannot be any database of known terrorists.

Once you start issuing cards, people will start relying on 'identity verification' rather than threat management. We'll see people relying on background checks [1] rather than xrays. We'll see special lines for frequent fliers, who are 'known trustworthy.' They differ from pilots and flight crew in that they don't run into co-workers who can notice and react to strange behavior before the flight. If you want to keep knives and guns off of planes, the answer lies in xrays, magnetometers, and other searching technology, not in believing that you know who's who. Many of the national id card risks come from a layer of indirection from the real problem, which is not "Is Alice trusted," but, "Is the person in front of me trusted?" National ID cards not only do nothing to solve this problem, they distract us from attempting to solve it."

[1] See the last para of
http://www.spectrum.ieee.org/WEBONLY/special/sept01/idcards.html

---

Category 4C2 *Risk management methodology & tools*

2002-05-23 **information warfare malware subversion programmatic attacks Internet research paper**

RISKS 22 09

[Paraphrased and edited from the authors' announcement:]

Stuart Staniford, Vern Paxson, and Nicholas C. Weaver completed the paper, "How to Own the Internet in Your Spare Time" http://www.cs.berkeley.edu/~nweaver/cdc.web/ to appear in the 11th Usenix Security Symposium (Usenix Security '02).

They combined an analysis of Code Red I, the effects of Code Red II and Nimda, and the possibility of some new threats. They then use this to make a case for a CDC-like institution to proactively develop defenses for such threats.

Category 4C2 *Risk management methodology & tools*

2002-06-27 **audit oversight independence management**

RISKS 22 13

Rob Slade asked a disturbing question in a RISKS submission entitled "Qui audit ipsos auditors?"

>The Enron/Anderson debacle is fading as news, but it has some reverberations for those of us in the info tech fields.

Anderson is not alone in engaging in questionable audit practices. Others of the "Big 5" are under scrutiny, in at least two cases involving, ironically, high tech companies. For the past decade or more, there have been pressures to reduce regulatory oversight, and we are now seeing the results.

So, what is the relation to IT? Well, these are the same firms who hold the major contracts for auditing information security and assurance.

(In relation to the subject line: yes, "ISACA," I know.) <

Category 4C2 *Risk management methodology & tools*

2002-06-28 **insurance risk statistics mandatory reporting**

NewsScan

WHITE HOUSE WORKING TO PROMOTE CYBERSECURITY INSURANCE
The White House has been meeting with insurance industry leaders to discuss ways in which the industry could develop viable cybersecurity insurance policies for businesses. Insurance executive Robert Hartwig says, "Businesses will soon purchase this in the same way they buy property insurance. They wouldn't think of not insuring the buildings they're in, and soon they won't go without insuring the value of their computer systems." A general problem in creating such policies is that there is no real way of estimating an insurance provider's financial risk: "If you're insuring automobiles," says White House cybersecurity advisor Richard Clarke, "you can anticipate that there will be a certain number of accidents out of a given number of drivers, so you know what your loss exposure is. With cyberinsurance, there's not a lot of data that allows anyone to make that kind of prediction." (Washington Post 27 Jun 2002)
http://www.washingtonpost.com/wp-dyn/articles/A55719-20...

Category 4C2 *Risk management methodology & tools*

2003-01-15 **Microsoft expands security rating system vulnerabilities listing**

NIPC/DHS

January 13, Info World — Microsoft adds category to security rating system.

After customers complained that they couldn't identify the most serious security vulnerabilities, Microsoft has added a fourth category to its vulnerability rating system. But critics feel that the extra tier adds even more complexity to an administrator's job. Under the new system, fewer bulletins get the "critical" stamp. Only vulnerabilities that could be exploited to allow malicious Internet worms to spread without user action are now rated critical. Many issues that were previously rated critical are now "important," a new category in the rating system. These "important" vulnerabilities could still expose user data or threaten system resources, but they might not receive the urgent attention from administrators that they deserve. A two-tiered system would let administrators quickly decide whether they need to drop all tasks at hand and apply a patch, or whether the risk is small enough that they can wait and include it in a weekly patch cycle.

Category 4C2 *Risk management methodology & tools*

2003-01-16 **network sharing attack data countermeasure hacking**

NIPC/DHS

January 13, eWeek — Sharing attack data could thwart hackers.

Two Harvard University security researchers have developed a model showing that enterprises that share their sensitive data about network attacks and security breaches are less attractive targets and, hence, less likely to be attacked. The reason is that attackers who spend time, and in some cases money, finding and exploiting vulnerabilities in common applications will not want information about their attacks shared, as it would reduce their chances of compromising other potential targets. The paper, to be presented later this month at the Financial Cryptography conference in Gosier, Guadeloupe, supports the U.S. government's contentions about the importance of sharing attack data. The next draft of the National Strategy to Secure Cyberspace, due early this year, is expected to include language encouraging CIOs to forward more information to the government. Security specialists and CIOs worry that sharing sensitive data with anyone will expose them to embarrassment and potential lawsuits from customers. The government's interest in attack data is partially due to the creation of the Department of Homeland Security which will be responsible for early warning and analysis.

Category 4C2 *Risk management methodology & tools*

2003-01-29 **hacking insurance risk mitigation**

NewsScan

HACKER INSURANCE
The latest cyber attack (last weekend's SQL Slammer virus, which infected thousands of computer servers throughout the world) has given a new boost to "network risk insurance" (AKA "hacker insurance"), which is expected to grow from the $100 million industry it is now to a $2.5 billion industry by 2005. Bruce Schneier, the chief technology officer for Internet security at Counterpane, thinks that insurance is every bit as important as prevention: "I believe that within a few years hacking insurance will be ubiquitous. The notion that you must rely on prevention is just as stupid as building a brick wall around your house. That notion is just wrong." But getting "hacker insurance" is not as easy as one might think, because insurers typically require a third-party assessment of the insurance applicant's security system, which might cost as much as $50,000. (Reuters/USA Today 28 Jan 2003)

Category 4C2 *Risk management methodology & tools*

2003-02-07 **probabalistic risk management software mathematics statistics**

NIPC/DHS

February 06, New York Times — Assessing the odds of catastrophe.

A rapidly evolving set of conceptual and computing tools allow mathematicians, engineers and insurance executives to assess the risk of low-probability, high-consequence events. The field, known as probabilistic risk assessment, helps companies and government agencies decide whether they are prepared to take the chances involved. And now some of the techniques are being used to analyze the chances of terrorist attack. Developed four decades ago, the idea behind probabilistic risk assessment is that mathematics can help determine the chances of a particular outcome (a power system failure, or a hurricane that destroys thousands of homes) based on what is known or estimated about the smaller variables that lead to those outcomes. Jim Goodnight of SAS, a maker of statistical software, said that with faster processors, more advanced software and a huge availability of memory - whether on big mainframe computers or on lashed-together PC systems - "the ability to do the incredibly difficult modeling is becoming more reachable every day." Probabilistic models, of course, are only as useful as the assumptions fed into them. Moreover, they are best used when a system or piece of equipment is being designed. The most daunting challenge, however, may be modeling minds. In describing the challenge of modeling terrorism, Hemant H. Shah of RMS, a risk-modeling firm, said, "Hurricanes do not make an effort to strike your weak points. In the case of terrorism you're dealing with a question of intent. You're modeling an adversary in the context of conflict."

Category 4C2 *Risk management methodology & tools*

2003-04-17 **coporate IT security disclosure secure cyberspace**

NIPC/DHS

April 14, eWEEK — Feds mull IT disclosure.

Momentum is building in Washington to require all public companies to annually report the performance of their IT security initiatives, not just the financial services and health care industries that face scrutiny now. The Bush administration considered requiring companies to report on network security during the crafting of the National Strategy to Secure Cyberspace. But the idea was unpopular in many enterprises and did not make the final plan, released in February. Last week, former presidential adviser for cyberspace Richard Clarke, who spearheaded the strategy, urged Congress to act quickly to legislate such obligations. Enterprises object to the suggestion of broad reporting requirements, but some see a certified audit process reflected in annual Securities and Exchange Commission filings as beneficial. Possible requirements include disclosing measures taken to secure systems, identifying IT security auditors and detailing breaches.

Category 4C2 *Risk management methodology & tools*

2003-05-07 **report attacks failure e-commerce serious damage businesses cyber police NHTCU Len Hynds Infosecurity**

NIPC/DHS

May 07, vnunet.com — UK ecommerce hit by failure to report attacks.

Consumer and corporate trust in ecommerce will be seriously damaged if businesses do not report electronic crimes, says the UK's online police force. The National Hi Tech Crime Unit (NHTCU) is trying to convince companies to report cyber attacks. Only 56 per cent of larger companies report electronic crime to the police, and the figure is believed to be even lower among smaller organizations. "It's vitally important that people trust their technology," Len Hynds, head of the NHTCU, told delegates at last week's Infosecurity conference in London.

Category 4C2 *Risk management methodology & tools*

2003-11-05 **data sharing disaster recovery business continuity planning Homeland Security**

NIPC/DHS

November 04, GCN.com — Data sharing needs to begin before first response, officials say.

For the National Guard Bureau, the ability to share data for disaster planning and first response has been hampered by a constant stream of hacker intrusions on its unclassified networks over the past two years. "We're getting hacked all over the place. I actually see it getting worse, and it's making it harder and harder for us to share information," said Maureen Lischke, CIO for the National Guard Bureau. She and other government officials spoke about data sharing to support homeland security at an Industry Advisory Council event in Washington. Although cultural barriers represent the biggest hurdle, federal groups also need to think about sharing information before a major atrocity occurs, not after, said David Boyd, the Homeland Security Department's deputy director of R&D and director of the Safecom program to provide wireless communications to federal, state and local first responders. There's very little of such pre-disaster data sharing occurring now, beyond of the tactical warfighting level, said John Paczkowski, director of operations and emergency management for the Port Authority of New York and New Jersey. An open architecture is necessary to maintain some fundamental level of interoperability, Paczkowski said.

Category 4C2 *Risk management methodology & tools*

2003-11-25 **Veterans Affair department security program**

NIPC/DHS

November 24, Federal Computer Week — VA has new security program.

The Department of Veterans Affairs (VA) started a proactive vulnerability management program to provide improved cybersecurity at more than 250 facilities nationwide. The new strategy will provide more frequent security assessments, reducing risks and ensuring compliance with privacy regulations and internal security standards, officials said. Potential vulnerabilities can more easily be identified and reported to the VA's central incident response center for centralized management. In addition, the new service will allow individual facilities to quickly respond to security bulletins released by the response center.

Category 4C2 *Risk management methodology & tools*

2004-04-18 **copyright insurance open source operating systems users Linux Unix SCO lawsuits**

NewsScan

STARTUP OFFERS INSURANCE AGAINST LINUX COPYRIGHT CLAIMS

Open Source Risk Management is launching insurance-like protection aimed at indemnifying Linux users against copyright infringement claims like those made by SCO Group. The company says it has completed a six-month study comparing Linux with several version of Unix and found no copyright problems. "We have come out of the examination process with the strong belief that there are no meritorious copyright infringement claims in the kernel. With all we have seen to date, I don't believe they have a strong case," says OSRM executive director John St. Clair. OSRM's legal protection covers only copyright infringement, but it plans to offer patent protection as well for an additional charge. It also has launched an Open Source Legal Defense Center, which offers companies expert legal advice for $100,000 per year, while charging $250 per year for individual programmers. The copyright-infringement protection is priced at 3% per year of the total coverage -- so for protection against $1 million of legal costs, a company would pay $30,000. Meanwhile, an SCO spokesman disputed OSRM's claims: "Everything we have looked at and found would run contrary to what they're finding." (CNet News.com 18 Apr 2004)

Category 4C2 *Risk management methodology & tools*

2004-05-25 **software suppliers risk management defense acquisitions**

DHS IAIP Daily; http://www.gao.gov/new.items/d04678.pdf

May 25, General Accounting Office — GAO-04-678: Defense Acquisitions: Knowledge of Software Suppliers Needed to Manage Risks (Report).

The Department of Defense (DoD) is increasingly reliant on software and information systems for its weapon capabilities, and DoD prime contractors are subcontracting more of their software development. The increased reliance on software and a greater number of suppliers results in more opportunities to exploit vulnerabilities in defense software. In addition, DoD has reported that countries hostile to the United States are focusing resources on information warfare strategies. Therefore, software security, including the need for protection of software code from malicious activity, is an area of concern for many DoD programs. GAO was asked to examine DoD's efforts to (1) identify software development suppliers and (2) manage risks related to foreign involvement in software development on weapon systems. To address software vulnerabilities and threats, GAO recommends that DoD better define software security requirements and require program managers to mitigate associated risks accordingly. DoD agreed with the findings but only partially concurred with the recommendations over concerns that they place too much responsibility for risk mitigation with program managers. GAO has broadened the recommendations to address DoD's concerns. Highlights: http://www.gao.gov/highlights/d04678high.pdf

---

Category 4C2 *Risk management methodology & tools*

2005-01-19 **risk analysis terrorism politics propaganda rationality fear hysteria**

RISKS 23 68

SCHNEIER ON THE ILLUSION OF SECURITY

Curt Sampson published a review of an interesting article in ATLANTIC MONTHLY in January/February 2005. [That article extensively quoted noted security expert Bruce Schneier.] Mr Sampson's review follows:

In the January/February 2005 issue of _The Atlantic Monthly_ there is an article by James Fallows entitled "Success Without Victory," discussing risk management as it applies to the war on terror.

One key point is that there are people out there who, in the tradition of RISKS readers themselves, take a sensible and scientific approach to the war on terror, seeing it as an exercise in risk management rather than something that can be "won," causing all of the risks to go away:

> There will always be a threat that someone will blow up an airplane or a building or a container ship…. But while we have to live in danger, we don't have to live in fear. Attacks are designed to frighten us even more than to kill us. So let's refuse to magnify the damage they do. We'll talk about the risk only when that leads to specific ways we can make ourselves safer. Otherwise we'll just stop talking about it, as we do about the many other risks and tragedies inevitable in life.
>
> We cannot waste any more time on make-believe….measures that seem impressive but do not make us safer, such as national threat-level warnings and pro forma ID checks. The most damaging form of make-believe is the failure to distinguish between destructive but not annihilating kinds of attack we can never eliminate but can withstand and the two or three ways terrorist groups could actually put our national survival in jeopardy. We should talk less about terrorism in general and more about the few real dangers.
>
> Screening lines at airports are perhaps the most familiar reminder of post-9/11 security. They also exemplify what's wrong with the current approach. Many of the routines and demands are silly, eroding rather than building confidence in the security regime of which they are part.
>
> [Daniel] Prieto argues that the roughly $4 billion now going strictly toward airline passengers could make Americans safer if it were applied more broadly in transportation -- reinforcing bridges, establishing escape routes from tunnels, installing call boxes, mounting environmental sensors, screening more cargo. All these efforts combined now get less than $300 million a year, which will drop to $50 million next year.

Where the article gets really interesting, however, is in pointing out the political barriers to doing the rational thing from a risk-analysis point of view. For example, spending less on airline security in order to spend more on land and water transportation:

> Rationally, this is an easy tradeoff: less routine screening of passengers who don't call out for special attention (watch lists, travel and spending patterns, and other warning mechanisms can be improved), in exchange for more and faster work to reduce the vulnerabilities of bridges, tunnels, and ports. In wartime a commander would easily make such a decision to protect his troops. But politically this decision is almost impossible. Such a tradeoff would make it likelier that some airplane, somewhere, would be blown up. If that happened, whoever had recommended the change would be excoriated -- even if more people had been spared equally gruesome fates in subways or near ports.

And even examples of where this is already happening:

> [Terror and counter-insurgency experts] understand that this struggle will be with us for a very long time, that success will mean reducing rather than absolutely eliminating the threat of attacks, and that because there is no enemy government or army to surrender, there can be no clear-cut

> moment of victory. "Ironically, when President Bush said this in the campaign, he was immediately jumped upon," Jenkins said. "It was a moment of truth for which he was promptly punished. Senator Kerry had a similar moment, when he said that the objective was to reduce terrorism to no more than a nuisance. Conceptually that was quite accurate, even if it was not the most felicitous choice of words. And he was punished too. In a campaign with a great deal of nonsense about the threat of terrorism, these two moments of truth were mightily punished, and the candidates had to back away and revert to the more superficial and less supportable assertions."

The article goes on with some general and specific recommendations for improving the security of America against terror attacks.

The approach will be nothing new to RISKS readers, though the details may be. But I find it very hopeful that articles like this are appearing in general interest magazines rather than just specialized forums like this.

Category 4C2 *Risk management methodology & tools*

2005-02-10 **proposed legislation security measures identification authentication I&A law enforcement risk management propaganda hysteria terrorism privacy**

RISKS; http://www.house.gov/paul/congrec/congrec2005/cr020905.htm 23 71

RISK MANAGEMENT AND TERRORISM

Larry Sudduth commented in RISKS that few congresscritters (MK's word) seem to understand risk management. He was pleased to report on one who apparently does.

H.R. 418, the "Immigrants ID bill" or "REAL ID Act of 2005," is advertised in part as establishing and rapidly implementing "regulations for State driver's license and identification document security standards, to prevent terrorists from abusing the asylum laws of the United States, to unify terrorism-related grounds for inadmissibility and removal." (See http://thomas.loc.gov/cgi-bin/bdquery/z?d109:h.r.00418:)

The Honorable Dr. Paul characterizes HR 418 as a National ID Card bill masquerading as immigration reform. The clarity and brevity of his comments merit reading, both from an infosec perspective as well as a countermeasures perspective (… excerpted and LMS-ed below):

" ...this bill will do very little to make us more secure. It will not address our real vulnerabilities. It will, however, make us much less free. In reality, this bill is a Trojan horse. It pretends to offer desperately needed border control in order to stampede Americans into sacrificing what is uniquely American: our constitutionally protected liberty."

"This bill establishes a massive, centrally-coordinated database of highly personal information about American citizens: at a minimum their name, date of birth, place of residence, Social Security number, and physical and possibly other characteristics ... that will be shared with Canada and Mexico!"

"This legislation gives authority to the Secretary of Homeland Security to expand required information on drivers' licenses, potentially including such biometric information as retina scans, finger prints, DNA information, and even Radio Frequency Identification (RFID) radio tracking technology."

"There are no limits on what happens to the database of sensitive information on Americans once it leaves the United States for Canada and Mexico - or perhaps other countries. Who is to stop a corrupt foreign government official from selling or giving this information to human traffickers or even terrorists? Will this uncertainty make us feel safer?"

Security practitioners know better than most the aptness of the saying, "err in haste, repent at leisure." I hope Representative Paul's common-sense proves to be contagious before HR 418 comes to a floor-vote.

Category 4C2 *Risk management methodology & tools*

2005-03-04 **nuclear power plant information security digital systems SCADA government regulations standards industry protest obstruction denial**

RISKS; http://www.securityfocus.com/news/10618?ref=rss 23 78

SECURITY? NUCLEAR PLANTS DON'T NEED NO STINKIN' SECURITY!

Jim Horning relayed a discussion of nuclear power industry opposition to proposals for improved cyber security in nuclear generator plants.

"Two companies that make digital systems for nuclear power plants have come out against a government proposal that would attach cyber security standards to plant safety systems. The 15-page proposal, introduced last December by the U.S. Nuclear Regulatory Commission (NRC), would rewrite the commission's 'Criteria for Use of Computers in Safety Systems of Nuclear Power Plants.' The current version, written in 1996, is three pages long and makes no mention of security. The plan expands existing reliability requirements for digital safety systems, and infuses security standards into every stage of a system's lifecycle, from drawing board to retirement. Last month the NRC extended a public comment period on the proposal until March 14th to give plant operators and vendors more time to respond. So far, industry reaction has been less than glowing."

"The NRC tries to promote the use of digital technology in the nuclear power industry on the one hand, but then over-prescribes what is needed when a digital safety system is proposed," wrote one company president.

"The entire cyber security section should be deleted and only a passing reference to the subject retained," another company wrote.

More information at
http://www.securityfocus.com/news/10618?ref=rss and
http://horning.blogspot.com/2005/03/security-nuclear-plants-dont-need-no.html

Category 4C2 *Risk management methodology & tools*

2005-03-07 **airport safety false sense security identification authentication counter-terrorism failure fraud propaganda illusion**

RISKS; http://www.nytimes.com/2005/03/06/magazine/06ADVISER.html 23 78

AIRPORT SECURITY CHECK OF LICENSES A FARCE

John F. McMullen provided this abstract of an article by Richard A. Clarke, former counter-terrorism adviser on the U.S. National Security Council that was published in the New York Times:

Have you ever wondered what good it does when they look at your driver's license at the airport? Let me assure you, as a former bureaucrat partly responsible for the 1996 decision to create a photo-ID requirement, it no longer does any good whatsoever. The ID check is not done by federal officers but by the same kind of minimum-wage rent-a-cops who were doing the inspection of carry-on luggage before 9/11. They do nothing to verify that your license is real. For $48 you can buy a phony license on the Internet (ask any 18-year-old) and fool most airport ID checkers. Airport personnel could be equipped with scanners to look for the hidden security features incorporated into most states' driver's licenses, but although some bars use this technology to spot under-age drinkers, airports do not. The photo-ID requirement provides only a false sense of security.

Category 4C2 *Risk management methodology & tools*

2005-03-12 **risk management assessment professionals credentials credibility software quality assurance QA**

RISKS 23 79

NEED PROFESSIONAL RISK ASSESSMENT TO IMPROVE SYSTEMS

Jack Goldberg published a thoughtful essay about risk management in RISKS:

Risks associated with developing and using computer systems have been documented widely (e.g., by PGN) and have become part of popular awareness. Economic costs resulting from these risks are huge, though presently unquantified. They include the costs of system failures, abandoned system developments, and lost opportunities to build valuable systems whose complexity is deemed beyond present art.

Despite the widespread awareness of this situation, nothing fundamental has been done to change it. New system technologies attempt to improve matters by giving system builders better tools. Large corporate and government initiatives to improve system trustworthiness have been announced. Despite many advances, system development risks have not abated. New systems keep getting developed whose defects are discovered too late to be repaired economically. Repairs become patches and basic defects remain embedded in the system. These problems are pervasive, both in safety and infrastructure-critical applications and in the mundane data-processing applications that support the national economy.

With all the awareness of the hazards of system building, why does this bad situation continue? We suggest that the reason is the weakness of current risk assessment for new systems. Warnings about computer system risks that are given in an early stage do not have the force of warnings in other disciplines such as medicine and civil engineering and so they are ignored or discounted.

What can be done to improve the believability of warnings about development hazards? We do not envision a super-powerful tool that can generate a high-confidence hazard assessment for all situations. Rather we see the need for a profession of hazard auditors who have earned acceptance based on their scientific skills and experience. The need for their skills should be assumed and demanded in all system development efforts. Their observations (and if necessary, testimonies) should be communicated to purchasers, builders and users. Tools should be developed to support their analyses.

Building such a profession would be a substantial effort but the effort would surely be justified by the enormous cost of current development deficiencies. Government agencies, corporations, universities and professional associations all have clear roles to perform.

Category 4C2 *Risk management methodology & tools*

2005-12-06 **terrorism threat counter-terrorism watch lists mistakes US DHS errors risk false positives identification authentication I&A**

RISKS; http://tinyurl.com/chvdq 24 11

HASSLES OF TERRORIST WATCH LISTS

Contributor Richard M. Smith documents a CNET news article bemoaning the hassles of being placed on a terrorist watch list. Nearly 30,000 airline passengers found out in 2004 that they were on such lists. The article continued:

>Jim Kennedy, director of the Transportation Security Administration's redress office, revealed the errors at a quarterly meeting convened here by the U.S. Department of Homeland Security's Data Privacy and Integrity Advisory Committee.

Marcia Hofmann, staff counsel at the Electronic Privacy Information Center, said this appeared to be the first time such a large error has been admitted. "It was a novel figure to me," Hofmann said. "The figure shows that many more passengers than we've anticipated have encountered difficulty at airports. The watch list still has a long way to go before it does what it's supposed to do."

Kennedy said that travelers have had to ask the TSA to remove their names from watch lists by submitting a "Passenger Identity Verification Form" and three notarized identification documents. On average, he said, it takes officials 45 to 60 days to evaluate the request and make any necessary changes.

Travelers have been instructed to file the forms only after experiencing "repeated" travel delays, he said, because additional screening can occur for multiple reasons, including fitting a certain profile, flying on a one-way ticket, or being selected randomly by a computer.<

Category 4C2 *Risk management methodology & tools*

2005-12-19 **UK psychology professor James Reason absent-mindedness risk management interview ABC**

RISKS; http://abc.net.au/rn/podcast/feeds/health_20051219.mp3 24 13

PSYCHOLOGY PROF. INTERVIEW ABOUT RISK MANAGEMENT

Contributor James Cameron refers us to a valuable interview of James Reason, Emeritus Professor of Psychology at University of Manchester (UK). Prof. Reason talks about:

* Absentmindedness,
* the Tenerife disaster (1977, two Boeing 747s collide),
* no remedial benefit from blame,
* root cause analysis,
* the Gimli Glider.

Mr Cameron writes, "Here is an interview that is very suitable for passing on to your non-technical friends who don't understand why you are so morbidly fascinated with risks."

Interview transcript: http://www.abc.net.au/rn/talks/8.30/helthrpt/stories/s1529677.htm

4C3 Certification of site security, privacy protection

Category 4C3 *Certification of site security, privacy protection*

2001-12-14 **Web site health information privacy security accreditation certification**

NewsScan

HEALTH SITES GET ACCREDITATION FROM STANDARDS GROUP
The American Accreditation Health Care Commission has put the stamp of its approval on 13 online health-care sites, the first such sites to earn AAHCC accreditation. AAHCC sets quality standards for managed-care and other health-care programs. The move is aimed at helping people sort out good information from bad in the health care field, which has become a popular area of online research among consumers. "There is so much bad information on the Internet, especially about health-care content," said Kevin Noland, COO of A.D.A.M., one of the sites to earn accreditation this week. "Someone needs to set a standard so people feel they are getting information from a trusted source." Standards for approval include full disclosure about funding and advertising, quality of editorial content, linking to other sites, and privacy and security. Other accredited sites include WellMed, WebMD and Health Insurance Association of America. (Wall Street Journal 14 Dec 2001)
http://interactive.wsj.com/articles/SB1008284518346277800.htm

---

Category 4C3 *Certification of site security, privacy protection*

2002-02-04 **Web security certification consumer guidance**

NewsScan

BETTER BUSINESS BUREAU TARGETS ONLINE PRIVACY WITH NEW SITE
The Better Business Bureau has launched a new Safe Shopping Web site that enables consumers to locate online companies that have met BBB standards for privacy in e-commerce. Visitors to
http://www.bbbonline.org/consumer/ will find nearly 11,000 Web sites that have earned one or both of the BBBOnline Privacy and Reliability seals. A recent survey showed that almost 90% of consumers would feel safer making a purchase from an online company that displays one of the seals than from a company that does not, according to Greenfield Online. "The BBB system will encourage the business community to step up to the plate and meet consumer expectations regarding online privacy," says Ken Hunter, president and CEO of the Council of Better Business Bureaus and BBBOnline. (E-Commerce Times 4 Feb 2002)
http://www.ecommercetimes.com/perl/story/16149.html

Category 4C3 *Certification of site security, privacy protection*

2003-08-13 **NIST IT security metrics National Institute Standards Technology policy Self-Assessment Guide Systems 800-26 800-55**

NIPC/DHS

August 13, Government Computer News — NIST releases guidelines for IT security metrics.

The National Institute of Standards and Technology (NIST) has released its final version of guidelines for developing metrics to help ensure agencies meet IT security requirements. Metrics-measurable standards-monitor the effectiveness of goals and objectives established for IT security. They measure the implementation of security policy, the results of security services and the impact of security events on an agency's mission. The publication uses the critical elements, and security controls and techniques laid out in an earlier NIST publication, 800-26, Security Self-Assessment Guide for IT Systems. NIST Special Publication 800-55, Security Metrics Guide for IT Systems is available online
http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf

---

Category 4C3 *Certification of site security, privacy protection*

2003-11-20 **Congress cyber security cyberspace report FISMA**

NIPC/DHS

November 19, Government Computer News — Congress plans report cards on cybersecurity.

On the heels of Office of Management and Budget efforts over the past year to boost cybersecurity, lawmakers are set to weigh in on agency progress. The House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census next month will issue a cybersecurity report card detailing agency progress in meeting the requirements of the Federal Information Security Management Act (FISMA). The subcommittee has been working to focus the legislative and executive branches on the importance of cybersecurity with a variety of hearings over the past year. Subcommittee staff director Bob Dix, speaking Wednesday, November 19, at the Enterprise Architecture 2003 Conference in Washington D.C. said the subcommittee also plans to explore whether the federal procurement process can be used to improve software security. "If we use the purchasing power of the federal government to insist that developers provide more secure products, that will benefit all users in both the public and private sectors," he said.

4C4 Professional certification in security, auditing

Category 4C4 *Professional certification in security, auditing*

2004-09-01 **information technology IT users United Kingdom UK IA security staff certification financial corporate auditing regulations**

DHS IAIP Daily; http://www.computing.co.uk/news/1157762

September 01, Computing (UK) — IT users seek to certify security.

IT security experts from some of the UK's most influential businesses are meeting this week to try to establish a professional body for certifying information security staff. The group, which includes the Royal Bank of Scotland, Royal Mail and BP, will meet with The Information Security Forum, in an attempt to create an industry body which links financial and IT security needs. David Lacey, Royal Mail director of information security, told Computing that the group hopes to establish codes of conduct and professional certification for IT security staff, to ensure compliance with growing corporate financial auditing regulations. Following the meeting, the group will expand its plans for security standards, benchmarking, business processes and vendor management. Lacey expects to produce a report before the end of October to share with IT suppliers.

Category 4C4 *Professional certification in security, auditing*

2004-10-18 **certification Australia ACS accreditation agency IT profession mandatory membership**

NewsScan; http://australianit.news.com.au/articles/0

ACS PUSHES OWN IT 'LICENSE'

The Australian Computer Society (ACS) has called on government to support its bid to become the accreditation agency for the IT profession, making membership mandatory for computer staffers ranging from Microsoft Certified Engineers to high-level project managers. ACS president Edward Mandla also called for state and federal governments to assist in funding Australian companies seeking to acquire quality assurance certification like CMMI and ISO 15504. Mandla announced the ACS software quality accreditation policy in an address to the Software Industry Action Group conference, being hosted by Software Engineering Australia (SEA) in Melbourne.

4C5 Academic/Industry/Vendor/Govt efforts

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2002-02-23 **hardware software integration identification authentication I&A BIOS firmware biometric fingerprint recognition digital certificate root key**

NewsScan

THE MARRIAGE OF HARDWARE AND SOFTWARE SECURITY
A number of technology companies are introducing new products that embed security features inside computer hardware, to add to the protections offered by software alone. IBM and Targus Systems have developed a new biometric fingerprint reader that's built into a PC card inserted into the new IBM ThinkPad laptops, and another example of the trend is the announcement that VeriSign's "root key" software will be put into the next version of Phoenix Technology's BIOS (i.e., its basic input-output software), so that no one but an authorized user can be authenticated on the computer. (Reuters/San Jose Mercury News 23 Feb 2002)
http://www.siliconvalley.com/mld/siliconvalley/2734756.htm

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2002-04-08 **Microsoft orientation security priority policy statement features**

NewsScan

MICROSOFT SAYS SECURITY IS JOB #1
In January Microsoft chairman and cofounder Bill Gates instructed the company to shift its priority from adding new software features to ensuring that its software is secure, and in the months since then the company's software designers have been reexamining the millions of lines of Windows operating system software, looking for security vulnerabilities. Rebecca Bace, a security consultant who has been critical of Microsoft, comments: "I think that the reason that people are upset with them is the perception that Microsoft will always choose the extra feature, begging the issue of whether that feature is actually of high value to the user and damning the security impact it might represent to all users." But Microsoft security expert Michael Howard insists that, if that was ever true, it's definitely not true since Gates called for a new company-wide emphasis on security as the number one priority: "Microsoft has always had a crisis-driven mentality. You have my word: we will lead the industry in delivering secure software." (New York Times 8 Apr 2002)
http://partners.nytimes.com/2002/04/08/technology/ebusiness/08SOFT.html

---

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2002-04-22 **management promotions publicity policy visibility**

Security Wire Digest 4 31

*SUN TAKES ANOTHER STEP TOWARD INCREASED SECURITY
Sun Microsystems last Thursday announced it had filled its two newly created security positions. Public key encryption inventor Whitfield Diffie was appointed chief security officer, but has been Sun's security expert since 1991. Sun also appointed Joanne Masters director of Sun's Global Security Program Office. Among her chief responsibilities are driving initiatives related to increasing Sun's presence on security issues. Sun says the positions are intended to further its development of secure information technology products and services.
http://www.sun.com/smi/Press/sunflash/2002-04/sunflash.20020417.2.html

---

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2002-05-20 **SSC consortium industry government security quality assurance QA reliability trustworthiness**

Security Wire Digest 4 39

In mid-May 2002, Carnegie Mellon University announced the formation of the new Sustainable Software Consortium (SSC), with membership including Microsoft, Cisco Systems, Pfizer, AIG and NASA and open to other industry and government participants. Cheryl Balian wrote for Security Wire Digest, "[T]he group will research and assess computer failures, which costs U.S. companies $100 billion per year, according to SCC research. The work of the consortium will include '...technical efforts to measure and reduce software-associated risks as well as economic, legal and policy efforts to manage risk within organizations, the broader markets and the national economy,' the group says. The SCC will also consider the feasibility of establishing widely accepted security standards for the software industry."

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2002-05-28 **homeland security biometrics surveillance privacy**

NewsScan

SECURITY-INDUSTRIAL COMPLEX
George Washington University law professor Peter Swire calls it "a new security-industrial complex," alluding to the phrase "military-industrial complex" made famous in President Eisenhower's Farewell Address. Swire says that industry is looking at homeland security needs as a lifeline for getting out of the recession, and here are some of the many security technologies now being marketed: a variety of automatic face-recognition systems; electronic body scanners that see through clothing to detect weapons; biometric cards with embedded computer chips containing personal ID data, fingerprints, or retinal scans; databases of "trusted travelers" who could avoid long security lines at airports; and links between passenger reservation systems to other government and private databases. Privacy advocates continue to express their concerns that some of these technologies intrude too much on individual privacy. (San Jose Mercury News 27 May 2002)
http://www.siliconvalley.com/mld/siliconvalley/3349627.htm

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2002-06-27 **PC security architecture announcement planning**

RISKS, http://www.ntsecurity.net/Articles/Print.cfm?ArticleID=25681 22 13

From an article in NTsecurity.net:

You've heard of Trustworthy Computing, and the massive corporate remodeling going on at Microsoft where every developer, product manager, and executive assistant has been asked to rethink everything they do in the context of security. Well, that's just the tip of the iceberg. Secretly, the company has been working on a plan to rearchitect the PC from the ground up, to address the security, privacy, and intellectual property theft issues that dog the industry today. Inexplicably, the company pulled an Apple and chose to detail its plans solely to Newsweek, so we only have that one report to work from. But if Newsweek's take on the plan is correct, and consumers and businesses buy into the new devices that would result, the PC landscape will soon change forever. [...]

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2003-01-10 **report INFOSEC standards US federal government infrastructure protection**

NIPC/DHS

January 09, Federal Computer News — Council offers vision for infosec standards.

President Bush's private-sector infrastructure protection advisory council agreed January 8 that the federal government should encourage the development and use of open standards in the market instead of dictating specific standards. But federal officials should also use the government's significant buying power to push for interoperability in those market standards and solutions that will raise the baseline of security across all sectors. The National Infrastructure Advisory Council's report will go to the president later this month along with a revised National Strategy to Secure Cyberspace, said Richard Clarke, chairman of the President's Critical Infrastructure Protection Board. The recommendations fall in line with the approach taken by the Bush administration in its draft cybersecurity strategy, which the White House released in September 2002 for comment. Revisions proposed by Clarke's office include setting specific priorities, such as taking a closer look at the Common Criteria security product certification program. Later this month, the council plans to meet again to look at other infrastructure protection issues, including the international migration to Version 6 of the Internet Protocol and developing a systematic vulnerability assessment program for private-sector infrastructure.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2003-01-16 **Microsoft international governments access secret code security testing Russia NATO**

NIPC/DHS

January 15, New York Times — Microsoft to give governments access to code.

Microsoft announced today that it will allow most governments to study the programming code of its Windows systems. Under the program, 97 percent of the code to Windows desktop, Windows server and Windows CE hand-held software will be available to governments online for inspection and testing. To view the other 3 percent - the most sensitive technology - government representatives must come to Microsoft headquarters in Redmond, WA. Governments will also be allowed to plug their security features instead of Microsoft's technology into Windows. More than two dozen countries are encouraging agencies to use "open source" software - developed by programmers who distribute the code without charge and donate their labor to debug and modify the software cooperatively. The best-known of the open source projects is GNU Linux, an operating system that Microsoft regards as the leading competitive threat to Windows. One appeal of Linux is that developers have complete access to the underlying source code, whereas Microsoft has kept some Windows technology secret. Microsoft expects that perhaps 60 foreign governments and international agencies will eventually join its government security program. The first to join were Russia and the North Atlantic Treaty Organization, and the company is negotiating with 20 other groups.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2003-02-03 **cyber security agenda research development**

NIPC/DHS

January 31, Federal Computer Week — Cybersecurity RD agenda unveiled.

The Institute for Information Infrastructure Protection (I3P) has unveiled its 2003 Cyber Security Research and Development Agenda, which identifies critical areas that require significant research and development to help secure the nation's information infrastructure. The agenda, announced January 30, outlines eight crucial RDgaps that are not being sufficiently addressed by ongoing government, private-sector or academic research: 1) Enterprise security management; 2) Trust among distributed autonomous parties; 3) Discovery and analysis of security properties and vulnerabilities; 4) Secure system and network response and recovery; 5) Traceback, identification and forensics; 6) Wireless security; 7) Metrics and models; 8) Law, policy and economics. The I3P, a consortium of 23 leading cybersecurity research institutions from academia, national labs and nonprofit organizations, is funded by the Commerce Department and the National Institute of Standards and Technology. The agenda will help the White House's Office of Science and Technology Policy better coordinate RDefforts across government agencies, said Susan Hays, deputy associate director for technology at the office. I3P received input, gathered over nine months in 2002, from more than 900 experts and security professionals from the private sector, academia and government, said Michael Vatis, chairman of I3P.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2003-03-18 **best security practice report Telecom NRIC FCC infrastructure**

NIPC/DHS

March 14, Government Computer News — Telecom advisory group finishes work on best security practices.

The Network Reliability and Interoperability Council (NRIC) completed work Friday on a set of best practices to ensure the security and availability of the nation's communications infrastructure. During its quarterly meeting, industry working groups chartered by the Federal Communications Commission (FCC) presented 162 recommendations for steps to be taken by network operators, manufacturers and service providers to help with service restoration in the event of man-made or natural disruptions. The recommendations will be voted on by the entire council by March 28. NRIC was created as an industry advisory committee in 1992, and received its most recent charter from FCC chairman Michael Powell in January 2002. NRIC VI focuses on homeland security and was charged with coming up with a set of voluntary best practices for network security and survivability. Approval of recommendations made Friday would complete the first phase of the council's current work. The second phase is education and outreach to encourage use of the best practices. Practices recommended for adoption Friday focus on restoring service after attacks on or damage to physical or cyber links.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2003-04-11 **Microsoft source code partner access shared debug test secure**

NIPC/DHS

April 10, New York Times — Microsoft to allow partners to alter some source code.

Microsoft announced Wednesday that it would allow its industry partners to modify and then redistribute the underlying programming code used in cellphones, hand-held computers, television set-top boxes and other small devices. The new policy does not apply to Microsoft's mainstay products in personal computer desktop software and data-serving software that runs computer networks. According to analysts, the move shows that even Microsoft must respond, at least in markets it does not dominate, to the changed attitudes and practices in the software industry prompted by the rise of "open source" software - software developed by programmers who distribute the code without charge and then cooperatively debug, modify and add improvements to the software. Microsoft does not embrace the open source formula as a way of doing business. But the company is selectively borrowing some of the open source practices for the way it develops software. It is doing so mainly in response to the growing popularity of the best-known open source project, the GNU Linux operating system, a competitor to Microsoft's Windows. Microsoft rivals like IBM and Oracle are promoting Linux. Microsoft calls its approach the Shared Source Initiative, which it began nearly two years ago.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2003-04-16 **Open Security Exhange group Computer Associates security standards specifications implementation**

NIPC/DHS

April 14, eWEEK — Companies form Open Security Exchange.

Computer Associates International Inc. (CA) and several other companies announced Monday the formation of a group that is working to define and implement open specifications and best practices for integrating information security and physical security. The group plans to submit the specifications to an industry standards body, but has yet to decide which one it will approach with the idea. The Open Security Exchange grew out of CA's own efforts to integrate the management of network and physical security within large enterprises. The announcement of the group's formation came at the RSA Conference in San Francisco. Among the specific problems that the new group plans to address initially are audit and forensics, authentication, and centralized provisioning. Whether competitors and large companies from disparate industries can work together to make the idea work remains to be seen. The group's specification is available on its Web site, which is http://opensecurityexchange.com.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2003-04-17 **e-government legislation bureaucracy services IT**

NewsScan

E-GOV
In implementing the E-Government Act of 2002, the Bush Administration is creating an Office of Electronic Government within the White House. A main mission of the E-Gov office will be to make it easier for citizens to apply for government services and to obtain information from federal agencies; other goals will be to reduce bureaucratic redundancies by providing better coordination and oversight of money being spent by federal agencies on information technology. (San Jose Mercury News 17 Apr 2003)

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2003-04-17 **industry vendor TechNet alliance security standards specifications**

NIPC/DHS

April 15, CNET News.com — Alliance takes security call to boardroom.

TechNet, a lobbying group of more than 150 information technology companies, said Tuesday that it would work with the Internet Security Alliance and the four large accounting firms to create guidelines and best practices that they say executives need in order to secure their companies. The accounting firms are KPMG, PricewaterhouseCoopers, Deloitte & Touche and Earnst & Young. The starting point will be a top-10 list of security steps for executives that the Internet Security Alliance has already created. "We wanted to aim at the top because we believe that at the top, with boardroom involvement and (policy) trickling down, we can get the best results," said John Shaughnessy of the Internet Security Alliance. President George W. Bush in February 2003 said the United States government would not regulate technology companies, but rather would promote cooperation between the industry and the government to secure infrastructure. The groups plan to release the guidelines and then to set a date by which its membership should comply with the security steps.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2003-04-22 **Indiana Purdue University cybersecurity center information assurance security research studies**

NIPC/DHS

April 18, Associated Press — Law professor will head university's cybersecurity center.

Indiana University (IU) law professor Fred Cate will be the inaugural director of the Center for Applied Cybersecurity Research which will research computer and Internet security issues. Cate, an expert on privacy and information law, said the center will encourage university partnerships with businesses and with federal and state government agencies. IU created the center with $125,000 from a private donor and a matching amount from its own funds, said Michael McRobbie, IU's vice president for information technology and chief information officer. He said the center will be based both in Bloomington and at Indiana University-Purdue University at Indianapolis. It will bring together university staff with computer-security duties - from information technology, legal, audit and police departments - with faculty performing research related to cybersecurity, he said.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2003-04-23 **cyber risk e-crime cyber sabotage Australia companies share information protect infrastructure**

NIPC/DHS

April 22, The Australian — Austrialian business called on to fight cyber risks.

Australian companies are being asked to share information freely in order to defeat threats ranging from cyber-sabotage to e-crime. "If just one part of the economy is attacked, the repercussions are likely to be felt by all sectors and all businesses," Attorney-General Daryl Williams told business representatives at the launch of the Trusted Information Sharing Network (TISN) in Melbourne this month. Businesses often view infrastructure protection as a government problem, according to Tom Patterson of Deloitte & Touche Security. "If you look at what runs the economy, it's not your government, it's your companies. Every company has an obligation to protect its business not only for its stakeholders and its shareholders but also for the economy as a whole," he says. The government hopes TISN will become a forum for open exchange of information about system attacks and vulnerabilities, as well as protection of key sites from cyber-sabotage. A Critical Infrastructure Advisory Council will be set up to oversee efforts in various industry sectors as well as developing strategies for business continuity and consequence management.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2003-07-25 **Microsoft integrated security Windows Office R&D**

NewsScan

MICROSOFT PROMISES 'INTEGRATED INNOVATION'
Microsoft plans to increase its R&D spending this year by perhaps 8%, to a total of $6.9 billion, and to expand its work force by 4,000 to 5,000 positions during the current fiscal year. Disputing recent pronouncements by others, Microsoft co-founder and chairman Bill Gates says that that the computer industry is far from being in decline or in a state of rapid consolidation: "The debate about what came out of the boom and what these information technology investments mean has really gotten fairly extreme. Obviously we put our money where our beliefs are in saying we disagree with all of this." And Microsoft's business strategy at this point in time? "Integrated innovation" that will give the company's Windows and Office software customers a continuous stream of features and service. Gates says, "It shouldn't be necessary for people to buy additional products for their secure infrastructures." (New York Times 25 Jul 2003)

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2003-10-22 **Carnegie Mellon lab cyber-security engineering technologies new CERT Internet Explorer CyLab education research**

NIPC/DHS

October 22, eWEEK — Carnegie Mellon lab tackles cyber-security.

Security, engineering and public policy experts at Carnegie Mellon University are joining together to form a new lab at the school dedicated to researching and developing new security technologies. The new organization, known as the Carnegie Mellon CyLab, will include representatives from the school's engineering, computer science and public policy departments, as well as personnel from the CERT Coordination Center. The group will seek to promote collaboration between the government and the private sector. CyLab's charter will differ significantly from that of CERT, which is charged with analyzing and responding to security threats and attacks. A quasi-public organization, CERT is partially funded by the federal government. CyLab will also receive public money, but will concentrate on finding long-term solutions to pervasive security problems instead of looking at how to mitigate the latest attack on Internet Explorer, as CERT does. The group's mission is essentially threefold: education; research and development; and response and prediction. In addition to offering bachelor's, master's and doctorate degrees in security-related disciplines, CyLab will also work to educate home users on the inherent dangers of the Internet and the steps they can take to combat those issues.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2003-10-24 **Iowa State University fight hackers ISEAGE Internet laboratory**

NewsScan

SECURITY PROJECT AT IOWA STATE
Iowa State University researchers are creating a laboratory to fight computer hackers. The project, which is being funded by a $500,000 grant from the U.S. Justice Department, will allow ISU to develop what it calls Internet-Scale Event and Attack Generation Environment (or ISEAGE, pronounced ice age), which is designed to allow realistic tests of security defenses. Computer scientist Doug Jacobson explains: "Since we can't take over the real Internet, we've decided to recreate our own Internet laboratory. We will be able to carry out computer attacks exactly as they happen in the real world." (AP/USA Today 24 Oct 2003)

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2003-11-14 **technology security alliance chief security officer importance Internet**

NIPC/DHS

November 12, Washington Post — Tech security chiefs form alliance.

Nearly a dozen top technology luminaries are lending their star power to a new think-tank that will look for ways to elevate the status of chief security officers in the private sector, a move that they say will go a long way toward improving Internet security. The Global Council of Chief Security Officers was formed by former White House cybersecurity adviser Howard Schmidt. The council will consult with technology vendors and industry groups to help design more secure products for the next generation of the Internet, Schmidt said. MCI's Vint Cerf said that the council should also encourage more compatibility between different and competing technologies. Failure to do so, especially as the Internet grows into even more of a commercial medium, could prove damaging to online networks. The council will hold its first meeting in San Jose in January and a CSO summit in San Francisco the following month. U.S. CERT, a new partnership between the Department of Homeland Security and the CERT Coordination Center—a government funded security watchdog group at Carnegie Mellon University in Pittsburgh—will oversee the council's day-to-day activities. The council is on the Web at:
http://www.csocouncil.org

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2003-11-19 **cyber security summit US CERT education strategy secure cyberspace**

NIPC/DHS

November 17, US-CERT — US-CERT announces the National Cyber Security Summit.

The National Cyber Security Summit, to be held December 3 in Santa Clara, CA, is the first of a series of invitational events focusing on Internet security. Invited delegates to this one-day summit may serve on one of the five cross-sectoral task forces, which will be responsible for recommending solutions to the challenges posed in the President's National Strategy to Secure Cyberspace. The five task forces, which will be sponsored by the private sector, are: Awareness for Home Users and Small Businesses, Cyber Security Early Warning, Best Practices and Standards: Corporate Governance, Best Practices and Standards: Technical Standards and Common Criteria, and Security Across the Software Development Life Cycle: Secure Software.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2003-12-04 **government official security summit Department Homeland Security DHS cooperation public private sector**

NIPC/DHS

December 02, CNET News.com — Government officials join security summit.

Silicon Valley executives are slated to meet on Wednesday , December 4, with top bureaucrats from the Department of Homeland Security (DHS) to hammer out ways that the private sector can work with government to enhance national security and avoid creating regulations. The National Cyber Security Summit will bring together top executives at security and technology companies with policy-makers. Corporate leaders are expected to announce several new task forces and initiatives aimed at making information security a boardroom issue. The gathering comes nine months after the Bush administration unveiled its plan to secure the Internet through cooperation instead of regulation. It also comes just in time to stiffen opposition to a bill that would require companies to reveal the results of a security audit in their financial reports. The meeting, which will be held at the Santa Clara Marriott, will try to convince government officials that security-savvy organizations can teach industry executives to consider information security at the boardroom level. The meeting will establish at least three task forces, including the Corporate Governance Task Force, the CEO Cyber Security Task Force, and the Technical Standards and Common Criteria Task Force.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2003-12-05 **industry security tools software release cyber summit GISRA FISMA**

NIPC/DHS

December 04, — Industry groups release security tools.

A pair of information technology industry groups unveiled security assessment tools at this week's National Cyber Security Summit in Santa Clara, CA. TechNet, an association of chief executive officers (CEO) and other senior executives, unveiled its Corporate Information Security Evaluation tool, which takes CEOs, chief information officers, and chief security officers through 88 points on risk management, people, processes, and technology. The Information Technology Association of America, in partnership with the Marshall School of Business at the University of Southern California, announced its Cyber Security Assessment, which will build on information provided by the TechNet evaluation. The key is performing both assessments regularly and measuring progress at every step, said Harris Miller, president of ITAA. Both tools drew from the government's recent experience with self-assessments under the Government Information Security Reform Act (GISRA) of 2000 and the Federal Information Security Management Act (FISMA) of 2002, said Art Coviello, co-chairman of TechNet's Cyber Security CEO Task Force. There, the focus also was on repeated measurements to identify shortcomings and demonstrate improvement or regression, he said.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2003-12-16 **National Science Foundation NSF program secure computer network**

NIPC/DHS

December 15, Government Technology — NSF announces $30 million program. To promote research into more dependable, accountable and secure computer and network systems, the National Science Foundation (NSF) has issued a solicitation for the Cyber Trust program, which expects to fund up to $30 million in awards. The Cyber Trust program will support up to three research center-level efforts as well as single-investigator and team awards, subject to NSF's merit-review process and the availability of funds. The Cyber Trust program is seeking innovative proposals in three broad areas: fundamental research, multi-disciplinary research, and education and workforce development. Fundamental research is needed to advance the state of the art in knowledge and technology about trustworthy computing. This covers such areas as security and privacy models and metrics, evaluation and certification methods, denial-of-service prevention, long-lived data archiving methods, privacy protection, and network and application forensics. Multi-disciplinary research is needed to improve understanding of the social, legal, ethical and economic trade-offs that affect the design and operation of trusted information systems. Additional information is available online:
http://www.nsf.gov/pubs/2004/nsf04524/nsf04524.htm

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2004-02-25 **computer security firms alliance secure US communication networks**

NewsScan

COMPUTER SECURITY FIRMS FORM NEW ALLIANCE

Eleven top U.S. computer security firms have banded together to form the Cyber Security Industry Alliance, a lobbying group that hopes to work cooperatively with Congress to come up with a plan for securing the nation's electronic communications networks. "Rather than saying to Congress, 'This is not an issue, stay out,' we as an industry need to figure out how to solve thee problems in a proactive way before someone gets fed up and says it's time to legislate," says Sanjay Kumar, CEO of Computer Associates. One of the Alliance's first tasks will be to develop common standards for reporting and sharing information on Internet security threats. Former White House technology adviser Richard Clarke says the proliferation of malicious worms and viruses in 2003 has fueled demand for action: "Last year was the worst in history in terms of the damage from cyber-attacks. I think we're getting to the point where Congress wants something to happen, the people and American corporations that buy information technology want something to happen, and so having the technology security industry organized to be part of that debate makes a lot of sense." Other companies involved in the Alliance include: Bindview Corp., Check Point Software Technologies, Netscreen Technologies (a subsidiary of Juniper Networks), PGP Corp., RSA Security and Secure Computing Corp. (Washington Post 25 Feb 2004)

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2004-03-18 **cybersecurity network US National Partnership**

NewsScan

PROPOSED CYBERSECURITY NETWORK

The National Cyber Security Partnership (which includes the U.S. Chamber of Commerce, the Business Software Alliance and the TechNet lobbying group) is asking Congress for money to create a cybersecurity information clearinghouse for the business community. The group's recommendations include development of a "Home User Cyber Security Tool Kit" and the designation of a "cyber security month." The clearinghouse would be known as the "National Crisis Coordination Center." (Washington Post 18 Mar 2004)

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2004-04-01 **softeware industry acknowledges network security Bush administration**

DHS IAIP Daily;
http://www.cnn.com/2004/TECH/internet/04/01/cybersecurity.ap /index.html

April 01, Associated Press — Software industry makes room for government.

In a surprise shift, leading software companies acknowledge in a report to the Bush administration that the government might need to force the U.S. technology industry to improve the security of America's computer networks. The companies, including Microsoft Corp. and Computer Associates International Inc., said the Homeland Security Department "should examine whether tailored government action is necessary" to compel improvements in the design of computer software. The 250-page report containing that recommendation and dozens more was being released Thursday, April 1. It cautioned that government should require security improvements only when market forces fail. It also said businesses already are demanding software that is safer and more resilient to attacks. But the report said the most sensitive computer networks -- such as those operating banks, telephone networks or water pipelines -- "may require a greater level of security than the market will provide." In those cases, the software companies recommend "appropriate and tailored government action that interferes with market innovation on security as little as possible." It urged the government to work with companies to produce a formal study during the 2005 fiscal year, which begins in October.

Category 4C5 Academic/Industry/Vendor/Govt efforts

2004-04-01 **computer crime vandalism government role reduction**

NewsScan

FIGHTING COMPUTER MISCHIEF

An industry task force is advising the federal government to set goals for reducing hacking, spam, worms, viruses and identity fraud -- though the group has refrained from offering specific measures. Indicating the need for the federal government to play a stronger role in computer security issues, the report calls for increased funding for cyber-security research at universities; improved university certification programs that stress security training for engineers; and a Department of Homeland Security evaluation of software vulnerabilities. Alan Paller of the SANS Institute, a computer-security research group, is critical of the report: "What we got was not solutions, but a description of the problem," in which "there's nothing about the companies that make billions of dollars selling this broken stuff." Task Force co-chairman Ron Moritz of Computer Associates insists: "We're far from doneMoritz says executives will have to go back and tell their programmers: "You've been doing this wrong for the past 25 years." (Washington Post 1 Apr 2004)

Category 4C5 Academic/Industry/Vendor/Govt efforts

2004-04-06 **industry security improvements cybersecurity recommendations corporate practice**

DHS IAIP Daily; http://www.fcw.com/fcw/articles/2004/0405/web−putnam−04 −06−0 4.asp

April 06, Federal Computer Week — Industry suggests security improvements.

The Corporate Information Security Working Group, which Rep. Adam Putnam (R-FL) convened five months ago, issued several lists of cybersecurity recommendations that Putnam has promised to review before considering any new security legislation on Tuesday, April 6. Most of the recommendations from the group's call on the federal government to provide incentives for good corporate security practices, but they reject any substantial role for the federal government in policing the information security practices of corporations. The group made recommendations on best practices, education, incentives, information sharing and procurement practices. One recommendation was to amend the Clinger-Cohen Act of 1996 to require that federal agencies include computer information security in making IT strategic plans and spending decisions. The recommendations are available online: http://reform.house.gov/TIPRC/News/DocumentSingle.aspx?Docum entID=3030

Category 4C5 Academic/Industry/Vendor/Govt efforts

2004-05-18 **data sharing government portal**

DHS IAIP Daily; http://fcw.com/fcw/articles/2004/0517/web−irish−05−18− 04.asp

May 18, Federal Computer Week — When Irish eyes are sharing.

Using a central portal for citizen services, Irish officials are allowing agencies to share information while ensuring that agencies retain their autonomy. "The idea is agencies don't talk directly to each other," said Sean McGrath, chief technology officer of business integration company Propylon, 11 speaking Monday, May 17 on a panel at the CIO Summit. "They talk to a single hub." That hub is at the heart of the Public Services Broker, which provides citizens with a single point of access to government services and allows for data sharing governmentwide. Rather than share information directly, agencies provide data to a central location, which packages and disseminates the requested information. This approach is faster and cheaper than distributed architectures and allows for flexibility and ownership among agencies. The Public Services Broker portal will go live next month, said Oliver Ryan, director of Ireland's Reach agency.

Category 4C5 Academic/Industry/Vendor/Govt efforts

2004-05-18 **data sharing security bridge federal government PKI federated identity**

DHS IAIP Daily; http://www.fcw.com/fcw/articles/2004/0517/web−pki−05−18−04.a sp

May 18, Federal Computer Week — Three agencies, supplier certified for security bridge.

Three federal agencies and a federal supplier have achieved cross-certification status with the Federal Bridge Certification Authority, a secure systems infrastructure for exchanging data. The admission of four new members doubles the number of organizations that have passed rigorous tests required for cross-certification with the bridge, federal officials announced at a recent Federal Public Key Infrastructure (PKI) Deployment Workshop in Washington, DC. Cross-certification means the eight federal agencies and supplier with that status can exchange sensitive information online knowing that the other cross-certified agencies' digital signatures and certificates be trusted. The conceptual architecture that includes the bridge has been expanded to include newer security policy concepts such as those defined by the Office of Management and Budget's E-Authentication program. But officials said the federal bridge continues to play an important role in secure data exchanges among agencies and among the federal government and the states, other countries and businesses.

Category 4C5 Academic/Industry/Vendor/Govt efforts

2004-05-20 **Federal Enterprise Architecture FEA government OMB security layer**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/25994−1.html

May 20, Government Computer News — FEA security layer due this summer.

The Office of Management and Budget (OMB) by the end of the summer will release a security layer for the Federal Enterprise Architecture (FEA). Environmental Protection Agency CIO Kim Nelson, the co-chairwoman of the CIO Council's Architecture and Infrastructure Committee, told lawmakers yesterday that committee members are reviewing CIO comments on the plan and will release it soon to be used by agencies. OMB decided to make security a layer that cuts across all the FEA reference models, instead of separate reference model, because of its importance to every aspect of the IT planning, design and implementation processes, said Karen Evans, OMB administrator for e-government and IT.

Category 4C5 Academic/Industry/Vendor/Govt efforts

2004-05-24 **outsource government network services treasury**

DHS IAIP Daily; http://fcw.com/fcw/articles/2004/0524/tec−treasury−05−24−04. Asp

May 24, Federal Computer Week — Treasury to outsource network services.

By the end of the year, U.S. Department of Treasury officials expect to award what could be the federal government's largest telecommunications contract for managed services. The new contract will be based on service-level agreements, which private-sector officials increasingly view as the most efficient way of buying telecom services. "We want obviously the best service for the cheapest price, as any organization would," said Mike Parker, acting chief information officer at Treasury. Department officials said they expect to use the managed services contract to acquire such advanced network capabilities as IP multicast, IP Version 6, IP telephony and optical-wavelength service. IP multicast is a way to broadcast video signals via networks that use relatively low bandwidth. The contract will cost Treasury as much as $1.5 billion, but it will get the agency out of the telecom business. It will no longer own the network assets on which it will depend.

Category 4C5 Academic/Industry/Vendor/Govt efforts

2004-06-01 **Internet access satellite television broadcast**

NewsScan

NEWS CORP. SCRAPS SATELLITE INTERNET PLANS

News Corp. is dropping plans to deliver broadband Internet access via satellite in the U.S. The company says it will still launch at least one Spaceway satellite, but will use it for television broadcast, not high-speed Internet service. The announcement came as a surprise to News Corp. subsidiary DirecTV, which disputed its parent company's statement, saying "we have not scrapped plans to use the satellites for broadband access. In fact, the satellites are being designed specifically so they can be used for video or broadband." (Reuters/CNet 1 Jun 2004)

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2004-06-07 **Microsoft Windows XP software strategy developing countries**

NewsScan

SPECIAL SOFTWARE STRATEGIES FOR DEVELOPING COUNTRIES

Departing from a one-size-fits-all global pricing strategy, Microsoft has tailored special government-promoted PC sales for Thailand and Malaysia in a new marketing approach for emerging markets. Localized versions of Microsoft Windows XP are offered without English-language support, and the company is apparently developing leaner Windows with features more appropriate to developing countries. Microsoft executive Barry Goff says, "This is a new market with very different needs, from an economic perspective, from a social perspective, from a technical perspective." In addition Microsoft, companies such as Symantec and Sun Microsystems have also introduced special government pricing strategies for developing countries. Jupiter Research industry analyst Joe Wilcox says, "What we're seeing is the beginning of a trend. The more companies test the waters, the more of a trend there is because of the competitive threat." (AP/San Jose Mercury News 7 Jun 2004)

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2004-06-24 **Brazil lawsuit Microsoft attacked Australia OSIA Bill Gates**

NewsScan

MICROSOFT'S BRAZIL LAWSUIT 'REPREHENSIBLE'

OSIA, Australia's Open Source industry body, has issued a scathing criticism of Microsoft's lawsuit against Sergio Amadeu, President of the Brazilian National Institute for Information Technology, calling it a "reprehensible action" that attempts to "curb freedom of speech and of criticism." The defamation lawsuit was filed after Amadeu defended the Brazilian government's decision to shift 300,000 PCs from Windows to Linux. He had said this decision "makes sense for a developing country where a mere 10% of the 170 million people have computers at home and where the debt-laden government is the nation's biggest computer buyer." OSIA also referred to Microsoft's "abuse" of its monopoly position, and Bill Gates's address to university students in 1998, where he made a statement saying, "Although about 3 million computers get sold every year in China, people don't pay for the software. Someday they will, though. As long as they are going to steal it, we want them to steal ours. They'll get sort of addicted, and then we'll somehow figure out how to collect sometime in the next decade." (The Age, 24 Jun 2004)

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2004-07-19 **Microsoft software anti-trust Justice Department compliance question**

NewsScan

IS THE NEW MICROSOFT SOFTWARE ANTITRUST-COMPLIANT?

The Justice Department has told a federal judge that the government wants to look at Microsoft's next-generation operating system (code-named Longhorn) early enough that changes can still be made in it if they are necessary for compliance with the antitrust agreement made two years ago.
Industry analysts have predicted introduction of Longhorn in 2006 or 2007, when the antitrust settlement is scheduled to expire. A Microsoft spokesman says, "All development is being done with full consideration for our obligations and commitments," and U.S. District Judge Colleen Kollar-Kotelly, who presided over the antitrust agreement, praises its effectiveness so far. (Washington Post 19 Jul 2004)

Category 4C5 Academic/Industry/Vendor/Govt efforts

2004-07-30 **Georgia Fulton County network security upgrade bandwidth usage**

DHS IAIP Daily;
http://www.informationweek.securitypipeline.com/news/2610099 8

July 30, InformationWeek — Georgia County looks at network traffic.

The Department of Information Technology in Fulton County, GA, has just completed a network-security upgrade that gives it the ability to detect the amount of network resources being consumed by applications across the county's 5,500 PCs. Use of instant messaging, radio broadcasts over the Web, and peer-to-peer file sharing apps such as Kazaa are not new to the county. But their proliferation had recently begun "eating up bandwidth that I'm purchasing with taxpayer dollars," says county CIO and IT director Robert Taylor. Not a good thing, particularly as Fulton County expands its E-government initiatives to provide its 886,000 residents with greater access to county records via the Web. Rather than buying additional DS3 lines, which run at around 45 Mbps and cost about $8,000 per month, Taylor and his staff decided to make better use of the network's existing bandwidth. The upgrade will also improve security. The network was hit last October by a denial-of-service attack caused by the Welchia virus, an aggressive infection designed to exploit a software flaw in recent versions of Windows. Although the virus was contained, Smith says, the server is being used to identify malicious behavior before it becomes a problem.

Category 4C5 Academic/Industry/Vendor/Govt efforts

2004-08-04 **Federal Communications Commission FCC network outage reporting rules**

DHS IAIP Daily; http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC−
250543 A1.pdf

August 04, FCC — FCC adopts rules to enhance network outage reporting.

The Federal Communications Commission (FCC) on Wednesday, August 4, adopted new rules requiring wireless, wireline, cable, and satellite telecommunications providers to report information electronically to the FCC about significant disruptions or outages to their communications systems. The Commission also ruled that all sensitive information collected as a result of these new rules will be protected from public disclosure. These actions will facilitate more reliable telecommunications throughout the United States and promote homeland security, building on the telecommunications industry's efforts to date to improve outage reporting. Under the new rules, both wireless and satellite providers will be subject to the FCC's reporting requirements. The increasing use of cell phones and pagers, as well as the Nation's growing dependence on satellite communications as critical infrastructure, necessitated these changes to the Commission's rules. Action by Report and Order and Further Notice of Proposed Rulemaking (FCC 04-188).

Category 4C5 Academic/Industry/Vendor/Govt efforts

2004-08-27 **cybersecurity memo required Office of Management and Budget OMB**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/27089−1.html

August 27, Government Computer News — OMB asks agencies for cybersecurity check-up.

Agencies have until October 6, 2004 to report to the Office of Management and Budget (OMB) on how they have improved their cybersecurity over the past year. In a memo to agency executives, OMB director Joshua B. Bolten said agencies should summarize the results of their annual IT security reviews of systems, agency progress in correcting weaknesses defined in their plans of actions and their inspector general evaluations. Last year, agencies said about 62 percent of all systems were secured, and OMB earlier this month, said that number had increased to 70 percent. Agencies still are well behind the administration's goal of 90 percent of all systems secured by December 2003.

Category 4C5 Academic/Industry/Vendor/Govt efforts

2004-09-21 **America Online AOL second level security subscription**

NewsScan

AOL OFFERS SECOND LEVEL OF SECURITY

AOL has become the first major U.S. online business to offer customers a second layer of security, which it will make available to subscribers for $1.95 a month in addition to a one-time $9.95 fee. The system uses a matchbook-size device displaying a six-digit log-on code that changes every minute; it requires that the second password be entered in order to check e-mail or access such services as calendars, stock portfolios and AOL's Bill Pay. Gartner analyst Avivah Litan estimates that no more than 5-15% of AOL subscribers will sign up initially but says that "you have to start somewhere." (AP/Washington Post 21 Sep 2004)

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2004-10-11 **National Institute of Standards and Technology NIST minimum security concerns document publication**

DHS IAIP Daily; http://www.fcw.com/fcw/articles/2004/1011/web−nist−10−11 −04. asp

October 11, Federal Computer Week — NIST details minimum security controls for federal information systems.

A new document by the National Institute of Standards and Technology (NIST) spells out the minimum security controls that federal agency officials must use to comply with the statutory requirements of the Federal Information Security Management Act of 2002. The document, Special Publication 800-53, will be available at www.nist.org until November 30 for public review and comment. NIST officials said they are especially interested in receiving comments about the cost and potential impact that the recommended computer security controls could have on federal agencies.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2004-10-18 **security Microsoft Cisco alliances Dell AOL Yahoo spyware customers**

NewsScan; http://www.washingtonpost.com/wp-dyn/articles/A41629-2004Oct18.html

SECURITY PROBLEMS PROMPT STRANGE BEDFELLOWS

With security looming as major issue for users, top technology firms are coming to terms with the need to form alliances in order to combat the plague of viruses, computer worms and spyware programs that threatens computing productivity. One case in point is today's announcement that Microsoft and Cisco are teaming up to tackle the problem, in an acknowledgement that many corporate customers have made major investments in both companies' technology and do not want to be forced to choose between them when it comes to security solutions. Meanwhile, Dell is partnering with the nonprofit Internet Education Foundation -- a coalition that includes tech giants like AOL and Yahoo -- to educate consumers about the risks of spyware. Dell VP Mike George says his company normally does not become involved in software issues, but in recent months has stepped up efforts to help consumers rid their computers of spyware and other problems because they are turning off potential users.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2004-11-04 **Microsoft patch issue help preparation security bulletin publication Website**

DHS IAIP Daily; http://www.infoworld.com/article/04/11/04/HNmicrosoftpatchin g_1.html

November 04, IDG News Service — Microsoft to help users prepare for patching.

Microsoft Corporporation will give customers advance notice of its monthly security updates in an effort to help them prepare to install related software patches, the company announced Thursday, November 4. Starting this month, Microsoft will publish on its Website a summary of planned security bulletins three days before they are released in their entirety. The summary will include information on which products are affected by updates, and severity ratings for security problems. The company normally releases security bulletins on the second Tuesday of each month. It previously offered customers who signed up through support personnel advanced notifications, but the information was not published for all customers. The information will be available at http://www.microsoft.com/technet/security/default.mspx

---

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2004-11-17 **Carnegie Mellon University CMU Korean Information Security Agency collaboration CyLab**

DHS IAIP Daily; http://www.cmu.edu/cmnews/extra/041116_cylab.html

November 17, Carnegie Mellon University — Carnegie Mellon to create collaborative research lab with Korea Information Security Agency.

Carnegie Mellon University and Korean officials have agreed to create a new collaborative research lab for the study and development of leading-edge security technologies. Officials from the Korea Information Security Agency (KISA) have pledged $6 million over the next three years to establish CyLab Korea at Carnegie Mellon. KISA will also establish CyLab Korea in Seoul, Korea, with more than 10 research staff members. Both sites will work together on research projects and develop new technologies and paradigms that will usher in an era of more secure computers, networks and communications systems. KISA is a center of excellence responsible for the computer network security of commercial information technology infrastructure that covers nearly 90 percent of the entire infrastructure of information technology in the Republic of Korea (South Korea).

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2004-11-18 **Oracle patch cycle security planning no surprise**

DHS IAIP Daily; http://www.informationweek.com/showArticle.jhtml;jsessionid=CNBEG43XHVO1YQSNDBGCKH0CJUMEKJVN?articleID=53700526

November 18, InformationWeek — Oracle moves to quarterly security-patch cycle.

Oracle's new quarterly patch schedule comes only months after the company said it would issue such security updates every month. The company says patches will be published simultaneously to all customers through its Web support site MetaLink each quarter beginning on January 18. Oracle says the new schedule will allow its customers to plan to patch, rather than react to "surprise" patch alerts.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2004-11-27 **UK IT computer network sprawl chaos failure prevention project healthcare banking**

DHS IAIP Daily; http://www.newscientist.com/news/news.jsp?id=ns99996706

November 27, New Scientist — Sprawling systems teeter on IT chaos.

The UK government is spearheading a $19 million program aimed at finding ways to avert catastrophic failures in large IT networks. Some systems are now so large they are untestable, making it impossible to predict how they will behave under all circumstances. The hidden flaws could lead to crashes in critical networks like healthcare or banking systems. The scheme has been given added urgency by the failures of power grids in the U.S. and Italy last year. There is a real danger that such massive interconnected systems will exhibit potentially disastrous "emergent behaviors," says David Cliff of Hewlett-Packard's laboratory in Bristol, UK. The $19 million the UK is to spend will be used to set up a national center to study IT complexity, managed by the Engineering and Physical Sciences Research Council.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2004-11-30 **University Texas cybersecurity research center CIAS technology multi disciplinary initiative**

DHS IAIP Daily; http://austin.bizjournals.com/austin/stories/2004/11/29/dail y13.html?jst=b_ln_hl

November 30, Austin Business Journal (TX) — UT's info security center to address cybersecurity concerns.

The University of Texas has established a new security center to address the growing cybersecurity problems across the country. The Center for Information Assurance and Security's (CIAS) goal is to conduct research that will lead to innovative cybersecurity solutions and address the national need to produce more trained professionals in the field. "Despite considerable industry spending to develop solutions, the cybersecurity problem continues to grow at an alarming rate," says Frederick Chang, director of the CIAS and a research professor. The new center will involve business, government and academia in its effort to be a multi-disciplinary initiative.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2004-12-02 **United States US Japan cooperation cybersecurity information networks security global culture**

DHS IAIP Daily; http://tokyo.usembassy.gov/e/p/tp−20041202−05.html

December 02, U.S. Department of State — United States, Japan should cooperate on cybersecurity.

The United States and Japan should intensify cooperative efforts to secure their information networks and work toward the creation of "a global culture of cyber security," according to Lincoln P. Bloomfield Jr., assistant secretary of state for political-military affairs. Bloomfield addressed the U.S.-Japan Critical Information Systems (CIP) Forum hosted by the Vanderbilt Institute for Public Policy Studies in Washington, DC on Tuesday, November 30. "Weaponizing" information technology (IT) is relatively cheap and attacks can be carried out with "a reasonable expectation of impunity," according to Bloomfield. For this reason, the United States and Japan must join forces to protect their own and global information systems, he said. The two countries' governments have made steps in this direction, Bloomfield pointed out. The first formal discussion of cybersecurity began in June 2002, and efforts continued with meetings in February 2004. Each nation must take systematic, coordinated actions to protect its own networked information systems, Bloomfield said. Global efforts to secure information systems, he said, include not just governments but information technology developers, vendors, data managers, and telecom providers.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2004-12-14 **General Services Administration GSA security working group revival standards evaluation**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/30948−1.html

December 14, Government Computer News — GSA will revive security working group.

The General Services Administration (GSA) will re-establish a government-wide working group to evaluate telecommunications security and draft standards. The effort will be part of GSA's Multitier Security Profile Program, an effort to package security services for agencies, said John Johnson, assistant commissioner for service development at GSA's Federal Technology Service. He said the working group would be in place within two months. Because of the importance of security, the new group will remain in place indefinitely, Johnson said. It will build on the early work to look at changes in telecomm security needs and recommend standards, he said.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-01-07 **IT technology schools Internet schoolwork curriculum**

EDUPAGE; http://www.siliconvalley.com/mld/siliconvalley/10588049.htm

PAIGE CALLS FOR STRONGER IT EMPHASIS

Education Secretary Rod Paige this week called for improved use of technology in U.S. schools. According to a report issued by the Department of Education, virtually all of the nation's schools are connected to the Internet, and schools on average have one computer for roughly every five students. Despite this level of technology available, and despite the fact that many students are using computers regularly for schoolwork, educators do not have the skills or the understanding to effectively integrate technology into the curriculum, according to the report. "Schools remain unchanged for the most part," said Paige, "despite numerous reforms and increased investments in computers." Although insufficient funding is frequently cited as a reason for the lag in teacher training, the report rejected that argument, pointing out that funding can come from a number of sources.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-01-12 **Opera browser education university education browser campus**

EDUPAGE; http://news.com.com/2100-1032_3-5533666.htm

OPERA BROWSER FREE FOR HIGHER EDUCATION

Opera Software said this week that its Opera browser will be freely available to any university worldwide, in an effort to protect higher education from flaws in "more vulnerable browsers." The company also touted its browser's customization features, which would allow colleges and universities to personalize the browser for their own campus. Opera CEO Jon von Tetzchner said his company's browser is "fully standards-compliant and offers extensive administration possibilities for network configuration." Institutions including Harvard University, the Massachusetts Institute of Technology, and Oxford University have reportedly already taken Opera up on its offer. CNET, 12 January 2005 l

---

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-01-13 **FBI computer system attacks intelligence agencies software**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=7324403

FBI'S NEW COMPUTER SYSTEM ALREADY OLD

A complete overhaul of the FBI's computer system following the September 11 attacks may prove to have been wasted effort, according to the agency. Criticism was leveled at intelligence agencies following the attacks of September 11, with some arguing that, had information been freely shared among the agencies, the attacks might have been prevented. The FBI undertook to replace all of its systems at one time, which agency officials said was the wrong approach. One official compared the initiative to "changing wheels on a car that is going at 70 miles per hour." Such an overhaul, he said, should be done in stages. Critics faulted the old system for being largely paper-based, preventing agents in the field from accessing needed information or from filing reports electronically. An application called Virtual Case File was supposed to fix many of those problems, but after numerous delays, the software that was finally delivered last month is largely unusable. Reuters, 13 January 2005

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-01-18 **Media Lab Europe funding MIT corporate funding research**

EDUPAGE; http://www.nytimes.com/2005/01/18/technology/18lab.html

MEDIA LAB EUROPE TO CLOSE

Five years after it was opened, Media Lab Europe will close its doors, unable to attract sufficient funding to remain viable. Modeled after the successful Media Lab at MIT, Media Lab Europe opened in Dublin, Ireland, hoping to secure 165 million euros as a 10-year budget. Despite 35.5 million euros from the Irish government--as well as another 22.5 million the government spent on Media Lab's facilities, which were rented to the lab for virtually nothing--organizers of the lab were only able to sign up eight corporate and private-sector partners. Some critics of the lab said the funding model that worked in the United States was unlikely to work in Europe and should have been adjusted accordingly. Others noted that in an environment where public funding of academic research was difficult to come by, the Irish government's generous support of Media Lab may have annoyed other researchers in the country, thereby isolating the lab from them. Nicholas Negroponte, founder of Media Lab, said he had hoped the lab would seed other such research projects in Europe, but he attributed its demise to the bursting of the dot-com bubble and to what he called "top-down, highly bureaucratic and geopolitical funding offered by the E.U."

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-01-18 **report spending cybersecurity Presidents Information Technology Advisory Committee research academic Cyber Trust NSF**

EDUPAGE; http://chronicle.com/prm/daily/2005/01/2005011802n.htm

REPORT CALLS FOR INCREASED SPENDING ON CYBERSECURITY

A new report from the President's Information Technology Advisory Committee calls for increased federal spending on cybersecurity research and stronger efforts to support academic research into cybersecurity. The report outlines a number of structural issues that contribute to the current problem, including a bureaucracy that causes confusion among federal agencies about the sources of funding for cybersecurity projects. According to the report, the Cyber Trust, which was established by the National Science Foundation (NSF), funded only 8 percent of the proposals it reviewed, while 25 percent warranted support. The report recommends increasing the NSF's cybersecurity budget by $90 million a year. Because cybersecurity projects often involve classified material, many colleges and universities cannot participate. The report argues that the government should take steps to increase the number of faculty involved in cybersecurity research--currently fewer than 250--and to attract more students to the field, with the goal of doubling the number of cybersecurity researchers in 10 years.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-01-26 **Sun Solaris open source Microsystems Dell HP Linux products systems products operating system**

EDUPAGE; http://www.nytimes.com/2005/01/26/technology/26sun.html

SUN MOVES SOLARIS TO OPEN SOURCE

Sun Microsystems has announced it will make its Solaris 10 operating system available as an open source product. Sun has lost ground to companies including Dell and HP that increasingly offer Linux-based products. Changing consumer sentiment regarding proprietary systems has left Sun defending its products, and the company's latest move is designed to persuade developers to once again consider Sun's technology. The open source Solaris will be available free of charge, and developers will be able to make changes to the operating system to improve it as they see fit. According to John Loiacono, executive vice president for software at Sun, the goal is to get more developers using Solaris, thereby increasing opportunities for Sun to sell its other products and hardware. The company also announced it would modify its stance on intellectual property and allow free use of 1,600 of the patents it holds on the Solaris operating system.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-01-31 **open source legal service Linux Software Freedom Law Center Moglen**

NewsScan; http://www.siliconvalley.com/mld/siliconvalley/10783701.htm

LEGAL CENTER FOR OPEN-SOURCE PROJECTS

A consortium of companies seeking promote use of the Linux operating system has contributed $4 million to establish a legal center for nonprofit open-source projects and developers. The Software Freedom Law Center will be headed by Columbia University law professor Eben Moglen, who explains: "The Law Center is being established to provide legal services to protect the legitimate rights and interests of free and open source software projects and developers, who often do not have the means to secure the legal services they need." (AP/San Jose Mercury News 31 Jan 2005)

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-02-10 **fighting computer distractions academic commercial reading checking weather online surfing Web sites music files Microsoft University applications Software message**

EDUPAGE;
http://www.nytimes.com/2005/02/10/technology/circuits/10info.html

FIGHTING COMPUTER DISTRACTIONS

A number of academic and commercial researchers are working to limit the distractions that computer users continually face. Activities such as reading e-mail, checking the weather online or surfing other Web sites, or simply fiddling with electronic music files can prove to be significant impediments to productivity for many people. Researchers often speak of "cognitive flow," a state of strong focus on a particular task. Some projects, including one involving researchers at Microsoft and the University of Maryland, study flow with the goal of designing applications that attempt to discern such a state in computer users. Software can then assign priority levels to potential interruptions, such as a new e-mail message, and determine whether to alert the user or to wait until the flow has ended. Alon Halevy, a professor of computer science at the University of Washington, is also working on e-mail systems that can decide when best to interrupt the user. Other efforts focus on understanding the types of functional structures that cause or promote distractions.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-02-21 **US government federal group IT security boost CISO exchange CIO council**

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml?artic leID=60402267

FEDERAL GROUP FORMED TO BOOST SECURITY

The consistent failure of many federal agencies to secure their IT systems has prompted government officials to create a new organization, which will be funded by the private sector, to help chief information security officers improve cybersecurity. The formation of the CISO (Chief Information Security Officer) Exchange was disclosed last week by the federal CIO Council and the chairman of the House Government Reform Committee, Tom Davis, R-VA, who also released a computer-security scorecard for two dozen federal departments and agencies. Unlike the CIO Council, the CISO Exchange will be an informal organization aimed at providing more than 100 departmental and agency chief information security officers with a way to collaborate. The exchange will be co-chaired by Justice Department CIO Van Hitch, who heads the CIO Council's cybersecurity and privacy committee, and Government Reform Committee staff director Melissa Wojciak. All money to support the CISO Exchange will come from business, mostly IT security companies. As of last week's announcement, no company had been asked to contribute money.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-02-22 **Singapore cyber terrorism plan computer virus hacker threat government collaboration Australia United States**

DHS IAIP Daily;
http://www.reuters.com/newsArticle.jhtml?type=internetNews&s toryID=7698536

SINGAPORE UNVEILS PLAN TO BATTLE CYBER TERROR.

Singapore is to spend $23 million over three years to battle online hackers and other forms of "cyber-terrorism" in one of the world's most connected countries, government officials said Tuesday, February 22. Describing the infrastructure behind the Internet as a "nerve system" in Singapore, Deputy Prime Minister Tony Tan said a new National Cyber-Threat Monitoring Center would maintain round-the-clock detection and analysis of computer virus threats. Singapore has one of the world's highest Internet penetration rates, with 50-60 percent of its 4.2 million people living in homes wired to the Internet. The Cyber-Threat Monitoring Center will link up with companies that provide anti-virus systems and governments running similar centers, including the United States and Australia. It is expected to be fully operational by the second half of 2006.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-02-24 **Britain UK Home Office Internet security hacking groups National Infrastructure Security Coordination Centre NISCC Website**

DHS IAIP Daily; http://www.computerweekly.com/articles/article.asp?liArticle ID=136955&liArticleTypeID=1&liCategoryID=2&liChannelID=22&li FlavourID=1&sSearch=&nPage=1

BRITAIN LAUNCHES INTERNET VIRUS ALERT SERVICE

Britain's Home Office has launched a high-profile campaign to secure the Internet against hacking groups using networks of infected computers to launch worm, spam and denial of service attacks against critical businesses and services. The campaign, which features a Website and an alert service to help non-IT specialists protect their computer systems, is designed to plug one of the weakest links in security on the Internet: home and small business PCs. The campaign will encourage home users and small businesses to sign up to an alert service, run by the National Infrastructure Security Coordination Centre (NISCC), part of the Home Office, which will give advice on urgent threats that affect home PCs, PDAs and mobile phones. Although the service is not designed to replace alert services run by firewall and anti-virus companies, NISSC believes that its links with international IT security organizations will help it to identify new computer threats as quickly as or before commercial alerting services. For more on the new service, visit http://www.itsafe.gov.uk

---

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-02-24 **U.K. ITsafe home National Infrastructure Security Coordination Centre personal data government messages mobile devices virus software patches**

EDUPAGE; http://www.pcworld.com/news/article/0,aid,119811,00.asp

U.K. OFFERS WEB SITE FOR SECURITY ALERTS

A new Web site called ITsafe will send security alerts to home and small-business computer users in the United Kingdom. The National Infrastructure Security Coordination Centre will run the free site, which also offers advice on protecting personal data. The government plans to issue official alerts by e-mail or text messages over mobile devices to users who sign up for the service if a particular virus or other security breach poses a significant threat and users can do something to combat it, such as updating software or downloading security patches. The ITsafe site will not supply either. The Home Office estimates up to 10 security alerts per year based on past experience.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-03-07 **technology companies coordinate efforts compliance Sarbanes-Oxley**

EDUPAGE; http://www.internetnews.com/bus-news/article.php/3487896

TECH COMPANIES COORDINATE COMPLIANCE EFFORTS

A group of eight leading technology companies has formed a working group to help organizations understand and meet a growing number of technology regulations, including such legislation as the Sarbanes-Oxley Act. Founding members of the Compliance and Management Electronic Information (CMEI) working group include Oracle, HP, Sun Microsystems, and Veritas; the group will begin posting resources on the Internet Law and Policy Forum Web site in the next six months. As technology increasingly underpins business processes, the range of regulations with which a company must comply can be daunting. For example, U.S. regulations require companies to maintain records on former customers for seven years; laws in the United Kingdom, in contrast, require companies to immediately delete information on former customers. The CMEI working group will publish best practices, work to foster communication between businesses and regulatory agencies, and offer resources for companies to help them understand various compliance requirements. Internet News, 7 March 2005

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-03-08 **US government Office of Management and Budget OMB six month study information technology IT security function vendor management**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/35249−1.html

OMB TO STUDY CONSOLIDATION OF IT SECURITY FUNCTIONS.

The Office of Management and Budget (OMB) expects this month to launch a six-month study of whether some federal IT security functions could be provided centrally by agencies or commercial vendors. Karen Evans, OMB administrator for e-government and IT, said Tuesday, March 8, at the Government Computer News Cybersecurity Conference in Washington, D.C. that a task force would complete its work by September so that guidance would be available to agencies for the fiscal 2007 budget cycle. The study will apply the Business Reference Model, a function-focused method for describing business operations, to cybersecurity. Each agency has its own security needs and acceptable risk profiles, and the study might not support the use of common providers for IT security, according to Evans. But she said there is enough common need that she doubts there is a good business case for 26 executive branch departments and agencies each going its own way for security. The study is part of a broader move by OMB toward focusing on the outcome of IT security management.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-03-16 **Florida Sarasota County wireless Wi-Fi network security intrusion prevention devices**

DHS IAIP Daily; http://www.fcw.com/article88313−03−16−05−Web

SARASOTA COUNTY, FLORIDA GOVERNMENT SECURES WIRELESS NETWORK.

Cautious about the security of its wireless network, the Sarasota County, FL government has installed devices in its buildings to detect and prevent wireless intrusion. By using such devices to secure about three million square feet of airspace across 15 of the county's 200 buildings, it is easier for information technology personnel to spot any unauthorized vulnerabilities or attacks on the wireless infrastructure. "We minimize the risk that occurs through these devices," said Bob Hanson, Sarasota County's chief information officer. Hanson said his government has security policies in place, but with considerable employee turnover each year, it's difficult to keep up their education. He said there are almost 5,000 employees in the area covered, and rogue wireless access points are perplexing. Sarasota IT officials can monitor their airspace using a centralized Web-based interface. Rich Swier, CEO of monitoring system company, said that although the benefits of wireless are obvious, it has also created a problem. Before, security personnel only had to worry about security within their facilities. "Now you're having your good guys, your employees and so forth bringing in devices and exposing your network outside your four walls."

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-03-18 **European government Internet terror watch team study information sharing police**

DHS IAIP Daily; http://news.bbc.co.uk/1/hi/technology/4360727.stm

EUROPEAN GOVERNMENTS TO FORM INTERNET 'TERROR WATCH' TEAM

Five European governments are setting up a hi-tech team to monitor how terrorists and criminals use the Internet. The group will make recommendations on shutting down Websites that break terrorism laws. The plans for the initiative came out of a meeting of the G5 interior ministers in Spain that discussed ways to tackle these threats. The five countries also agreed to make it easier to swap data about terror suspects and thefts of explosives. The interior ministers of Spain, Britain, France, Germany and Italy -- the G5 -- met in Granada, Spain last week for an anti-terrorism summit. To combat terrorism the ministers agreed to make it easier for police forces in their respective states to share data about suspects connected to international terror groups. Part of this anti-terror work will involve the creation of the technical team that will keep an eye on how organized crime groups and terrorists make of the web.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-03-21 **IT security function improvement cybersecurity team meeting Office of Budget and Management OMB**

DHS IAIP Daily; http://www.gcn.com/24_6/news/35313−1.html

NEW CYBERSECURITY TEAM MEETS THIS WEEK

The Office of Management and Budget (OMB) has created a task force that this week will begin figuring out how agencies can share cybersecurity functions. The team of senior IT managers will look at training, incident response, disaster recovery, contingency planning and how agencies select security products. The March 23 kick-off meeting will start a six-month study. By September, the group must develop a business case for IT security functions that can be provided centrally by agencies or vendors. OMB wants the new cybersecurity task force to ferret out functions that, if shared or standardized, will mean quick and easy improvements across the government. Karen Evans, OMB's administrator for IT and e-government, said guidance from the task force's findings will be available to agencies for the fiscal 2007 budget cycle. OMB Website: http://www.whitehouse.gov/omb/

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-03-24 **Federal Bureau of Investigation companies report intrusions management concern security breaches stock prices**

DHS IAIP Daily; http://www.computerworld.com/securitytopics/security/story/0 ,10801,100598,00.html

FBI ASKS COMPANIES TO REPORT CYBER INTRUSIONS.

Corporate executives are often reluctant to report network intrusions for fear of having those security breaches made public and drag down stock prices. But state and federal law enforcement officials who spoke at an information security panel in New York on Wednesday, March 23, said such reports can sometimes provide an important missing link in larger cybersecurity investigations. "It may be a critical piece of information you're submitting to us – you never know where that fits into the pie," said Ron Layton, section chief of the cyber coordination branch for the Department of Homeland Security (DHS). Layton was one of several law enforcement officials who spoke at an information security conference sponsored by AIT Global Inc. and InfoWorld Media Group. Network intrusion reports don't necessarily have to fall within the statutory $5,000 minimum loss for federal authorities to investigate them, said Kent McCarthy, a special agent for the Secret Service in New York. McCarthy said the Secret Service does its best to protect the anonymity of corporations that report network intrusions. "We're not looking for a press release," he said. DHS cyber coordination branch: http://www.uscert.gov and Secret Service: http://www.ustreas.gov/usss/index.shtml

---

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-03-28 **Internet service providers ISP telecommunications companies alliance attacker information sharing**

DHS IAIP Daily;
http://www.computerworld.com/managementtopics/outsourcing/is ptelecom/story/0,10801,100695,00.html

ISPS AND TELECOMM COMPANIES FORM ALLIANCE TO SHARE DETAILED INFORMATION ON ATTACKERS.

Leading global telecommunications companies, Internet service providers (ISPs) and network operators will begin sharing information on Internet attacks as members of a new group called the Fingerprint Sharing Alliance, according to a published statement from the new group. The companies, including EarthLink, Asia Netcom, British Telecommunications and MCI, will share detailed profile information on attacks launched against their networks. Information to be shared will include the sources of attacks. The alliance will make it easier for service providers and network operators to crack down on global Internet attacks more quickly, according to Tom Schuster, president of Arbor Networks, which launched the new alliance. The alliance replaces an ad hoc system of e-mail messages and phone calls that operators of large networks have used to coordinate their response to attacks and threats, Arbor said. The alliance will make it easier for them to cooperate and will lower the threshold that attacks must surpass to get the attention of ISPs. Even attacks on small ISP customers will prompt a response from large infrastructure providers.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-04-05 **federal information security improvement CISO Exchange Government Accountability Office GAO**

DHS IAIP Daily; http://www.federaltimes.com/index2.php?S=766429

GROUP AIMS TO BOOST FEDERAL INFORMATION SECURITY

A group of government and industry executives will meet for the first time this month to map out a strategy for improving the government's information security. The CISO Exchange is comprised of five chief information security officers from various federal agencies, one federal chief security officer, and two executives from information technology companies. It is a privately funded working group that will hold quarterly educational meetings and produce an annual report on the government's information technology security policies and operational issues. The exchange was announced in February by the federal Chief Information Officers Council and Representative Tom Davis from Virginia, chairman of the House Government Reform Committee. They announced the exchange as a way to boost security through educational meetings between chief information security officers and others in government and private industry. The group also will work with the Government Accountability Office and inspector general offices. At least 50 companies have inquired about joining the exchange, said Stephen O'Keeffe, of O'Keeffe & Company, the company managing the meetings. The two fellows on the exchange so far paid $75,000 apiece, he said.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-04-11 **National Science Foundation NSF cybersecurity foundation research**

DHS IAIP Daily;
http://www.nsf.gov/news/news_summ.jsp?cntn_id=103178&org=OLP
A&from=news

NATIONAL SCIENCE FOUNDATION ANNOUNCES INTENT TO ESTABLISH CYBERSECURITY CENTER

The National Science Foundation (NSF) has announced it intends to establish two new Science and Technology Centers (STCs) in fiscal 2005. One is a major collaborative cybersecurity project led by the University of California, Berkeley, and a second, centered at the University of Kansas, will study polar ice sheets. The cybersecurity center will investigate key issues of computer trustworthiness in an era of increasing attacks at all levels on computer systems and information-based technologies. The Team for Research in Ubiquitous Secure Technology (TRUST) will address a parallel and accelerating trend of the past decade–the integration of computing and communication across critical infrastructures in areas such as finance, energy distribution, telecommunications and transportation. The center will lead development of new technologies based on findings from studies of software and network security, trusted platforms and applied cryptographic protocols. Formal approval of the new centers, with funding estimated at nearly $19 million over five years for each center, is still subject to final negotiations between NSF and the lead institutions. UC Berkeley Press Release: http://www.berkeley.edu/news/media/releases/2005/04/11_trust .shtml

Additional information from an article by Daniel S. Levine in the SF Business Times:
* The project leader will be S. Shankar Sastry, UC Berkeley professor of electrical engineering;
* "Other members of the TRUST effort are Carnegie Mellon University, Cornell University, Mills College, San Jose State University, Smith College, Stanford University and Vanderbilt University. The initiative also brings together industrial and other affiliates, including Bellsouth, Cisco Systems, ESCHER (a research consortium that includes Boeing, General Motors and Raytheon), Hewlett-Packard, IBM, Intel, Microsoft, Oak Ridge National Laboratory, Qualcomm, Sun Microsystems and Symantec."

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-04-12 **NSF funding computer security research Team for Research in Ubiquitous Secure Technology TRUST University of California Berkeley critical infrastructure protection**

EDUPAGE; http://www.nytimes.com/cnet/CNET_2100-7349_3-5666782.html

NSF TO FUND COMPUTER SECURITY RESEARCH CENTER

The National Science Foundation (NSF) has awarded a $19 million grant to create a technology center to study cybersecurity. The project, called the Team for Research in Ubiquitous Secure Technology (TRUST), will be led by the University of California, Berkeley, and will receive the funds over five years. Other higher education institutions participating in the project include Carnegie Mellon University, Cornell University, Mills College, San Jose State University, Smith College, Stanford University, and Vanderbilt University. S. Shankar Sastry, professor of computer sciences at Berkeley and director of TRUST, said, "The cybersecurity community has long feared that it would take an electronic Pearl Harbor for people to realize the scale of disruptions possible from a concerted attack by terrorists." The TRUST project will conduct research into computer security in a variety of industries, specifically addressing the integration of technologies among "critical infrastructures." New York Times, 12 April 2005 (registration req'd)

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-04-14 **Chief Information Security Officers CISO Exchange CIO council withdrawal vendor fundraising practices**

DHS IAIP Daily; http://www.informationweek.com/story/showArticle.jhtml;jsessionid=D4M3LDAZ5RJUCQSNDBGCKH0CJUMEKJVN?articleID=160900663

FEDERAL GOVERNMENT ABANDONS VENDOR-BACKED CYBERSECURITY FORUM

The federal CIO Council is the latest government institution to retreat from the Chief Information Security Officers (CISO) Exchange because of fund-raising practices. Karen Evans, the administration's top IT official, said in a White House statement issued Thursday, April 14, that she accepts the CIO Council's recommendation to withdraw from the CISO Exchange, a privately financed group headed by government IT experts to help develop practices to improve cybersecurity. Evans said she's asking the CIO Council's best-practices committee to develop ways to improve weak cybersecurity scores among federal departments and agencies. Evans' comments came nearly a week after House Reform Committee chairman Tom Davis, R-VA, announced his withdrawal of support for the CISO Exchange because of the way the group solicited money from vendors to support its operations. The CISO Exchange was to hold quarterly education meetings as well as produce a report on federal IT security priorities and operations. CISO Exchange Website: http://www.cisoexchange.org/

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-04-15 **vendor government cybersecurity focus call Congress legislation information technology CSIA Department of Homeland Security DHS**

DHS IAIP Daily; http://www.nwfusion.com/news/2005/0415vendocall.html

VENDORS CALL FOR MORE GOVERNMENT CYBERSECURITY FOCUS

The U.S. government needs to get more serious about cybersecurity, but Congress should look at broader ways to combat security problems than focusing on bills that address specific issues such as spam or spyware, a group of executives from IT security product vendors said last week. Members of the Cyber Security Industry Alliance (CSIA), meeting in Washington, DC, Thursday, April 14, repeated their call for Congress to create an assistant secretary for cybersecurity position at the Department of Homeland Security. Members of the year-old CSIA, meeting as a rash of data breaches have been announced in recent months, said they committed this week to helping Congress and administration officials understand cybersecurity issues. While most CSIA executives said they would welcome the right kind of cybersecurity legislation, not all technology companies favor new laws. Private companies should have time to find their own solutions to data breaches and explain their efforts to Congress, said Howard Schmidt, chief security strategist at eBay, during a forum on ID theft at the Washington think tank the Center for Strategic and International Studies Friday, April 15. CSIA Website: https://www.csialliance.org/home

---

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-05-09 **Iowa State University ISU computer network Internet attack simulation ISEAGE Department of Justice critical infrastructure protection**

DHS IAIP Daily; http://www.eweek.com/article2/0,1759,1813648,00.asp

UNIVERSITY LABORATORY STUDIES EFFECTS OF INTERNET ATTACKS

A new test laboratory at Iowa State University (ISU) will allow researchers to study how computer networks respond to massive Internet attacks and could lead to breakthroughs in computer defenses and forensics, said a researcher behind the project. The new test network, ISEAGE (Internet Simulation Event and Attack Generation Environment), was funded by a $500,000 grant from the Department of Justice. ISEAGE is the first research lab to be able to re-create any cyber-attack on any part of the Internet infrastructure, said Doug Jacobson, director of information assurance at ISU. The guts of the new test lab are software tools, developed by Jacobson, that let researchers change traffic patterns, replay attacks in endless configurations and collect attack data, Jacobson said. "We can make an attack that looks like it came from 1,000 computers, but we don't need 1,000 computers to do it," he said. The testbed can just as easily simulate attacks from 100,000 Internet-connected machines—or from every Internet address in existence, Jacobson said. Researchers will use ISEAGE to model attacks on critical cyber-infrastructure, such as state and federal computer networks.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-05-13 **US House Science Committee DARPA research funding cybersecurity long-term project shift**

EDUPAGE; http://chronicle.com/prm/daily/2005/05/2005051301t.htm

HOUSE HEARS DEBATE OVER DARPA FUNDING

The debate over what some describe as a troubling shift in the stance of the Defense Advanced Research Projects Agency (DARPA) for research it chooses to fund moved to the House Science Committee this week. DARPA came under fire from a number of sectors recently when it acknowledged that it would give preference in funding decisions to projects with more immediate results, rather than basic, long-term research with less obvious--but some say more vital--implications for developing new technologies. Critics of the change also said funding for cybersecurity projects was inadequate and should be increased. Joining the academics at the hearing who were critical of DARPA's changed focus was Rep. Sherwood L. Boehlert (R-N.Y.), who expressed his support for basic research and for cybersecurity projects specifically. Anthony J. Tether, director of DARPA, defended his agency, saying that projects of the type described are in fact being funded. In addition, he suggested that funding for certain types of research, such as computer science, is often included in grants supporting other types of research, such as microelectronics. Chronicle of Higher Education, 13 May 2005 (sub. req'd)

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-06-06 **US Department of State cybersecurity awareness month June NSA FBI help**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/35993−1.html

DEPARTMENT OF STATE TO PROMOTE CYBERSECURITY AWARENESS

June is designated as the Department of State's Cybersecurity Awareness Month. Between June 7 and June 29, the Diplomatic Security Bureau's Computer Security Office and the Information Resources Management Bureau's Information Assurance Office will sponsor the project to improve employees' understanding of proper security procedures. The bureaus plan to hold events that will include topics on how to fend off phishing scams and other security risks based on social engineering, a demonstration of how hackers work, explanations of how to become a certified IT professional and information on spyware, antivirus software and other tools. The sessions will feature speakers from the National Security Agency, the FBI, the Agency for International Development and leading technology companies.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-06-20 **Office Management Budget OMB security reporting guidelines FISMA**

DHS IAIP Daily; http://www.fcw.com/article89321−06−20−05−Web

OFFICE OF MANAGEMENT AND BUDGET MODIFIES SECURITY REPORTING

The Office of Management and Budget (OMB) has issued new security reporting guidelines that emphasize contractor oversight and data privacy protections. Under the 2005 Federal Information Security Management Act (FISMA) reporting guidelines issued Monday, June 13, agencies will have to answer new questions about data privacy and contractor oversight in reports they must submit to OMB by October 7. When OMB officials added the new questions, they also dropped some old ones. Agencies, for example, will no longer have to report how many times they were victims of a malicious code attack because someone in the agency had not installed a necessary security patch. The new guidelines emphasize that agencies are responsible for ensuring that federal contractors maintain appropriate security controls on equipment used to deliver network or other managed services. The security controls also apply to contractor support staff, government-owned and contractor-operated equipment and contractor-owned equipment in which any federal data is processed or stored. "Agencies must ensure identical, not equivalent security procedures," according to the guidelines. That means agencies must make certain that federal contractors conduct risk assessments, develop contingency plans, certify and accredit their systems and everything else that federal agencies must do to comply with FISMA.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-07-19 **Federal NIST draft standard documents information security seretary FIPS Publication cost effective program assessment**

DHS IAIP Daily; http://www.fcw.com/article89611−07−18−05−Web

NIST OFFICIALS INVITE COMMENT ON DRAFT STANDARD

Computer scientists at the National Institute of Standards and Technology (NIST) have released draft versions of two documents that they consider to be among the most important in a recent series of NIST documents on information security. One is a small publication describing minimum security requirements that will become mandatory after the Commerce Department secretary signs the document, as he is expected to do at the end of this year. That document is "Draft Federal Information Processing Standard (FIPS) Publication 200: Minimum Security Requirements for Federal Information and Information Systems." A second document, "Draft Special Publication 800-53A: Guide for Assessing the Security Controls in Federal Information Systems," is a 152-page guide to developing a cost-effective information security program based an agency' s assessment of its risks. Both documents are meant to help federal agencies secure their information systems and comply with the Federal Information Security Management Act (FISMA) of 2002, NIST officials said.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-08-01 **annivsary issue RISKS FORUM DIGEST congratulations great work splendid achievement mazal tov**

RISKS 23 96

20TH ANNIVERSARY OF RISKS!

Congratulations and THANKS to Peter G. Neumann for his stellar work on the RISKS FORUM DIGEST, which reached its 20th anniversary on 1 August 2005. Here's Peter's comment:

>Somehow it escaped my attention when I put out RISKS-23.95 a few minutes ago, that it was exactly the 20th anniversary of the day on which I had put out RISKS-1.01, on 1 Aug 1985 -- using a primitive line-by-line editor on a huge (not-so-)Silent 700 with an acoustic coupler over a very slow cross-country phone line. Since then, the various technologies have of course increased dramatically. Unfortunately, the risks have also -- in that the same kinds of problems still recur with respect to safety, reliability, security, survivability, interoperability, human culpability, and so on, seemingly ad infinitum, combined with the reality that so many more people are now dependent upon computers and their interconnectivity.

I imagine that I won't keep it up for *another* 20 years (for example, I observe that my ratio of puns seems to have declined), but hopefully one (or some) of you will want to continue the tradition when the time comes. It would be a real shame to let the Risks Forum disappear. Even though the same or similar problems keep recurring, there is an important message herein -- and just another reminder of the needs for constant vigilance, increased awareness, better education, and -- above all -- BETTER SYSTEMS.

Cheers to all! PGN<

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-08-19 **Germany German government efforts national IT security plan**

DHS IAIP Daily;
http://www.infoworld.com/article/05/08/19/HNgermansecurity_1
.html?source=rss&url=http://www.infoworld.com/article/05/08/
19/HNgermansecurity_1.html

GERMAN GOVERNMENT LAUNCHES NATIONAL IT SECURITY PLAN

The German government aims to counter the alarming rise in computer viruses with a national IT security plan that includes the establishment of a computer emergency response center. The new plan was unveiled Thursday, August 18, in Berlin by Interior Minister Otto Schily. The German government's "National Plan to Protect IT Infrastructures" has three major focuses: early prevention, swift response and security standards. The Federal Office for Security in Information Technology (BSI) will play a key role. It will be responsible for developing and implementing new security standards in the public sector, and publishing guidelines for the private sector. BSI will also house the computer emergency response center, which will collaborate with providers of IT security services in the private sector. Among the planned tasks of the center: sending e-mail alerts about potential threats and responding to attacks with hotline technical support. The German IT security plan is available in German on the ministry's Website at: http://www.bmi.bund.de/cln_028/nn_122688/Internet/Content/Co
mmon/Anlagen/Nachrichten/Pressemitteilungen/2005/08/National
er__Plan__Schutz__Informationsinfrastrukturen,templateId=raw
,property=publicationFile.pdf/Nationaler_Plan_Schutz_Informa tionsinfrastrukturen.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-08-24 **FBI DoJ information sharing IT project criminal investigations**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/security/36759−1.html

DEPARTMENT OF JUSTICE, FBI TO SPUR INFORMATION SHARING

The FBI and Justice Department plan to accelerate their efforts to consolidate systems and improve sharing of information needed for criminal investigations and prosecutions by launching two major IT projects. The FBI project, known as Next Generation IAFIS, is aimed at upgrading the Integrated Automated Fingerprint Identification System run by the bureau's National Crime Information Center in Clarksburg, WV. Next Generation IAFIS is intended to improve the efficiency of IAFIS' function of matching fingerprint evidence to the bureau's trove of millions of sets of 10-finger images, according to FBI officials and procurement documents. Next Generation IAFIS will also interact with the IDENT fingerprint database run by the Department of Homeland Security's U.S. Visitor and Immigrant Status Indicator Technology system. Justice's Litigation Case Management System (LCMS) project is intended to promote information sharing among the 94 U.S. attorneys' offices and six major divisions at headquarters that bring cases to court. As it stands now, the U.S. attorneys' offices have litigation case management systems that link poorly or not at all with one another and with headquarters systems. National Crime Information Center: http://www.fbi.gov/hq/cjisd/iafis.htm Department of Justice: http://www.usdoj.gov/

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-09-19 **information cybersecurity government academia college collaboration Iowa State NSF Center for Information Protection**

DHS IAIP Daily; http://www.pcworld.com/news/article/0,aid,122596,00.asp

COLLEGES, GOVERNMENT TEAM ON CYBERSECURITY

Iowa State University and the U.S. National Science Foundation will join with private businesses to attack cybersecurity problems. The new Center for Information Protection will focus on short-term cybersecurity issues identified by member companies. It also has a to develop new technologies that participants can use to fight common cybersecurity problems.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-09-19 **Iowa State information protection center CIP fund NSF**

EDUPAGE; http://www.fcw.com/article90846-09-19-05-Web

IOWA STATE TO HOST INFORMATION PROTECTION CENTER

The National Science Foundation (NSF) is providing the initial funding for a new Center for Information Protection (CIP) at Iowa State University. Corporations, security vendors, and academic researchers will work together through the center to develop solutions to short-term security concerns. The center has already attracted 13 charter members, including Boeing, Cargill, Principal Financial Group, Palisade Systems, Iowa State University, and the New Jersey Institute of Technology. The center's goal is to draw 30 corporate members and to develop security solutions in one year or less. Kurt Shedenhelm, chief executive officer and president of Palisade Systems, said the new center differs from similar efforts in its quest for short-term fixes, compared to the five- and ten-year cycles of other initiatives. The NSF will continue to provide funding for three years, at which time the center can apply for further funds; organizers hope the center can be self-sustaining in five years. Federal Computer Week, 19 September 2005

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-09-20 **Pennsylvania Penn State University peer-to-peer P2P academic use project pilot tests successful**

EDUPAGE; http://chronicle.com/daily/2005/09/2005092001t.htm

PENN STATE DEBUTS P2P FOR ACADEMIC PURPOSES

A new application developed at Pennsylvania State University at University Park puts P2P technology to use in academic pursuits. Funded in part by a $1.1 million grant from the Andrew W. Mellon Foundation, LionShare allows users to search for and access files on other users' computers, similar to P2P applications that have opened the door to a wide range of copyright violations. LionShare, in contrast, is designed for academic purposes, including sharing very large files and other educational materials among approved users. For example, faculty can restrict usage to students registered in their classes. In addition, users can attach keywords and other metadata to files, making them easier to locate and organize. Pilot tests of LionShare have been successful. Michael J. Halm, senior strategist for Penn State's Teaching and Working With Technology office, said that in courses where LionShare was used, although faculty are driving the usage of the tool, students have said they would "definitely use it too" in classes where it was available. The application will be available free from Penn State. Chronicle of Higher Education, 20 September 2005 (sub. req'd)

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-09-28 **cybersecurity firms business tax break US government effort Congress incentive security**

DHS IAIP Daily; http://www.nytimes.com/cnet/CNET_2100−7348_3−5884149.html

TAX BREAKS FOR CYBERSECURITY FIRMS?

Congress may start offering tax breaks to companies that adopt good cybersecurity standards. Dan Lungren, chair of the U.S. House of Representatives cybersecurity subcommittee, is working on an "overall view of ways we can work with the private sector" to develop cybersecurity tools, including the possibility of creating an incentive-based system. Andy Purdy, acting director of the Department of Homeland Security's National Cybersecurity Division, said in a speech that his agency is also working closely with the private sector to equip itself for responding to cyberattacks.

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-10-18 **Schools cyberattack data colleges universities assessment project U.S. Department of Justice New York firwall intrusion reports networks**

DHS IAIP Daily; http://news.com.com/Schools+get+tailored+cyberattack+data/2100−7347_3−5900684.html?tag=cd.top

SCHOOLS GET TAILORED CYBERATTACK DATA

U.S. colleges and universities are getting a service that analyzes security data to help fend off cyberattacks. According to Steffani Burd, the executive director of Information Security in Academic Institutions, "The goal is to have an accurate assessment of information security in academic institutions." The project is sponsored by the research arm of the U.S. Department of Justice and run by Columbia University's Teachers College in New York. Academic organizations will be expected to submit logs from their firewall and intrusion detection systems so the service can parse the data and generate reports on attacks. Those reports can then be used to protect networks. Johannes Ullrich, the chief research officer at the SANS Institute and founder of DShield.org states, "Academic institutions face the challenge of maintaining an open network while also providing security for their users. This data will help them decide what protection to deploy while minimizing restrictions."

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-10-25 **OMB IT cybersecurity security training reporting situational awareness incidence response lifecycle security solutions**

DHS IAIP Daily; http://www.gcn.com/vol1_no1/daily−updates/37418−1.html

OFFICE OF MANAGEMENT AND BUDGET TO IMPROVE IT SECURITY NEXT FISCAL YEAR

The Office of Management and Budget (OMB) plans to set up several lines of business for IT security in the next fiscal year. A " line of business" is a necessary business function that typically is outside of agencies' primary missions, such as cybersecurity. Rather than have each agency duplicate non-essential functions, OMB designates agencies with expertise in these areas to provide them to other agencies on a fee-for-service basis. Four problem areas will be addressed: (1)security training: to standardize security processes, develop common criteria, and help provide a career path for information security professionals; (2) Federal Information Security Management Act reporting: to standardize reporting processes and help ensure consistent and effective IT program management; (3) situational awareness and incident response: to improve the sharing of information about IT vulnerabilities and threats and provide resources for responding to security incidents; and (4) lifecycle security solutions: to provide a methodology for evaluating security tools. The program will not replace existing IT security programs and resources, such as the U.S.-Computer Emergency Readiness Team. According to OMB estimates, federal spending on security has been static, at about $4.2 billion a year for the last three years, while total IT spending has been slowly growing.

Category 4C5 Academic/Industry/Vendor/Govt efforts

2005-10-27 **US administration information technology IT system agency consolidation**

DHS IAIP Daily; http://fcw.com/article91215−10−27−05−Web

ADMINISTRATION TO CONSOLIDATE INFORMATION TECHNOLOGY SYSTEMS ACROSS AGENCIES

According to Karen Evans, the Office of Management and Budget's administrator for e-government and information technology, the government is looking to consolidate information technology systems and turn them into a "utility" instead of keeping them agency-specific. Rather than restricting IT to individual agencies, IT should be seen as an enterprise, she told members attending the Government Electronics and Information Technology Association (GEIA IT). A recent example is that during the recent hurricane disasters along the Gulf Coast, a number of e-government initiatives were tapped to keep government agencies operational: the Coast Guard and the Transportation Security Administration used the National Finance Center and epayroll.gov to make sure 67,000 customers were paid, and USAServices.gov helped the Federal Emergency Management Agency add call centers and handle over one million calls.

Category 4C5 Academic/Industry/Vendor/Govt efforts

2005-10-27 **PC United Kingdom National Hi-Tech Crime Unit IT BT Dell eBay HSBC Lloyds TSB Microsoft MessageLabs securetrading Yell**

DHS IAIP Daily; http://www.getsafeonline.org./

PC AWARENESS PROGRAM LAUNCHED IN THE UNITED KINGDOM

The UK's National Hi-Tech Crime Unit has teamed with the IT industry to launch an awareness program to increase understanding about PC security. The program, "Get Safe Online," is a joint initiative among the government, the National Hi-Tech Crime Unit, and private sector sponsors including BT, Dell, eBay, HSBC, Lloyds TSB, Microsoft, MessageLabs, securetrading.com, and Yell.com. A report released to coincide with the program's launch found that over three quarters of the UK's population (83 percent) don't know enough about protecting themselves online, and that 42 percent of the population just rely on friends and family for online safety advice rather than finding expert information for themselves.

Category 4C5 Academic/Industry/Vendor/Govt efforts

2005-11-04 **government accounting office GAO report Internet Management Prevalence of False Contact Information for Registered Domain Names**

DHS IAIP Daily; http://www.gao.gov/new.items/d06165.pdf

INTERNET MANAGEMENT: PREVALENCE OF FALSE CONTACT INFORMATION FOR REGISTERED DOMAIN NAMES (REPORT)

Individuals or organizations seeking to register the names of their Websites may provide inaccurate contact information to registrars in order to hide their identities or to prevent members of the public from contacting them. Contact information is made publicly available on the Internet through a service known as Whois. Data accuracy in the Whois service can help law enforcement officials to investigate intellectual property misuse and online fraud, or identify the source of spam e-mail, and can help Internet operators to resolve technical network issues. The Government Accountability Office was asked, among other things, to (1) determine the prevalence of patently false or incomplete contact data in the Whois service for the .com, .org, and .net domains; (2) determine the extent to which patently false data are corrected within one month of being reported to the Internet Corporation for Assigned Names and Numbers (ICANN); and (3) describe steps the Department of Commerce and ICANN have taken to ensure the accuracy of contact data in the Whois database. Highlights: http://www.gao.gov/highlights/d06165high.pdf

---

Category 4C5 Academic/Industry/Vendor/Govt efforts

2005-11-08 **Liberty Alliance authentication protocols devices hardware software improvement efforts tokens biometrics**

EDUPAGE; http://news.zdnet.com/2100-1009_22-5940442.html

LIBERTY ALLIANCE LOOKS TO STRENGTHEN AUTHENTICATION

The Liberty Alliance has announced the creation of the Strong Authentication Expert Group, charged with developing standards of interoperability for authentication tools that go beyond simple passwords. User passwords are widely considered a weak link in the chain of efforts to safeguard online resources and transactions, and calls have gone out recently to add other layers of authentication. New layers could include hardware devices, password tokens, biometric identification, or others. The new group will develop a specification known as Identity Strong Authentication Framework (ID-SAFE), the first version of which is expected in 2006, according to the Liberty Alliance. American Express, Axalto, HP, Oracle, RSA Security, and VeriSign are among the members of the new group. All other members of the Liberty Alliance may also join. ZDNet, 8 November 2005

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2005-12-15 **computer science research laboratory lab University California Berkeley Reliable Adaptive Distributed Systems Google Microsoft Sun Microsoft nonproprietary freely licensed ACM**

EDUPAGE; http://www.nytimes.com/2005/12/15/technology/15research.htm

BERKELEY FUNDED FOR NEW RESEARCH LAB

Google, Microsoft, and Sun Microsystems plan to fund the Reliable, Adaptive, and Distributed Systems Laboratory at the University of California, Berkeley, to focus on the design of more dependable computing systems. According to Berkeley researchers involved with the new lab, research results will be nonproprietary and freely licensed. The three companies have pledged $500,000 each yearly for five years to support the project. The lab's founding director, computer scientist David Patterson, is currently president of the Association for Computing Machinery. According to Patterson, "We're trying to sustain the broad vision, high-risk, and high-reward research model" in establishing the new research facility. New York Times, 15 December 2005 (registration req'd)

Category 4C5 *Academic/Industry/Vendor/Govt efforts*

2006-03-27 **national IT disaster response council cyber attack response**

DHS IAIP Daily; 23
http://www.washingtontechnology.com/news/1_1/homeland/28284− 1.html

COUNCIL TO DRAW UP CYBER ATTACK RESPONSE.

Setting up a national IT disaster response apparatus is one possible topic to be addressed by the IT Sector Coordinating Council as it drafts a sector-specific plan for protecting the nation's computer networks against a terrorist attack or other disaster, according to the group's chairman. The goal is for private sector IT companies and government to work together to prevent and to respond to cyber attacks. The council wants ideas from the IT industry and from the Department of Homeland Security as it begins work on the sector-specific critical infrastructure protection plan at its Tuesday, April 4, meeting. The council expects to complete the plan by September.

4D Funny / miscellaneous

Category 4D *Funny / miscellaneous*

1997-01-30 **pornography**

EDUPAGE

In its defense of the Communications Decency Act, lawyers for the government argued that censoring the Net is designed to protect First Amendment rights by allowing parents to use the Net without fear for their children's moral development. The ACLU responded that this argument was outrageous and oxymoronic. For some survivors of the sixties, it reminded one of the satirical slogan, "Kill for Peace!" and other more risqué versions.

Category 4D *Funny / miscellaneous*

1997-02-25 **censorship CDA law**

EDUPAGE

Over two dozen organizations, including the American Association of University Professors, filed a brief in the U.S. Supreme Court in preparation for the deliberations over the constitutionality of the Communications Decency Act. The AAUP commented that it "is concerned that the CDA will chill online expression and discussion on a wide variety of academic subjects (e.g., medicine, biology, anatomy, social work, art, and journalism), impairing use of this promising new medium for legitimate pedagogical and research purposes."

Category 4D *Funny / miscellaneous*

1997-05-04 **law e-mail archives**

EDUPAGE

With more and more e-mail and other files being left on disks and tapes, lawyers find that the costs of discovery are sometimes so huge that lawsuits are being settled out of court just to avoid having to delve into the electronic mountains of material. More important, having plaintiffs required to dig through defendants' hard drives raises serious questions of industrial espionage. According to Judge Paul Niemeyer of the U.S. Court of Appeals in Baltimore, "I sense that discovery is being used as a tool of oppression, rather than as a tool of fairness."

Category 4D *Funny / miscellaneous*

1997-07-17 **speech recognition**

EDUPAGE

Lernout & Hauspie announced plans for voice-operated control over Microsoft Word. Commentators imagined a new form of hacking: yelling commands through open doors to bollix up voice-operated software. A hoax message instantly popped up claiming that at a demonstration, someone in the audience yelled "FORMAT C colon return" and another one yelled immediately "YES return" — ignoring the fact that the software cannot control DOS.

Category 4D *Funny / miscellaneous*

1997-09-30 **security paradigm criteria**

Information Systems Security Update 97 9

At the 13th International Information Security Conference, 14-15 May 1997 in Copenhagen, RAND Corporation's Willis Ware presented a paper on "New Vistas on Info-System Security" emphasizing the importance of moving away from DoD dogma that he characterized as "protect the system and data at any cost" and urged practitioners to emphasize protection at acceptable cost. Dr Ware's paper (RAND #P-7996) is available for $5 and shipping by searching on "Ware" using the engine at <http://www.rand.org/Abstracts/abstracts.html>.

Category 4D *Funny / miscellaneous*

1997-11-23 **social effects computerization**

EDUPAGE

Speaking at an OECD conference in November, Ira Magaziner (the White House Special Advisor on Technology) warned that the effects of increasing computerization will be as overwhelming as the industrial revolution. Millions of people will lose their jobs and millions of other people will take on new jobs, he said. One of the big questions, said the Director General of the OECD, Donald Johnston, is whether and how governments should tax transactions carried out internationally via the Internet.

Category 4D *Funny / miscellaneous*

1998-01-29 **social effects computerization**

EDUPAGE

The Canadian government commissioned a study of the social effects of increasing computerization. The predictions were not cheerful: the report, _Growth, Human Development, Social Cohesion_, warned that computerization could increase social inequality between the techno-illiterates and the cyber-elite with dire consequences for the future.

Category 4D *Funny / miscellaneous*

1998-02-27 **textbook collection papers articles reference**

RISKS 19 60

Professors Dorothy E. Denning and Peter J. Denning published an excellent collection of classic and updated papers in _Internet Besieged: Countering Cyberspace Scofflaws_ published by Addison-Wesley (Don Mills, ON). ISBN 0-201-30820-7. Regular RISKS contributor Robert M. Slade wrote, "[T]his work is both interesting and valuable. It should be of particular use to the student or teacher of data security, although there is much to hold the attention of any interested individual."

Category 4D *Funny / miscellaneous*

1998-02-27 **pornography TV cable quality assurance QA bug**

RISKS 19 60

Inveterate punster Peter G. Neumann wrote, "From at least 1 Feb 1998 until it was fixed on 10 Feb, at 5:20am each morning TCI gave San Francisco's Channel 27 viewers 40 minutes of free porn from the Adam-and-Eve network on its pay-per-view preview channel. (However, there were interruptions for commercials advertising similar stuff.) The glitch was attributed to the computer system turning off the masking supposedly provided by the scrambler, ahead of schedule. [Premature emasculation?]"

Category 4D *Funny / miscellaneous*

1998-05-21 **ergonomics repetetive strain injury RSI carpal tunnel**

EDUPAGE

Carnegie Mellon University researches found a significant increase in the occurrence of repetetive strain injuries among young people and academics. About 22% of the students, faculty and staff studied at several universities experienced RSI. With the increasingly early age of exposure to computers, proper ergnomic habits should be part of every computer course.

Category 4D *Funny / miscellaneous*

1998-06-10 **GPS buffer overflow rollover global positioning satellites**

RISKS 19 80

Pioneer electronics issued a worldwide recall on its older model GPS systems. The microprocessor code on these models failed to take into account the week-counter rollover that will occur at the end of Aug 21, 1999 in the GPS transmissions. At that time, the non-compliant receivers will be receiving data marked as having originated on 6 Jan 1980.

Category 4D *Funny / miscellaneous*

1998-06-23 **ISP vulnerabilities password policy publicity stunt contest**

RISKS 19 83

How Not To Solve ISP Security Problems: WorldOnline in the Netherlands was criticized for assigning passwords consisting of the first four letters of the user ID plus four digits. Instead of solving the problem, some bright light in the public relations department (1) denied that security was weak and then (2) started a contest with a $7500 for the first person to crack the system. The winner stole thousands of e-mail messages within a few days.

Category 4D *Funny / miscellaneous*

1998-12-28 **stupidity satellite navigation automobile user error**

RISKS 20 14

In a spectacular demonstration of slavish obedience, a pair of nitwits demonstrated the crucial role of observation and thought when using mission-critical technology. Peter G. Neumann wrote, "A German couple drove their BMW with great confidence under control of its computerized satellite navigation. Indeed, they drove it past a stop sign, down a ferry ramp, and into the Havel River in Caputh, near Potsdam/Berlin, Germany. The computer system reportedly neglected to tell them they needed to wait for the ferry. Ship traffic was stopped for two hours, but the couple was OK."

Category 4D *Funny / miscellaneous*

1999-01-15 **data leakage covert channel recording eavesdropping toy**

RISKS 20 16

The electronic stuffed toys called Furbys were declared machina non grata at government installations when the NSA realized that the little devils could record human speech and play it back. RISKS correspondent Bruce Martin wrote (in issue 20.16), "The risk of U.S. national security resting in the hands of adults who play with children's toys during office hours is left as an exercise to the reader."

Category 4D *Funny / miscellaneous*

1999-01-25 **operating system refund complaint UNIX PCs**

New York Times

A group of LINUX users announced plans to demand refunds from Microsoft because they were charged for unwanted installations of MS-Windows on PCs sold by various vendors. Microsoft frostily replied that there would be no refund.

Category 4D *Funny / miscellaneous*

1999-02-12 **software law legal interference judge court case self-help**

RISKS 20 21

Peter Neumann wrote in RISKS: "U.S. District Judge Barefoot Sanders is moving to ban the sale of self-help legal software such as Quicken Family Lawyer." [What more need one say?]

Category 4D *Funny / miscellaneous*

1999-02-22 **jargon English style punctuation capitalization newspseak**

SYDNEY MORNING HERALD (Australia)

John Huxley wrote an amusing article for the Sydney Morning Herald of Australia on the growing use of computer jargon in Silicon Valley and elsewhere. Some of his observations on new fashions in writing and speaking:
* being out of personal bandwidth.
* writing entirely in lowercase and without punctuation.
* use of abbreviations such as the "@" symbol and acronyms such as IMHO (In my humble opinion), OTOH (On the other hand), and G,D&R (Grin, duck and run).
* emoticons :-) (and one of Dave Barry's better gags, :-(8 — a person who is unhappy with the results of breast-enlargement surgery.
* Spammers = senders of unsolicited email.
* Marketing pukes = salespeople who know buzzwords but little else.
* Ponytails = artistic or creative people.
* SLIRKs = Smart Little Rich Kids — successful entrepreneurs or techno-criminals.
* WOMBATS = people who are a Waste of Money, Brains and Time.
* PEBCAK = Problem Exists Between Chair And Keyboard.
* FRED = Fucking Ridiculous Electronic Device.

Category 4D *Funny / miscellaneous*

1999-03-08 **stupid laws privacy regulations copyright download caching**

LA Times

In a spectacularly stupid move, the European Parliament issued a directive forbidding disk caching of Web pages. Any ISP serving European users would be banned from applying this simple technique, thus forcing a significant increase in bandwidth utilization and undoubtedly slowing access to all sites on the Net for everyone, not just Europeans. Internet Society CEO Don Heath commented, "The Internet does not need laws that slow its performance, clog its arteries and reduce value received," noting also that HTML already provides mechanisms for preventing caching of specific pages.

Category 4D *Funny / miscellaneous*

1999-05-05 **spoof virus spellcheck funny**

Washington Post

Bob Hirschfeld published an amusing spoof in the Washington Post in May 1999 in which he claimed that a new virus was paralyzing government and business by blocking ungrammatical e-mail."

Category 4D *Funny / miscellaneous*

1999-10-03 **CIA government investment**

Philadelphia Inquirer, New York Times, Washington Post

The CIA announced its new venture capital firm, In-Q-It, to funnel funds into high-tech firms. CEO Gilman Louie has no known experience in espionage or security; however, he did found a toy company later acquired by Hasbro.

Category 4D *Funny / miscellaneous*

2000-01-06 **criminal hackers gray-hat commercial company consulting**

AP,. New York Times, NewsScan, OTC, PC Week, TechnologyEvaluation.com

Eight self-described top computer hackers who were members of L0pht Heavy Industries formed a new consulting firm called @Stake in January 2000. These people insisted that they would continue to use their hacker handles (e.g., Mudge, Weld Pond, Space Rogue, Brian Oblivion, Dildog) and claimed that they did not break into systems illegally. They were described in glowing terms by such security luminaries as Counterpane's Bruce Schneier ("They're very, very good — first rate. . . .") and by NTBugtraq's Russ Cooper ("The eight brilliant geniuses down at the L0pht. . . ."). However, other commentators such as John Taschek of PC Week expressed horror at the move: "This is clearly an example of the farmer giving the fox the key to the chicken coop. I can't imagine that any legitimate startup would actually seek out L0pht." He added, ". . . L0pht's history shows that the group is not ethical, maintained practices that bordered on being illegal and is simply downright scary. I wouldn't want any organization that hired the brain trust of L0pht as my security consultant. "

Category 4D *Funny / miscellaneous*

2000-01-13 **mouse ergonomics carpal tunnel syndrome**

Edupage, New York Times

According to research by Cornell University's Prof. Alan Hedge, there may be an advantage to using a larger computer mouse. Tests suggested that the larger devices might reduce strain on fingers and wrists. The author explicitly refused to claim that changing mouses would reduce carpal tunnel syndrome but suggested it might help.

Category 4D *Funny / miscellaneous*

2000-05-22 **generational experience QA quality assurance**

RISKS 20 89

Zygo Blaxell wrote about an alarming tendency among those who have grown up with bad software:

>While at a bookstore the other day, my spouse was presented with a credit card signature slip printed by an Interac point-of-sale terminal. It was just like any other credit signature slip, except that the usual "customer signature" line was printed twice, one on top of the other, with ample space for the signature in both places — a harmless glitch, probably due to an obvious and simple programming error.

We pointed the error out to the cashier, who was probably barely old enough to be legally employed, and her response, if she speaks for her generation, was ominous, even terrifying:

"It does that because ... because it's a computer."

An entire generation is growing up believing that the current sorry state of affairs in information technology could ever be accepted as _normal_!<

Category 4D *Funny / miscellaneous*

2000-07-12 **spoof joke humor**

NewsScan, CNet http://news.cnet.com/news/0-1003-200-2249491.html

A humorous posting on Bugtraq, a popular computer security e-mail list, . . . [warned] that hackers have found a way to take over Sony's Aibo robot dog and command it to attack and perform other annoying canine tricks. The posting, written in the style of security alerts issued by the Computer Emergency Response Team (CERT), warns: "The buffer used to hold the variable MyOwner in the function process_face() can be overflowed, reverting Aibo into experimental AiboPitBull code." Other malicious codes that can affect Aibo's usually friendly and obedient nature include PeeOnRug(), ShoeChew() and KillTheCat(). In addition, "owners who accidentally have left their television on late at night have reported incidents of Aibo attacking their small children and pets within minutes of the airing of 'Tom Vu's Real Estate Seminar.'" CERT spokesman Shawn Hernan noted, "This is, of course, a forgery, but nonetheless pretty amusing." (CNet News.com 12 Jul 2000)

Category 4D *Funny / miscellaneous*

2000-07-14 **joke funny spoof amusing satire**

RISKS, segfault.org http://segfault.org/story.phtml?id=396f3e5c-0958dfa0 21

Leonard Richardson posted an amusing spoof of the usual responses to new breaches of cryptographic algorithms, availability of cracker tools, and so on. The satirical piece began, "The well-known polynomial x^2+8x+6 was defaced today by a teenager who had "r00ted" the beloved function of one variable through the use of a popular script known as "QuAd 3QaZh0n". The attack set off the usual sequence of events: an initial panic setting off an orgy of media hype reaching a crescendo with an article in the mainstream media, a string of copycat successors, and a meaningless stream of empty promises from vendors who immediately lapsed back into apathy as the incident left the public's short-term memory."

Category 4D *Funny / miscellaneous*

2001-01-03 **virus propagation e-mail joke satire funny amusing**

SatireWire; http://www.satirewire.com/news/0103/outlook.shtml

FOOT-AND-MOUTH BELIEVED TO BE FIRST VIRUS
UNABLE TO SPREAD THROUGH MICROSOFT OUTLOOK
Researchers Shocked to Finally Find Virus That Email App Doesn't Like

Atlanta, Ga. (SatireWire.com) — Scientists at the Centers for Disease Control and Symantec's AntiVirus Research Center today confirmed that foot-and-mouth disease cannot be spread by Microsoft's Outlook email application, believed to be the first time the program has ever failed to propagate a major virus.

"Frankly, we've never heard of a virus that couldn't spread through Microsoft Outlook, so our findings were, to say the least, unexpected," said Clive Sarnow, director of the CDC's infectious disease unit.

The study was immediately hailed by British officials, who said it will save millions of pounds and thousands of man hours. "Up until now we have, quite naturally, assumed that both foot-and-mouth and mad cow were spread by Microsoft Outlook," said Nick Brown, Britain's Agriculture Minister. "By eliminating it, we can focus our resources elsewhere."

However, researchers in the Netherlands, where foot-and-mouth has recently appeared, said they are not yet prepared to disqualify Outlook, which has been the progenitor of viruses such as "I Love You," "Bubbleboy," "Anna Kournikova," and "Naked Wife," to name but a few.

Said Nils Overmars, director of the Molecular Virology Lab at Leiden University: "It's not that we don't trust the research, it's just that as scientists, we are trained to be skeptical of any finding that flies in the face of established truth. And this one flies in the face like a blind drunk sparrow."

Executives at Microsoft, meanwhile, were equally skeptical, insisting that Outlook's patented Virus Transfer Protocol (VTP) has proven virtually pervious to any virus. The company, however, will issue a free VTP patch if it turns out the application is not vulnerable to foot-and-mouth.

Such an admission would be embarrassing for the software giant, but Symantec virologist Ariel Kologne insisted that no one is more humiliated by the study than she is. "Only last week, I had a reporter ask if the foot-and-mouth virus spreads through Microsoft Outlook, and I told him, 'Doesn't everything?'" she recalled. "Who would've thought?"

RECOMMEND
THIS PAGE

Category 4D *Funny / miscellaneous*

2001-03-13 **bugs history folklore**

NewsScan

WORTH THINKING ABOUT: THE HISTORY OF BUGS
Princeton University's Edward Tenner wants us to know that bugs, those notorious enemies of technology, have been around long before computers: "The bug, that perverse and elusive malfunctioning of hardware and later of software, was born in the nineteenth century. It was already accepted shop slang as early as 1878, when Thomas Edison described his style of invention in a letter to a European representative: 'The first step is an intuition and it comes with a burst, then difficulties arise -- this thing gives out and then that -- "Bugs" -- as such little faults and difficulties are called -- show themselves, and months of intense watching, study and labor are requisite before commercial success -- or failure -- is certainly reached.' "Edison implies that this use of 'bug' had not begun in his laboratory but was already standard jargon. The expression seems to have originated as telegrapher's slang. Western Union and other telegraph companies, with their associated branch offices, formed America's first high-technology system. About the time of Edison's letter, Western Union had over twelve thousand stations, and it was their condition that probably helped inspire the metaphor. City offices were filthy, and clerks exchanged verse about the gymnastics of insects cavorting in the cloakrooms. When, in 1945, a moth in a relay crashed the Mark II electromechanical calculator that the Navy was running at Harvard -- it can still be seen taped in the original logbook -- the bug metaphor had already been around for at least seventy-five years."

See http://www.amazon.com/exec/obidos/ASIN/0679747567/newsscancom/ for Edward Tenner's "Why Things Bite Back." (We donate all revenue from our book recommendations to Literacy Action's adult literacy programs.)

Category 4D *Funny / miscellaneous*

2001-04-30 **error message funny amusing QA quality assurance**

RISKS 21 37

Jean-Jacques Quisquater reported this gem to RISKS:

"Q276304 - Error Message: Your Password Must Be at Least 18770 Characters and Cannot Repeat Any of Your Previous 30689 Passwords"

Commented the correspondent dryly, "New level of security at Microsoft."

Category 4D *Funny / miscellaneous*

2001-05-05 **cryptography geek humor funny**

RISKS 21 42

Date: [not included]
From: "Keith F. Lynch" <kfl@KeithLynch.net>
Subject: Converting Pi to binary: DON'T DO IT! (via Russ Perry Jr.)

Newsgroup: alt.math.recreational

WARNING: Do NOT calculate Pi in binary. It is conjectured that this number is normal, meaning that it contains ALL finite bit strings.

If you compute it, you will be guilty of:

* Copyright infringement (of all books, all short stories, all newspapers, all magazines, all web sites, all music, all movies, and all software, including the complete Windows source code)
* Trademark infringement
* Possession of child pornography
* Espionage (unauthorized possession of top secret information)
* Possession of DVD-cracking software
* Possession of threats to the President
* Possession of everyone's SSN, everyone's credit card numbers, everyone's PIN numbers, everyone's unlisted phone numbers, and everyone's passwords
* Defaming Islam. Not technically illegal, but you'll have to go into hiding along with Salman Rushdie.
* Defaming Scientology. Which IS illegal -- just ask Keith Henson.

Also, your computer will contain all of the nastiest known computer viruses. In fact, all of the nastiest POSSIBLE computer viruses.

Some of the files on my PC are intensely personal, and I for one don't want you snooping through a copy of them.

You might get away with computing just a few digits, but why risk it? There's no telling how far into Pi you can go without finding the secret documents about the JFK assassination, a photograph of your neighbor's six year old daughter doing the nasty with the family dog, or a complete copy of the not-yet-released Pearl Harbor movie. So just don't do it.

The same warning applies to e, the square root of 2, Euler's constant, Phi, the cosine of any non-zero algebraic number, and the vast majority of all other real numbers.

There's a reason why these numbers are always computed and shown in decimal, after all.

Category 4D *Funny / miscellaneous*

2001-05-29 **spam humor etymology**

NewsScan

SPAM THE LUNCHEON MEAT
Look, we don't want to waste your time -- or ours. So here's the story: Hormel Foods, the maker of Spam luncheon meat, no longer minds if you use the lower-case word "spam" to refer to unsolicited commercial mail that invites you to make $$$, lose weight, or find new friendships. But if you want to say something about SPAM, the luncheon meat, use capital letters and show a little respect. It's not Hormel's fault that the name of its product was appropriated as a synonym for junk mail. So how did that happen? In an old Monty Python comedy routine, a group of Vikings bellowed a chorus of "spam spam spam spam" to drown out all other conversation, in the same way spam in your inbox makes it harder and harder to find real and important mail -- like NewsScan Daily. (San Jose Mercury News 29 May 2001)
http://www.siliconvalley.com/docs/news/svfront/026425.htm

Category 4D *Funny / miscellaneous*

2001-07-12 **default design flaw error QA quality assurance power failure charge charging rechargable batteries brake on switch**

RISKS 21 50

Ray Todd Stevens was in a store where wheelchairs with rechargeable batteries were lined up against a wall being recharged. Mr Stevens wrote in RISKS, "When the power failed, all of these units took off and most ran into things before the staff could stop them, trailing their cords behind them. . . . It seems that there are several . . . glaring design flaws in these units.

1. The stopped position on the handle is not the default position. Instead, the control is all the way down for forward, all the way up for reverse and half way in between for neither. Meaning that the nature position is forward.

2. There is also a foot brake, but it must be pushed to stop.

3. [The] power switch. . . . must be turned on to charge the unit.

. . . . They seem to assume that no electricity means that they are now to take off and do so driverless."

Mr Stevens added that we ought to be thinking about the default mode for computers and network equipment when planning for power failures.

Category 4D *Funny / miscellaneous*

2001-07-19 **automated alertness monitor automobile squirtgun water distraction startle emergency**

RISKS 21 53

[The following item from John Arundel in RISKS leaves this editor speechless:]

Annova notes an IBM system to stop drivers falling asleep at the wheel. It asks you questions and if you fail to respond promptly, it shoots a jet of cold water over you.
http://www.ananova.com/news/story/sm_355015.html

In the time-honoured phrase, "the RISKS are obvious". I wouldn't like to imagine the consequences if a driver was unexpectedly soaked with ice water during a high-speed overtaking manoeuvure on a motorway...

[FORDing the flood? CHEVY to the levee? NOVAcaine mutiny? PGN]

Category 4D *Funny / miscellaneous*

2002-01-19 **data compression advertising claims proof snake oil**

RISKS 21 87

Jeremy Epstein wrote, >Snake oil is on the rise. Latest to join the fray is Zeosync (www.zeosync.com), which announced on 7 Jan 2002 that they have new algorithms that can provide 100:1 lossless data compression over "practically random" data. (What they mean by "practically" isn't defined.) Lots of criticism and proofs that it's impossible in Slashdot http://slashdot.org/article.pl?sid=02/01/08/137246&mode=thread and elsewhere. So far the algorithms haven't been given, except to provide the single longest stream of buzzwords I've seen in a long time.<

MORAL: Be skeptical of miracles using undocumented methods.

Category 4D *Funny / miscellaneous*

2002-01-20 **Microsoft security initiative**

Security Wire Digest 4 5

Bill Gates' announcement in January 2002 caused ripples of amazement, incredulity, approval and encouragement in the IT and security industries. Writing in a memo to employees, Gates affirmed, "When we face a choice between adding features and resolving security issues, we need to choose security. Our products should emphasize security right out of the box, and we must constantly refine and improve that security as threats evolve."

Shawna McAlearney and Anne Saita wrote in Security Wire Digest, "Gates's proclamation comes after the U.S. National Academy of Sciences (NAS) recommended that Congress create laws that punish software companies that knowingly release flawed and insecure products. The BBC last week reported the NAS Computer and Telecommunications Board suggests in a preliminary report that U.S. laws be amended to make software producers liable if their products pose a public or business risk."

Category 4D *Funny / miscellaneous*

2002-01-29 **search engine play game bandwidth denial-of-service attack resource exploitation saturation**

NewsScan

GOOGLEWHACKING GAINS POPULARITY
Googlewhacking -- an offbeat pursuit of bored Web surfers -- is increasing in popularity and spawning its own legion of enthusiasts. The game starts by typing two unrelated words, such as colonoscopy and cockatiel, into Google's search bar, with the goal of obtaining a single result. The challenge is to find two words so disparate that only one match will occur among Google's 3 billion indexed Web pages. The idea originated with Gary Stock, who tracks the trend on his Web site (http://www.unblinking.com/heh/googlewhack.htm). "It used to be people wandered around the Web, but today people find themselves a space and stay there too much," says Stock. "To me, this is a good way to get people to learn." (CNet News.com 29 Jan 2002)
http://news.com.com/2100-1023-825602.html

Category 4D *Funny / miscellaneous*

2002-02-08 **geek humor music rock 'n' roll logic gates circuit design**

NewsScan

COMPUTERS AND ROCK 'N' ROLL: THAT'S WHAT IT'S ALL ABOUT
In the current issue of Computer magazine, former Intel computer architect Bob Colwell has an amusing piece on the relation between computers and rock 'n' roll, and here's a sample: "I particularly like spotting the correspondences between the arts and sciences. For example, you might not think a rock musician would understand what an inverter logic gate does, but apparently Eric Clapton does in his song 'Opposites': "Night after day, day after night./White after black, black after white./Fight after peace, peace after fight./Life after death, death after life." Colwell comments that "Clapton clearly understands that there is a time delay involved in propagating through the gate -- hence the word 'after.' When he figures out AND and OR gates, Clapton will be able to devise entire computers in his lyrics. Wait -- maybe that's what 'I Shot the Sheriff' is all about. Never could figure out why it was okay to shoot the sheriff but not the deputy. But that construction is very clearly a conjunctive logical expression (S AND NOT D -- hey, maybe that's why he needed the inverter)." To explain functional languages, Colwell analyzes the lyrics of "The Locomotion": "Ev'rybody's doin' a brand new dance now./ C'mon baby, do the locomotion./ I know you'll get to like it if you give it a chance now./ C'mon baby, do the locomotion." And vector processing? Well, what better example than "The Hokey Pokey": "You put your right foot in,/ You put your right foot out,/You put your right foot in,/And you shake it all about./You do the Hokey-Pokey,/ And you turn yourself around./That's what it's all about!" (IEEE Computer Feb 2002)
http://www.computer.org/computer/homepage/0202/ar/index.htm

Category 4D *Funny / miscellaneous*

2002-04-01 **joke**

RISKS 22 01

Yet another entry in the RISKS April-Fool's Day celebration:

Date: Mon, 21 Jan 2002 23:07:30 -0500
From: Gene Spafford <spaf@cerias.purdue.edu>
Subject: Surprise Settlement Evenly Splits Microsoft (unknown source)

[From SatireWire, via various intermediaries. Reprised for the occasion. PGN]

Decision Keeps Redmond from Monopolizing Massive Microsoft Patch Industry

Surprise Settlement Evenly Splits Microsoft; One Firm To Make Software, Other To Make Patches

Redmond, Wash. In a surprise settlement today with nine U.S. states, Microsoft agreed to be split into two independent companies -- one that will continue to make Microsoft operating systems, browsers, and server software, and another, potentially larger company that will make patches for Microsoft operating systems, browsers, and server software.

Critics immediately charged that the settlement -- which overrides a previous agreement with the U.S. Department of Justice -- does nothing to diminish Microsoft's standing as the world's most powerful software company. But industry analysts argued that providing patches for security holes in Microsoft programs is a major, untapped growth industry, and applauded the states for not allowing Redmond to control it.

"Just consider, Microsoft can make an operating system, such as Windows XP, and sell 200 million copies, but each one of those copies is going to need at least five patches to fix security holes, so that's 1 billion patches," said Gartner Group analyst Mitch Fershing. "That is an enormous, undeveloped market."

Microsoft employees seem to agree, as sources in Redmond described a "mad scramble" among staffers to position themselves for spots at the new company, called Patchsoft. Asked why people would want to leave Microsoft for a startup, the source said the answer was "really quite simple."

"Everyone here is asking themselves, 'Do I want to be part of the problem, or part of the solution?'" he said.

But J.P. Morgan analyst Sherill Walk suspects another motive. "Considering the sheer number of patches we're talking about, I think the new company will become another monopoly, and I believe the people who've jumped ship very well know that."

"Nonsense. It's really all about consumer choice," responded Patchsoft's new co-CEOs, Bill Gates and Steve Ballmer.

But how will Patchsoft make money? Currently, Microsoft issues free patches for problems in Windows XP, SQL Server, Internet Explorer, Outlook, Windows 2000, Flight Simulator, Front Page, Windows Me, Media Player, Passport, NT Server, Windows 98, LAN Manager (for a complete list of MS software needing patches, see www.support.microsoft.com). Under the agreement, Microsoft will no longer issue patches, which Gates said explains the recent five-day outage at Microsoft's upgrade site. "That was planned," he said. "It was a test of the Microsoft No Patch Access system. Went perfectly. No one was able to download anything."

At a press conference to outline the settlement, Connecticut Attorney General Richard Blumenthal pledged to keep a close eye on Patchsoft to ensure it would not overcharge for its services. He also expressed hope that other firms would soon become Certified Microsoft Patch Developers (CMPDs) and challenge the spin-off. Asked if Patchsoft, with so many former Microsoft employees, will have an advantage over potential competitors in the Microsoft patch market, Blumenthal said the settlement prohibits collaboration.

"Patchsoft developers will not have any foreknowledge of bugs or security holes before software is released. They'll just have to be surprised," he said.

"So it will be just like it was when they were at Microsoft," he added.

One Reuters reporter, meanwhile, questioned the long-term viability of Patchsoft. "This seems like a logical split right now, but what if Microsoft's products improve to the extent that patches are needed less frequently, or perhaps not at all?" she asked.

"I'm sorry, I can only respond to serious questions," Blumenthal answered.

Category 4D *Funny / miscellaneous*

2002-04-01 **joke**

RISKS 22 02

Date: Mon, 01 Apr 2002 08:54:41 -0800
From: Crispin Cowan <crispin@wirex.com>
Subject: Announcing Immunix SnackGuard

New Product Release: SnackGuard WireX Communications, Inc., 1 Apr 2002

[This arrived too late for the April Fool's Issue, but better late than never? (Or better never than later?) PGN]

WireX is pleased to announce the latest addition to the Immunix family of security tools: SnackGuard. SnackGuard effectively guards your favorite snacks in the break room from "snack smashing" attacks: the predations of other hungry engineers. This protection is especially vital in these trying times of unemployment, when nomadic tribes of hunter/gatherer geeks roam the halls of once mighty dot.com's in search of food and caffeine.

Following on StackGuard's "canary" defense, SnackGuard employs WireX's patent-pending "turkey" defense: when SnackGuard detects the "gobbling" noise of some turkey scarfing down your favorite pop tarts and heavily caffeinated beverages, it issues a pink slip, halting the gobbler.

While SnackGuard is effective in defending your snacks, it is not without costs. SnackGuard increases run time when you are running to catch the bus or the elevator, in that successful defense of your snacks tends to increase "programmer's butt". Excessive consumption of caffeinated beverages without intervening bathroom breaks may also induce personal "buffer overflows".

While SnackGuard is "free speech", it is not "free beer": you may modify and distribute this gag as you wish, but go buy your own brewskis.

Crispin Cowan, Ph.D., Chief Scientist, WireX Communications, Inc.
http://wirex.com Security Hardened Linux Distribution
http://immunix.org

Category 4D *Funny / miscellaneous*

2002-04-01 **joke**

RISKS 22 01ff

Rob Slade published a hilarious sendup of his usual book reviews, this time proposing that Bill Murray and Gene Spafford were the madcap authors of _Hacking for Dummies_ and adding digs at familiar security icons throughout the review:

>Date: Mon, 1 Apr 2002 07:19:57 -0800
From: "Rob, grandpa of Ryan, Trevor, Devon & Hannah" <rslade@sprint.ca>
Subject: REVIEW: "Hacking for Dummies", Bill Murray III/Gene Spafford

BKHAKDUM.RVW 20020401

"Hacking for Dummies", William Hugh Murray III/Eugene Spafford, 1802,
076455302X, U$21.99/C$437.84
%A William Hugh Murray III whmurray3@spryguy.com
%A Eugene Spafford spif@serious.purdue.edu
%C 155 Divet Road, Suite 310, San Mateo, CA 94402
%D 1902
%G 076455302X
%I International Data Group (IDG Books)
%O U$21.99/C$411.95 415-312-0650 fax: 415-286-2740
%P 166 p.
%S for Dummies
%T "Hacking for Dummies"

As regular RISKS readers will note, I always enjoy a new addition to the "for Dummies" series. This time the imprint has outdone itself with a lighthearted romp through network naughtiness, by two of the least known, but most accomplished, practitioners of the field.

Some may question the need for such a work, but the authors maintain that they are performing a valuable service to corporations and society at large. "A vital system security penetration community is important," they state in the introduction. "It thins the herd of security practitioners. We have a moral responsibility to ensure that those who, not having the authority to fire people who insist on using Outlook, get blamed when major events happen and are forced to look for work in other fields."

In a switch from the standard format, the "Part of Tens" comes first, pointing out how to knock holes in each of the ten domains of the security common body of knowledge. This sets up a series of helpful icons used to point out specific attacks that can be mounted against each domain. (Security management attacks tend to get a bit repetitive after a while: there are only so many ways of rewording the advice to pretend to be the CEO's secretary.)

Some common and handy attacks (such as the ubiquitous brute force denial-of-service attack, featuring a sledgehammer) are listed, but there are a number of little-known tricks, like the means of attacking a computer that has been sealed in a lead-lined vault, surrounded by armed guards, and cast in concrete. Dorothy Denning's sidebar on starting wars by manipulating e-mail systems is particularly interesting. Security professionals are not ignored: in an interesting display of fair-mindedness, the authors suggest that incident-response team members prepare by ensuring they always have plenty of sugar in their gas tanks for extra energy on late-night calls.

Critical reaction to the tome has been spirited but mixed. Winn Schwartau, in the foreword, asks "is it moral, is it ethical" to provide such information to the general public, before concluding, "Who cares? Nobody has time for this." Phil Zimmermann has roundly condemned the section on anonymous communications, stating that the government has a legitimate need for access to private communications, while Fred Cohen is upset that the authors suggest viruses could be used for beneficial purposes. Richard Stallman is reported to be disturbed by the position that software

development can take place in the kind of anarchic environment promoted by the book, and has launched a campaign to ensure that everyone has valid licenses for Microsoft products. Bruce Schneier, on the other hand, points out that the information in the book presents no danger to the public. "As long as you've got a strong crypto algorithm and good technical solutions, it doesn't matter about implementation and people."

rslade@vcn.bc.ca rslade@sprint.ca slade@victoria.tc.ca p1@canada.com
http://victoria.tc.ca/techrev or http://sun.soci.niu.edu/~rslade

---

RISKS 22.02

Date: Thu, 4 Apr 2002 12:21:17 PST
From: "Peter G. Neumann" <neumann@csl.sri.com>
Subject: April Foolishness

Quite a few people have apparently gone to Amazon.com to order "Hacking For Dummies" -- a bogus (i.e., nonexistent) book reviewed by Rob Slade in RISKS-22.01. Perhaps, not surprisingly, the ISBN bears a strange resemblance to the ISBN for "S*x for Dummies". We have to call a Slade a Slade. Perhaps his review was too subtle? Perhaps your fearless moderator needs to be more obvious in highlighting April Fools' items, besides putting it up front in the issue rather than buried in its usual end-of-the-issue position? Aw, come on! April Fool's Day is seemingly a worldwide tradition, and that's part of the fun.<

Category 4D *Funny / miscellaneous*

2002-04-01 **joke**

RISKS 22 01

On April Fools, Peter Neumann's traditional joke issue of the RISKS FORUM DIGEST published a tongue-in-cheek report on the addition of software piracy law enforcement to the duties of the Bureau of Alcohol, Tobacco and Firearms:
>WASHINGTON (Reuters) - The Department of the Treasury announced today that responsibility for enforcement of new federal regulations of the software industry will fall under the jurisdiction of the Bureau of Alcohol, Tobacco and Firearms (ATF). As the regulations come into effect, the bureau will be renamed to be the Bureau of Alcohol, Tobacco, Firearms, and Software (ATFS).

The new regulations have been taken by most observers as a key indication of the Federal Government's serious concern over the software production scandal gripping the nation. The final verdict of the grand jury investigation into the dangers of unregulated software production was praised as a major victory by software leaders in Redmond last month.

The grand jury investigation centered on the disturbing trend that key portions of the nation's critical infrastructure are being entrusted to a software product for which the secret inner workings (known as `source code') are becoming as prevalent as pornography on the Internet.

The Director of the ATF's 5,000-strong team of agents has pledged his full support to enforce the new regulations, under which all software development must take place only in licensed facilities by trained induhviduals. He was joined at a press conference this morning by the Director of the National Infrastructure Protection Center, who said, "It's about time the ATF took the entire software industry into its jurisdiction." He continued, "We would never consider laying the blueprints for our critical assets out for all to see. I applaud the new regulations for bringing sanity to a long unchecked industry."

The public will have until 1 Jun 2002 to dispose of all unregulated software products they may own. Possession of unlicensed software products can result in penalties up to 20 years in jail and multi-million dollar fines. Currently, only Smallsoft of Redmond, Washington, has achieved the necessary regulatory status to produce software in compliance with the new regulations.

An underground group of activists using the moniker ``the Electronic Frontier Foundation" (EFF) has been strongly critical of the Federal Government's position throughout. Police have indicated the violent clashes are expected between supporters of the EFF and US Presidential nominee Billy Doors, the major proponent of the regulations, as he addresses business leaders in Winnemucca, Nevada, this afternoon.

[I suppose we can understand why they chose the acronym ATFS, given alternatives such as FATS, AFTS, FAST, etc. PGN]<

Category 4D *Funny / miscellaneous*

2002-04-01 **joke**

RISKS 22 01

Date: Mon, 1 Apr 2002
From: Peter Neumann <risks@sri.com>
Subject: Computers to Cars (unknown source)

[I have had several requests for including this item in RISKS from those who have not yet seen it, even though it has been circulating for a while. I have no idea who originally created it, but I am grateful to the author for his or her incisive observations. PGN]

For all of us who feel only the deepest love and affection for the way computers have enhanced our lives:

At a recent computer exposition (COMDEX), Bill Gates reportedly compared the computer industry with the auto industry and stated: "If General Motors had kept up with the technology like the computer industry has, we would all be driving $25.00 cars that got 1,000 miles to the gallon."

In response to Bill's comments, GM issued a press release stating: "If General Motors had developed technology like Microsoft, we would all be driving cars with the following characteristics:

1. For no reason whatsoever, your car would crash twice a day.

2. Every time they repainted the lines in the road, you would have to buy a new car.

3. Occasionally your car would die on the freeway for no reason. You would have to pull over to the side of the road, close all of the windows, shut off the car, restart it, and reopen the windows before you could continue. For some reason, you would simply accept this.

4. Occasionally, executing a maneuver such as a left turn would cause your car to shut down and refuse to restart, in which case you would have to reinstall the engine.

5. Macintosh would make a car that was powered by the sun, was reliable, five times as fast and twice as easy to drive -- but would run on only five percent of the roads.

6. The oil, water temperature, and alternator warning lights would all be replaced by a single "General Protection Fault" warning light.

7. The airbag system would ask "Are you sure?" before deploying.

8. Occasionally, for no reason whatsoever, your car would lock you out and refuse to let you in until you simultaneously lifted the door handle, turned the key and grabbed hold of the radio antenna.

9. Every time GM introduced a new car, car buyers would have to learn to drive all over again because none of the controls would operate in the same manner as the old car.

10. You'd have to press the "Start" button to turn the engine off.

Category 4D *Funny / miscellaneous*

2002-04-22 **social engineering joke unexpected consequences**

RISKS 22 04

At the University of New South Wales, Geoffrey Brent runs a discussion list on which he posted an amusing April Fool's joke to illustrate many of the features of hoaxes. One of the list participants was taken in, however, and vented embarrassingly in front of the whole list. Realizing he'd been fooled, he became nasty and even physically threatening; he eventually had to be thrown off the list. Brent commented in RISKS, "The (April Fool-specific) risks: Forgetting that there will ALWAYS be somebody who doesn't get the joke, no matter how obvious you make it - and that human failure modes are just as bizarre and dangerous as technological ones."

[MK comments: This incident illustrates one of the dangers of any security testing that includes social engineering: embarrassing the victims. I have long held that one should be extremely careful in running social engineering simulations during penetration tests; one way to avoid trouble is to ensure that everyone is prepared for the tests so they can treat the whole thing as a contest.]

Category 4D *Funny / miscellaneous*

2002-09-30 **spam joke funny poem satire spoof parody**

NewsScan

OUT, DAMNED SPAM!
Seeing increasing spam spam spam in his mail, the NewsScan Poet Laureate, Andrew Rafalski, turned for inspiration to Shakespeare and to Macbeth's famous soliloquy in Act II, Scene I in Shakespeare's play. (Surely you're not surprised that we have our own Poet Laureate!). Here is Andrew Rafalski's Spam Soliloquy:

Is this junk mail which I see before me, And headed my way? Come let me trash you: I keep you not and yet I get you more. Are you not, virtual gunk, sensible To feelings and to right? Or are you but A mail for the can, unwanted spam Never to be opened, read or replied? . I get you still, in numbers virtual And unwanted, numbing My mailbox with cache overfilled. You lead me to trash you and revile you, Ignore and defile you. Hotmail and Yahoo I was to use But now both are flooded with Nonsense, gobbledygook and lies. . I see you still, and on your Subject lines, deception, deceit And fabrication. Your marketing Eyes polluting the ether, the net And my mailbox to boot. Out, damned spam! Out, I say! What! Will this mailbox ne'er be clean?

Category 4D *Funny / miscellaneous*

2003-03-24 **Microsoft security advertisement withdrawn South Africa software vulnerable**

NewsScan

ADVERTISING AUTHORITY TELLS MICROSOFT: 'NOT SO FAST THERE'

South Africa's Advertising Standards Association has forced Microsoft to withdraw a magazine ad suggesting that Microsoft's software is now so secure that it has almost made hacking as extinct as the dodo, the wooly mammoth, and the sabre-tooth tiger. A freelance journalist had called attention to the ad and claimed it was untrue because Microsoft software has been shown to have many vulnerabilities. (VNUnet 24 Mar 2003)

Category 4D *Funny / miscellaneous*

2003-07-29 **Pentagon DARPA INFOWAR betting assassinations contracts Middle East**

NewsScan

PENTAGON'S ONLINE TRADING MARKET PLAN DRAWS FIRE
The U.S. Defense Department's Defense Advanced Research Projects Agency (DARPA) has plans to set up an online Policy Analysis Market that will allow traders to bet on the likelihood of future terrorist attacks and political assassinations in the Middle East. The bizarre scheme has drawn fire from Senators Ron Wyden (D-Ore.) and Byron Dorgan (D-N.D.). "The idea of a federal betting parlor on atrocities and terrorism is ridiculous and it's grotesque," said Wyden, while Dorgan described the plan as "useless, offensive and unbelievably stupid. How would you feel if you were the King of Jordan and you learned that the U.S. Defense Department was taking bets on your being overthrown within a year?" However, the Pentagon defended the initiative, comparing it to commodity futures markets. "Research indicates that markets are extremely efficient, effective and timely aggregators of dispersed and even hidden information. Futures markets have proven themselves to be good at predicting such things as election results; they are often better than expert opinions." The market would allow traders to deposit money in an account and then use it to buy and sell contracts. If a particular event comes to pass, the bettors who wagered correctly would win the money of those who guessed wrong. (BBC News 29 Jul 2003)

Category 4D *Funny / miscellaneous*

2003-09-04 **virus names sophos anna kournikova VBSWGJ**

NewsScan

WHAT'S IN A VIRUS NAME?
Did you ever wonder who's responsible for all those quirky virus names making the news headlines from time to time? There are macho names, like Blaster, Chernobyl and Slammer; cute ones like Birthday, Smile and Teddy Bear; steamy ones like DeepThroat, Hooker and NakedWife; and nonsense names like Klez, Nimda and Yaha. Then, of course there are those names that seem to refer to the virus creator, like Brat, Faker and Slacker. "Sometimes it's obvious what to call a new virus because it's similar to a previous virus, or contains a message inside its code," says Chris Beltoff, security analyst with Sophos. "Other times analysts have to seek inspiration — I remember there was one which was named after the meal a virus analyst had just had." There *are* some rules: researchers are not supposed to name viruses after businesses, brand-name products or celebrities. That's why the Anna Kournikova virus is officially know as VBSWG.J. But sometimes analysts just have to scan those memory banks to come up with something appropriate. Researcher George Smith recalls naming one particularly shoddy virus "Heevahava" after a childhood memory: "I grew up in Pennsylvania Dutch country and a heevahava was the farmhand given the job of holding the bull's pizzle during the collection of semen. Locally, heevahava was used as an insult meaning 'dolt' or 'idiot.'" (Wired.com 4 Sep 2003)

Category 4D *Funny / miscellaneous*

2004-01-06 **puns computer Internet security funny**

RISKS 23 14

PUN-INTENDED DEFINITIONS

RISKS moderator Peter Neumann lists a few pun-ful computer-related definitions from _The Sunday San Jose Mercury_ (January 4, 2004):

off-shorn: vt. Getting cut because your job moved overseas. [Rainer Richter, San Jose]

Microsofa: n. A piece of furniture that, while it looked fine in the showroom, gradually begins to dominate the living room, eventually forcing you to replace all the other furniture, including the TV, to be "compatible". [Earl T. Cohen, Fremont]

motherbored: n. In many homes, a technology discussion at dinner between father and the kids. (Bruce Kerr)

Luddate: n. Someone you are going out with who does not understand the [Santa Clara] Valley's obsession with technology. (Lisa Lawrence, Palo Alto)

Crisco: n. A person who got fried by buying Cisco at $80 a share. (Jim Schutz)

Category 4D *Funny / miscellaneous*

2004-01-12 **Potato computer scam Germany fraud**

NewsBits; http://zdnet.com.com/2110-1105_2-5139288.html

'Potato' computer scam under investigation

German police are investigating after an angry man returned a computer he had just bought saying it was packed with small potatoes instead of computer parts. The store replaced the computer free of charge but became suspicious when he returned a short time later with another potato-filled computer casing, police in the western city of Kaiserslautern said on Monday. ``The second time he said he didn't need a computer any more and asked for his money back in cash,'' a police spokesman said. Police are now investigating the man for fraud.

Category 4D *Funny / miscellaneous*

2004-03-21 **psychology cyberspace honesty open up online permanent records**

NewsScan

THE ONLINE HONESTY PARADOX

Cornell University professor Jeffrey Hancock conducted an experiment recently that concluded people are less likely to fib online than when talking in person or on the phone. While this proposition flies in the face of warnings over psycho-weirdos lurking in chat rooms and on cyber-dating sites, New York Times columnist Clive Thompson says actually it makes sense, considering the relative durability of the e-mail message. While a lie spoken in person or over the phone can later be denied, on the Internet, your words may come back to haunt you. "Today's titans of industry are laid low not by ruthless competitors but by prosecutors gleefully waving transcripts of old e-mail, filled with suggestions of subterfuge… We all read the headlines; we know that in cyberspace our words don't die, because machines don't forget." A second contributing factor, says Thompson, is that there's "something about the Internet that encourages us to spill our guts, often in rather outrageous ways. Psychologists have noticed for years that going online seems to have catalytic effect on people's personalities." Indeed, an experiment conducted by Open University psychologist Adam Johnson found that strangers chatting online were much more likely to offer up personal details about themselves than when conversing face-to-face. "Our impulse to confess via cyberspace inverts much of what we think about honesty," says Thompson, citing the current corporate convention of flying cross-country for that all-important five-minute face-to-face meeting before signing off on a deal. Instead, Thompson suggests that "as more and more of our daily life moves online, we could find ourselves living in an increasingly honest world, or at least one in which lies have ever more serious consequences." (New York Times 21 Mar 2004)

Category 4D *Funny / miscellaneous*

2004-03-30 **super computer laptop flash mob gathering processing power**

DHS/IAIP Update

March 29, New Scientist — Flash mob to attempt supercomputing feat.

An attempt to transform a motley collection of laptops into the first ad-hoc supercomputer is scheduled for April 3 at the University of San Francisco. Over 1000 laptop owners will gather in the university gym in an attempt to build a "flash mob" supercomputer. The project's organizers hope that FlashMob will run fast enough to beat supercomputers in the list of the world's top 500 supercomputers. One of the challenges facing John Witchel, the USF graduate student running the project, and his colleagues, is that "You essentially don't know anything about the computers until they show they up that day." The team therefore had to write code that not only allows the computers to share lots of data quickly, but also determines each processor's speed and memory as it goes. This allows the computational tasks to be allocated in the most efficient way possible. To beat the slowest computer in the top 500, FlashMob will have to perform a rigorous mathematical calculation called Linpack at a rate of at least 403 billion flops (floating point operations per second).

Category 4D *Funny / miscellaneous*

2004-05-04 **computers health research disease fighting MIDAS initiative NIH**

DHS IAIP Daily; http://www.nih.gov/news/pr/may2004/nigms−04.htm

May 04, National Institutes of Health — Computers combat disease.

A new initiative, called MIDAS, will develop powerful computer modeling techniques to analyze and respond to infectious disease outbreaks, whether they occur naturally or are released intentionally in a bioterrorist attack. MIDAS is sponsored by the National Institute of General Medical Sciences (NIGMS), a part of the National Institutes of Health (NIH). NIGMS recently awarded the first four grants in this new initiative, totaling more than $28 million over five years. Three of these grants will support the creation of mathematical models to study various aspects of infectious disease epidemics and community responses. These research grants together total $9.5 million over five years. A fourth award, totaling $18.8 million over five years, funds researchers to develop a central database to organize information from the other three groups. It also supports the development of user-friendly computer modeling tools for the broader scientific community, policy makers and public health officials to use to simulate epidemics, and response strategies.

Category 4D *Funny / miscellaneous*

2004-05-17 **cartoon character terrorist intelligence search engine homeland security**

NewsBits;
http://www.usnews.com/usnews/issue/040517/whispers/17whisplead_2.htm

THE GOOGLE TERRORIST

It was the lead item on the government's daily threat matrix one day last April. Don Emilio Fulci described by an FBI tipster as a reclusive but evil millionaire, had formed a terrorist group that was planning chemical attacks against London and Washington, D.C. That day even FBI director Robert Mueller was briefed on the Fulci matter. But as the day went on without incident, a White House staffer had a brainstorm: He Googled Fulci. His findings: Fulci is the crime boss in the popular video game Headhunter. "Stand down," came the order from embarrassed national security types.

Category 4D *Funny / miscellaneous*

2004-06-01 **online newspaper reading increase India China Russia news entertainment**

NewsScan

ONLINE NEWSPAPER READERSHIP UP 350% OVER 5 YEARS

The audience for online versions of newspapers has grown 350% over the past five years, according to the World Association of Newspapers, which notes that while print circulation figures have declined in mature markets like Europe and the U.S., they are sharply up in emerging markets
like China and India. In Russia, the number of published dailies has nearly doubled in two years. WAN attributed the increase in online newspaper popularity to the growth of broadband in many countries, noting that in those countries where broadband Internet access is more readily available,
people are watching TV less and surfing the Web more, both for news and for entertainment. (BBC News 1 Jun 2004)

Category 4D *Funny / miscellaneous*

2004-06-14 **Matsuhita Eletric Japan sleep room 30-minute assesment sleep deprived profile**

NewsScan

MATSUSHITA DEBUTS HIGH-TECH 'SLEEP ROOM'

Matsushita Electric Works is taking the wraps off its "Sleep Room" next week in Tokyo, giving the sleep-deprived a chance to analyze their sleep patterns and catch 40 winks while they're at it. The company says its new product is geared toward the growing market of insomniacs in a country
where students start burning the midnight oil in elementary school -- a pattern that's then replicated in the typical workday. A Health Ministry survey indicated in 2000 that 31% of Japanese don't get enough sleep because of work, school or long commuting times. Another 29% cited stress
as a prime source of wakefulness. At Matsushita's "Vitality Diagnostic Corner," visitors are greeted by a "sleep counselor" who leads them through a 30-minute software program designed to pinpoint sleep problems and develop a "sleep profile." Customers can then try out a 30-minute session
in the sleep room, where they're greeted by a wall-sized TV displaying a soothing river scene surrounded by forest and augmented by gentle guitar and piano music blended with gurgling water and bird sounds. After a few minutes, the lights dim, the TV screen goes blank, and the bed's mattress kicks into gear, vibrating and kneading strategically to administer a massage and ease the customer into sleep. After 30 minutes, the lights slowly come on and the TV displays a crystal lake, while the bed gradually cranks up to a sitting position. The company plans to market the device to
homeowners for $30,000, and says even though the price is high, there will be takers. "Nobody who's come in here for 30 minutes hasn't fallen asleep," says a Matsushita official. (AP/USA Today 14 Jun 2004)

Category 4D *Funny / miscellaneous*

2004-08-15 **supercomputer link security 150 fastest US Department of Energy**

DHS IAIP Daily;
http://www.eweek.com/article2/0%2C1759%2C1636023%2C00.asp

August 15, Associated Press — Computer could link workers, stay secure.

A new supercomputer could join workers at the Idaho National Engineering and Environmental Laboratory in Idaho Falls, ID, with colleagues in France, Chile and across the U.S. while keeping sensitive information secure. The system could reach speeds of up to 1,500 gigaflops, making it one of the 150 fastest supercomputers in the world, officials said. Calculations and models that formerly took researchers a year will only take days to complete using the new system, officials said. Researchers will use the supercomputer to design the next generation of nuclear power plants, research the cause of mad cow disease and develop microbes that can eat heavy metals to use cleaning up contaminated sites. Those outside the laboratory must be approved by the U.S. Department of Energy to use the system. The computer can isolate information, essentially giving each user its own part of the system to control, Greenwade said.

Category 4D *Funny / miscellaneous*

2004-08-26 **Friday no e-mail Veritas employee communication face-to-face**

NewsScan

COULD 'E-MAIL-FREE' FRIDAYS REPLACE KHAKIS AND KNIT SHIRTS?

We all know that e-mail is turning into a huge time and productivity sink, but one lone crusader in Silicon Valley is trying to do something about it. Two months ago Jeremy Burton at Veritas Software decreed that Fridays in his marketing department were to be "e-mail free" -- employees
who needed to communicate with each other were instructed to stop by and chat or use the phone. "E-mail is supposed to be this big productivity tool, but it's getting to the point where it is out of control," says Burton, who complains that he was regularly spending two hours a day just dealing with e-mail. The ban applies only to interdepartmental communications and violators are fined $1 per transgression, with the proceeds going toward charity (so far, almost $70 has been collected). Many workers have endorsed the ban, noting the advantages of face-to-face conversations, and Burton says he plans to continue the policy indefinitely. (Wall Street Journal 26 Aug 2004)

Category 4D *Funny / miscellaneous*

2004-11-02 **study top technology nations world Information Society Index ISI Denmark Sweden US Switzerland**

DHS IAIP Daily;
http://management.silicon.com/careers/0,39024671,39125505,00 .htm

November 02, Silicon.com — Top tech nations revealed.

Denmark is the most technologically savvy nation, taking the top spot from Sweden. Sweden is now second, followed by the U.S., Switzerland and Canada. The rankings are based on the IDC Research's Information Society Index (ISI), which aims to measure the ability of 53 countries to access and use information technology. IDC rates each country on a total of 15 variables in four areas: computers, internet, telecoms and social. David Emberley, senior analyst for the IDC, noted a new trend this year - less of a link between social and technology scores. Previously companies with high social rankings tended to have a high level of technology. Report: http://www.idc.com/groups/isi/main.html

---

Category 4D *Funny / miscellaneous*

2005-01-06 **Welsh university supercomputer Government fastest Swansea IBM college biology research studies disease prevention Wales**

EDUPAGE; http://news.bbc.co.uk/2/hi/uk_news/wales/4150285.stm

WELSH UNIVERSITY ANNOUNCES SUPERCOMPUTER PLANS

The Welsh Assembly Government this week announced plans to build one of the world's fastest supercomputers at Swansea University. The tennis-court-sized machine will be developed with funding from the government and with support from IBM. The supercomputer, to be built at Swansea's new clinical college, will be used for biology research, including studies of disease prevention. The project is part of technology efforts by the government of Wales to strengthen the country's economy by 2010. Another initiative aims to make broadband access available throughout Wales. Organizers hope the project will lead to the creation of spin-off companies, attracting even more jobs to the area.

Category 4D *Funny / miscellaneous*

2005-01-21 **video gaming life skills technology learning games Racing Academy cars data performance chat student**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4189411.stm

USING VIDEO GAMES TO TEACH LIFE SKILLS

According to researchers at Futurelab, a British nonprofit investigating how technology can be used for innovative learning, video games have the potential to be highly effective tools for holding students' attention and teaching them about a variety of topics. This sentiment echoes recent findings of the London Institute of Education, which said video games have educational potential. "Games teach life skills such as decision making [and] problem solving," according to Futurelab's Martin Owen. One company, Lateral Visions, saw an opportunity in the educational potential of video games and developed an auto-racing game called Racing Academy. In it, players build and maintain the cars they race, using data to try to improve their performance. The game allows players to use chat rooms to exchange information and ideas, and Owen finds this aspect of the game particularly promising for developing student learning. Futurelab researchers who have been testing the game in two secondary schools have had a positive response from most students, and the researchers have generally been supportive of using the game to enhance learning.

Category 4D *Funny / miscellaneous*

2005-01-21 **California parks wireless SBC Wi-Fi campgrounds Hiking**

EDUPAGE; http://www.reuters.com/newsArticle.jhtml?storyID=7397115

CALIFORNIA PARKS TO GO WIRELESS

Officials from California State Parks this week announced a partnership with SBC Communications to bring Wi-Fi access to 85 of the state's parks over the next six months. Wi-Fi access is already available in the baseball stadium of the San Francisco Giants and in downtown San Jose. The fist state park to have Wi-Fi access will be San Elijo State Beach, near San Diego. Current customers of SBC will be able to access the Wi-Fi service in the state parks for free; others will have to pay $7.95 per day. According to a spokesperson from SBC, the revenue from the service will be split between the company and the state. California State Parks spokesman Roy Stearns said that access will largely be limited to areas in and around visitors' centers and campgrounds. Hiking trails, said Stearns, will not be part of the coverage area.

Category 4D *Funny / miscellaneous*

2005-01-24 **tech companies grid computing consortium Globus Consortium IBM Intel HP Sun Microsystems Nortel Networks corporations academic research organizations Linux**

EDUPAGE; http://www.nytimes.com/2005/01/24/technology/24grid.html

TECH COMPANIES FORM GRID COMPUTING GROUP

A group of leading high-tech companies has announced the formation of a consortium that will work to bring grid computing to corporate enterprises. The Globus Consortium, which includes IBM, Intel, HP, Sun Microsystems, and Nortel Networks, will work to develop grid computing tools geared specifically for corporations, as opposed to existing tools, which typically focus on the needs of academic and research organizations. The consortium's work will be based on software from the Globus Project, which was founded in 1996 by a group of researchers at labs and universities. All of the Globus Project's applications are freely shared and open source. The formation of the new consortium echoes the move of Linux, the open source operating system, from its beginnings in research laboratories into the corporate world. As Ken King, vice president of grid computing at IBM, said, "It starts in government labs and universities and then moves into broader commercial use."

Category 4D *Funny / miscellaneous*

2005-01-25 **word hyperlink Web Liquid Information project connections links CNN menu choices definition**

EDUPAGE; http://www.wired.com/news/culture/0,1284,66382,00.html

MAKING EVERY WORD A LINK

A researcher at University College London wants to change the basic functioning of the Web, allowing readers of Web pages to change those pages--similar to wikis--and making every word a "hyperword." The Liquid Information project is the brainchild of Frode Hegland, who is collaborating with Doug Engelbart, inventor of the computer mouse. Hegland's vision of the Web is one in which consumers of content can also be producers of content. Users would be able to make connections, add links, and change the way information is presented. On an example page, Hegland has modified a CNN Web page such that users can hover over any word to display a menu of choices, including getting a definition of the word, performing a Google search for the word, and highlighting instances of the word in various colors. Hegland said that we need to replace the current Web, which consists of "handmade, one-way links" with what he calls "deep legibility" so that users can "make connections, explicit or otherwise." Hegland conceded that a Web like the one he envisions would require smart users. But, he added, "people are pretty smart. The days of baby steps when everything is shown to users are over."

Category 4D *Funny / miscellaneous*

2005-01-27 **software scan Arabic texts scanners texts language word vowels benefits writings**

EDUPAGE; http://www.nytimes.com/aponline/technology/AP-Arabic-Software.html

DEVELOPING SOFTWARE TO SCAN ARABIC TEXTS

Computer researchers at the University at Buffalo are working on software that will allow computer scanners to read Arabic writing, including handwritten texts. Arabic is a visually complicated language, with some words, for example, having multiple representations. In addition, Arabic characters can be represented differently depending on where they appear in a word, and vowels are often not written at all. Intelligence-gathering efforts after September 11 were hampered by the lack of Arabic-language scanning software, but organizers of the project note other potential benefits, including expanded access to Arabic writings and the ability to digitize vast amounts of Arabic literature and put it on the Web. Venu Govindaraju, director of the Center for Unified Biometrics and Sensors at the University at Buffalo, noted that "The whole Internet is skewed toward people who speak English." Govindaraju said the software will help prevent classic texts in Arabic from "disappear[ing] into oblivion."

Category 4D *Funny / miscellaneous*

2005-02-07 **MIT Media Lab inexpensive laptop education text books TV telephone games machine applications operating system**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4243733.stm

MEDIA LAB FOUNDER PROPOSES INEXPENSIVE LAPTOP FOR EDUCATION

Nicholas Negroponte is developing a sub-$100 laptop computer that he said could be a vital educational tool for children in developing countries. Negroponte, the chairman and founder of MIT's Media Lab, said the idea comes from pilot programs in Maine, in which schoolchildren were given laptops, and in Cambodia, where he and his wife have set up two schools and given the students laptops. Children can use the devices as text books, according to Negroponte, who said such computers could become "very important to the development of not just that child but now the whole family, village, and neighborhood." Negroponte noted that in Cambodia, the students use them not just as text books but also as "a TV, a telephone, and a games machine." Building a laptop for less than $100, he said, will require deleting extraneous applications and running a Linux-based operating system. "[I]f you can skinny it down," he said, "you can gain speed and the ability to use smaller processors and slower memory." Negroponte hopes to start distributing the machines by the end of 2006. BBC, 7 February 2005

Category 4D *Funny / miscellaneous*

2005-02-14 **trading color sound visually impaired graphics blind graduate Cornell University colored maps**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4257961.stm

TRADING COLOR FOR SOUND FOR VISUALLY IMPAIRED

Working with a graphics specialist and another student, a blind graduate student at Cornell University has developed a computer application that translates colors into sounds, allowing him to read and understand colored maps of the atmosphere. Victor Wong, who has been blind since age seven, said he recognized the need for such a tool for his own studies, as well as for blind scientists generally. The application translates the colors of digitally created images into one of 88 notes, with blue at the low end and red at the high end. Users manipulate a stylus on a tablet to "read" the images through sound. Wong believes that because he formerly could see, his "color memory" may afford him the ability to visualize the colors and use the application in a way that someone who has never been able to see could not. The software remains primitive, but Wong said he hopes it can one day be developed to give blind people access to photographs and other images.

Category 4D *Funny / miscellaneous*

2005-02-14 **UW project graphics accessible researchers blind visually impaired National Science Foundation Tactile Graphics Project science engineering software printers**

EDUPAGE;
http://www.registerguard.com/news/2005/02/14/b3.wa.research.0214.html

UW PROJECT WORKS TO MAKE GRAPHICS MORE ACCESSIBLE

Researchers at the University of Washington are looking for ways to make graphics accessible to blind or visually impaired students. Funded in part by a grant from the National Science Foundation, the Tactile Graphics Project aims to open up science and engineering to students with visual disabilities, who have traditionally been largely left out of such fields due in part to the difficulty of "seeing" graphics with their hands. Researchers in the project are working with blind students from the university and local high schools to develop new and effective means of representing graphics and figures in a way that the blind can understand clearly. Such representations must be sufficiently detailed to be useful but not so complex as to be confusing. Tactile printers, or embossers, is one technology that already exists, but because the software is outdated and difficult to learn, the printers are not extensively used, according to Melody Ivory-Ndiaye, an assistant professor at the university's Information School.

Category 4D *Funny / miscellaneous*

2005-02-28 **pilot distributes handhelds Kenya school organization EduVision textbooks information satellite text images questions Google**

EDUPAGE; http://news.bbc.co.uk/2/hi/technology/4304375.stm

PILOT PROGRAM DISTRIBUTES HANDHELDS IN KENYAN SCHOOL

A pilot project run by an organization called EduVision is distributing handheld computers to schoolchildren in western Kenya to replace aging, outdated textbooks. In the program, students receive devices called E-slates, which receive transmissions from a base station in the school. The base stations receive and process information delivered by satellite and transmit text, images, and study questions to the E-slates. EduVision's Matthew Herren explained that the system is very simple to set up but that "getting feedback or specific requests from end users is difficult" because the system uses one-way connections. Herren said organizers of the program are working with Google, which has begun an initiative to digitize millions of public-domain texts and make them available online. Putting those resources into the handheld program, said Herren, would give "every rural school in Africa ... access to the same libraries as the students in Oxford and Harvard."

Category 4D *Funny / miscellaneous*

2005-04-02 **Pentagon US government DARPA computer science research funding diverted universities**

EDUPAGE; http://www.nytimes.com/2005/04/02/technology/02darpa.html

DARPA FUNDS DIVERTED FROM UNIVERSITIES

Confirming rumors among academics at a number of colleges and universities, the Pentagon's Defense Advanced Research Projects Agency (DARPA) has acknowledged a shift away from university projects. DARPA has long been a supporter of broad-ranging, long-term research initiatives at institutions of higher education, and many credit such programs with many of the innovations that underpin today's household technologies. In seeking shorter-term projects with more concrete deliverables, however, DARPA has significantly cut back funds for university projects. Since 2001, the portion of DARPA's relatively stable budget allocated to university projects has dropped by nearly 50 percent. Many in the research community fear that the shift away from basic, open-ended research will result in slower technological progress. Ed Lazowska, a computer scientist at the University of Washington and co-chairman of the President's Information Technology Advisory Committee, said, "Virtually every aspect of information technology upon which we rely today bears the stamp of federally sponsored university research." He characterized DARPA's change in focus as "killing the goose that laid the golden egg." New York Times, 2 April 2005 (registration req'd)

Category 4D *Funny / miscellaneous*

2005-04-07 **ACM ICPC international programming contest US falling behind computer science industry**

EDUPAGE; http://news.zdnet.com/2100-9595_22-5659116.html

CODING CONTEST SHOWS U.S. STUDENTS FALLING BEHIND

At this year's Association for Computing Machinery International Collegiate Programming Contest, the University of Illinois's tie for 17th place was the best result for any U.S. team, representing the worst performance for U.S. institutions in the 29 years of the competition. Many observers believe the result is indicative of a variety of factors that have resulted in a striking shift in technological preeminence away from U.S. schools and companies. As recently as 1997, the United States came out on top, when a team from Harvey Mudd College won the competition. David Patterson, president of the Association for Computing Machinery and a computer science professor at the University of California, Berkeley, noted, "The U.S. used to dominate these kinds of programming Olympics." Others pointed out that applications from outside the United States to computer science and other technology programs at U.S. graduate schools have dropped lately. ZDNet, 7 April 2005

Category 4D *Funny / miscellaneous*

2005-04-15 **telephone toll-free phone number rollover process vetting checking verification re-use**

RISKS; http://tinyurl.com/4ba24 23 84

SAFE BOATING = PHONE SEX?

Kark Klashinsky reported that in New Brunswick, Canada, the federal government's toll-free number originally assigned to a safe-boating information line was recycled to a phone-sex company. He notes, "The risk here is that the "recycle" process does not appear to check that the prior use of a toll-free number doesn't conflict in some social/moral way with the new user's intended use of the number. Oh, well, it could have been worse… at least the number wasn't previously used for Mattel's _Barbie_ hotline."

Category 4D *Funny / miscellaneous*

2005-04-22 **report US college university computer science degree pursuant decline CRA**

EDUPAGE; http://news.com.com//2100-1022_3-5681438.html

FEWER COLLEGE STUDENTS PURSUING COMPUTER SCIENCE DEGREES

A new report from the Computing Research Association (CRA) shows a significant drop in the number of college freshmen in the United States who say they plan to major in computer science. The CRA looked at data from the Higher Education Research Institute at the University of California at Los Angeles and found that between fall of 2000 and fall of 2004, interest in computer science fell by more than 60 percent and is now 70 percent below its all-time high. Interest among women has fallen even further, said the CRA, dropping 80 percent since 1998 and 93 percent since 1982. The CRA also conducted surveys of higher education institutions and came up with similar results. The report goes on to suggest that the United States will have difficulty meeting the demand for IT workers in coming years, increasing the gap with countries including India and China that are producing larger numbers of computer science graduates. "Freshmen interest levels at any given point have been an accurate predictor of trends in the number of degrees granted four to five years later," according to the report. CNET, 22 April 2005

Category 4D *Funny / miscellaneous*

2005-07-01 **quantum computing information processing progress HP DARPA**

EDUPAGE; http://www.nytimes.com/2005/07/01/technology/01hewlett.html

HP CLAIMS PROGRESS ON QUANTUM COMPUTING

Researchers at HP said they have taken a significant step in the development of a functioning quantum computer, and the Pentagon's Defense Advanced Research Projects Agency (DARPA) is contributing as much as $10 million to support the project. As opposed to the transistors--which can register either 1 or 0--that underlie today's computer processors, quantum computing is based on the physics of subatomic particles, allowing so-called "qubits" to represent both 1 and 0 simultaneously. The result could be vastly expanded processing power of quantum computers compared to those based on transistors. The DARPA funding will be used by the researchers to construct a functioning prototype. One researcher commented that to perform a single demonstration will not be difficult; the challenge lies in doing it reliably and "in a way that will allow us to do quantum information processing." Other quantum physics researchers question the basis of the HP team's approach, saying that fundamentally different approaches to quantum computing hold more promise. New York Times, 1 July 2005 (registration req'd)

Category 4D *Funny / miscellaneous*

2005-07-15 **science engineering higher education graduates US losing group internationally**

EDUPAGE; http://www.insidehighered.com/news/2005/07/15/science

U.S. LOSING GROUND IN SCIENCE AND ENGINEERING

Confirming the suspicions of many, a new report from the National Bureau of Economic Research indicates that the United States is steadily losing ground to a number of other countries, particularly China, in the number of PhDs it awards in science and engineering fields. In 1970, nearly one-third of the world's college students attended a college or university in the United States, and more than half of the science and engineering PhDs were awarded by U.S. schools. A number of global factors contributed to those numbers, making them artificially high. Since that time, however, higher education around the world, and especially programs in science and engineering, has greatly expanded, leaving the United States with just 14 percent of the world's college students by 2001. According to the report, China could surpass the United States as early as 2010 in the number of science and engineering PhDs it awards. Inside Higher Ed, 15 July 2005

Category 4D *Funny / miscellaneous*

2005-07-21 **science graduates shortage bill US Senate Technology Talent Act**

EDUPAGE; http://www.internetnews.com/bus-news/article.php/3521851

SENATORS TO ADDRESS SHORTAGE OF SCIENCE GRADS

U.S. Senators said they will propose a bill next week to increase federal funding of multidisciplinary research and support for "revolutionizing" manufacturing technologies and processes. The legislation will also increase spending for the Technology Talent Act, which provides grants to colleges and universities to increase the number of science and engineering graduates. The proposed legislation is based on the 2004 National Innovation Initiative Report released by the Council on Competitiveness. That report calls for creating 5,000 new federally funded graduate fellowships, reworking immigration laws, and building 10 "innovation hot spots." Internet News, 21 July 2005

Category 4D *Funny / miscellaneous*

2005-08-15 **research University of California Berkeley Internet search technology improvement**

EDUPAGE; http://news.com.com/2100-1038_3-5831050.html

BERKELEY PROJECT AIMS TO CREATE BETTER SEARCH TECHNOLOGIES

Researchers at a new center being developed at the University of California at Berkeley will study search technologies in an effort "to solve the problems that have been engendered by the success of search," according to Robert Wilensky, the director of the center. Among the topics of study will be privacy, fraud, multimedia search, and personalization. Plans for the new center have not been finalized, but organizers said it will be an interdisciplinary effort, including 20 or so faculty from various departments. Wilensky said that having an environment with so many researchers from differing fields of study results in "something bigger than its parts." The new research center will encourage commercial search companies to participate. Higher education has played a prominent role in the development of search technologies. Both Google and Yahoo were started at Stanford University, while Lycos was born at Carnegie Mellon University. Other institutions around the country are also working on projects to further develop search technologies. CNET, 15 August 2005

Category 4D *Funny / miscellaneous*

2005-08-30 **hurricane Katrina disaster communications cut down new technology search rescue sensor system wiki networks**

DHS IAIP Daily; http://msnbc.msn.com/id/9131498/

SCIENTISTS BRING TECHNOLOGY TO POST-KATRINA DISASTER SCENE

In Hurricane Katrina's wake, researchers are bringing cutting-edge technologies to the disaster area. The search-and-rescue tools include devices and software that can turn walkie-talkies into Internet grids when the phones are out, robots and aerial mini-planes that can look for signs of life amid the wreckage, and sensor systems that can sniff out public health threats in the storm's aftermath. Cisco Systems is setting up mobile communication kits and wiki-based networks to deal with Katrina's information overload. "It's not us saving people. It's us getting the technology to the people who will use it to save people," explained Robin Murphy, a professor at the University of South Florida who directs the Institute for Safety Security Rescue Technology. Murphy and her USF team are heading to New Orleans to link up with Louisiana State University's Fire Emergency Training Institute and put their tools to the test.

Category 4D *Funny / miscellaneous*

2005-09-12 **hurricane Katrina disaster search research University of South Florida robots**

DHS IAIP Daily; http://www.physorg.com/news6383.html

UNIVERSITY OF SOUTH FLORIDA DEPLOYS MINI UNMANNED SEARCH AIRCRAFT AFTER KATRINA

The University of South Florida's Center for Robot-Assisten Search and Rescue (CRASAR) team worked with other rescuers in Mississippi immediately following Hurricane Katrina. They used two types of small unmanned aerial vehicles (UAVs), one fixed wing and one helicopter. Within two hours of deployment the responders had date form the UAVs showing there were no survivors trapped in the Pearl River. In addition, the UAV reported the flood waters from the river were not posing any additional threats to the community.

Category 4D *Funny / miscellaneous*

2005-10-05 **Google Sun partnership Microsoft competition**

EDUPAGE; http://www.siliconvalley.com/mld/siliconvalley/12823481.htm

GOOGLE AND SUN ANNOUNCE PARTNERSHIP

Google and Sun Microsystems have announced a partnership that many see as a joining of forces against Microsoft. Sun has long been a direct competitor with Microsoft, and most analysts believe Google has aspirations to compete with the software giant. Few specifics were released about the new arrangement. Google, which already buys Sun hardware, will expand those purchases, and Sun customers who download Java will have the option of also downloading Google's toolbar. Beyond those changes, most speculation about the deal concerns Sun's OpenOffice, an open source application that competes with Microsoft's Office suite of software. The companies said they will jointly develop OpenOffice, though some analysts expect Google to take primary responsibility for the work. John Rymer, an analyst with Forrester Research, said he believes Google will not simply redistribute OpenOffice. "When [Google does] something," he said, "it has to be cool. It has to go further than Microsoft Office." The deal is also a reunion of sorts for Sun CEO Scott McNealy and Google CEO Eric Schmidt, who worked together at Sun for 14 years. San Jose Mercury News, 5 October 2005

Category 4D *Funny / miscellaneous*

2005-10-13 **science technology research development R&D US leading position loss**

EDUPAGE; http://news.com.com/2100-11395_3-5894854.html

PANEL WARNS U.S. NOT KEEPING PACE IN SCIENCE

A new report says that the United States stands to lose its leading position in science and research unless efforts are made to strengthen support for educational and other scientific programs. The panel that wrote the report was convened by the National Academies and included representatives from corporations and higher education, as well as Nobel laureates and former presidential appointees. The panel pointed to the narrowing scientific gap between the United States and countries such as China and India; recent results showing declining performance among U.S. students in science and math compared with students around the world; and economic factors that work against U.S. scientific interests. Among the report's recommendations are funding scholarships to support 10,000 students annually to pursue careers in teaching math and science; allocating money for 30,000 students per year to study science, math, and engineering; and relaxing visa regulations to allow international students to find employment in the United States after they graduate. CNET, 13 October 2005

Category 4D *Funny / miscellaneous*

2005-10-27 **GPS data error human judgement override accident consequences legal liability**

RISKS 24 10

WHICH DO YOU BELIEVE: COMPUTERS OR REALITY?

Mike Scott contributed this chilling tale of excessive dependence on computerized information:

>My son was being driven by a friend in London. The friend's car was equipped with some sort of GPS navigation. They were driving eastbound along the north side of the River Thames, intending to cross at Tower bridge to a destination on the south side of the river. The GPS said "turn right" when they reached the bridge. The only snag is that this is a one-way system. To cross the bridge you turn left, *away* from the bridge, and drive right round the block. Unfortunately, said friend [paid] more attention to the GPS than the road signing, and very nearly collided with a car coming the other way.<

Mr Scott wondered about legal liability of the GPS navigator makers if there had been an accident.

[Lightly edited by MK]

Category 4D *Funny / miscellaneous*

2005-10-28 **MIT Nokia research laboratory lab CSAIL**

EDUPAGE; http://www.theregister.com/2005/10/28/mit_nokia_joint_research/

MIT AND NOKIA TO FORM RESEARCH LAB

MIT and Nokia announced a venture to create a joint research lab, to be called the Nokia Research Center Cambridge. The lab is part of MIT's Computer Science and Artificial Intelligence Laboratory, and researchers there will study "the state of the art in mobile computing and communications," according to a statement from the two organizations. Specifically, researchers will focus on low-power hardware and user interfaces, in particular those that are based on speech. More broadly, the center will address questions concerning software architecture, wireless technologies, and methods of managing information. The center will comprise about 20 researchers from each of the two organizations and will be directed by James Hicks of the Nokia Research Center. The Register, 28 October 2005

Category 4D *Funny / miscellaneous*

2005-12-06 **Internet Web browser Firefox plug-in George Mason University research bibliography sources citing bookmarking**

EDUPAGE; http://chronicle.com/daily/2005/12/2005120602t.htm

GEORGE MASON DEVELOPS ACADEMIC BROWSER ADD-ON

Researchers at George Mason University are developing a plug-in for the Firefox browser that will help academics organize sources and properly cite them. The tool is designed to harvest bibliographic information from online sources and organize it for someone doing research on the Web. Assuming the bibliographic elements are formatted in a way the software can recognize, the application will parse title, author, and other information and correlate it with the source. Daniel J. Cohen, assistant professor of history and one of the developers, said it can be thought of as "incredibly smart bookmarking…. You're not just bookmarking the page, but you're automatically [capturing]…all that info that scholars want to save." Unlike commercial products that organize sources, the new application will tie directly into the browser, eliminating the step of manually collecting citation details. The open source application is expected to be completed next year and will be available for no charge from George Mason's Web site. Cohen said he believes the application will make unintentional plagiarism less likely than if a researcher were keeping sources organized manually.
Chronicle of Higher Education, 6 December 2005 (sub. req'd)

Category 4D *Funny / miscellaneous*

2005-12-11 **China overtake US information technology IT good supplier**

DHS IAIP Daily;
http://www.nytimes.com/2005/12/11/business/worldbusiness/11c nd−
hitech.html?adxnnl=1&adxnnlx=1134398046−RvJh6wxlZ7Zf7UdIW s/ljg

CHINA OVERTAKES U.S. AS SUPPLIER OF INFORMATION TECHNOLOGY GOODS

After almost a decade of explosive growth in its electronics sector, China has overtaken the U.S. as the world's biggest supplier of information technology goods, according to a report by the Organization for Economic Cooperation and Development. Data in the report, published on Monday, December 12, show that China's exports of information and communication technology increased by more than 46 percent to $180 billion in 2004 from a year earlier, easily outstripping for the first time U.S. exports of $149 billion, which grew 12 percent from 2003. The figures compiled by the Organization for Economic Cooperation and Development, based in Paris, also reveal that China has come close to matching the U.S. in the overall value of its trade in information and communications technology products. The value of China's combined exports and imports of such goods soared to $329 billion in 2004 from $35 billion in 1996. Over the same period, the value of American information technology trade expanded at a slower rate, to $375 billion from $230 billion. Organization for Economic Cooperation and Development's data: http://www.oecd.org/document/8/0,2340,en_2649_201185_3583309 6_1_1_1_1,00.html

---

Category 4D *Funny / miscellaneous*

2005-12-16 **Wikipedia free online encyclopedia content evaluation Nature Britannica science accuracy**

EDUPAGE; http://networks.silicon.com/webwatch/0,39024667,39155109,00.htm

STUDY EVALUATES WIKIPEDIA CONTENT

According to a research study published in the journal Nature, Wikipedia compares favorably with the Encyclopedia Britannica in the accuracy of its information despite recent criticisms of its content and methods. The Nature study compared articles from both Web sites on a wide range of topics, asking field experts to review the accuracy of the entries. Serious errors (such as misunderstandings of vital concepts) were evenly distributed between the two encyclopedias, with four serious errors each. As for errors of fact, omissions, or misleading text, Wikipedia had 162 such errors and Britannica had 123. The study is the first to use peer review to compare the accuracy of the two sources' coverage of science. Silicon.com, 16 December 2005

Category 4D *Funny / miscellaneous*

2006-03-16 **hackers competition Windows XP run Intel Mac**

DHS IAIP Daily; 23
http://www.macworld.com/news/2006/03/16/xponmac/index.php

HACKERS GET INTEL MAC TO RUN WINDOWS XP.

A contest to see who could get Windows XP working first on an Intel Mac has been won, according to the contest's coordinator, Colin Nederkoorn. Getting Windows XP to work on the Mac is not a plug and play process. According to the documentation included with the file download provided on Nederkoorn's Website, users must create an install CD themselves using a PC equipped with a CD-R drive, Microsoft's Windows XP SP 2 CD-ROM and Nero CD burning software. Step-by-step instructions for creating the disc are included. Users must also reformat and repartition their Intel Mac's hard disk drive to include a separate partition where Windows XP can be installed, then go through a multi-step process to make sure the software is installed properly and the Mac can recognize it. Once that's done, users will be able to switch between Mac OS X and Windows after rebooting the Mac. To load Windows XP on an Intel Mac: http://onmac.net/

Category 4D *Funny / miscellaneous*

2006-05-03 **Iraq online library US Department of Defense DoD weapons systems research**

EDUPAGE; http://chronicle.com/daily/2006/05/2006050301t.htm 23

ONLINE LIBRARY PART OF INTERNATIONAL SECURITY

A group of academics has partnered with the U.S. Department of Defense to develop an online library in Iraq that organizers hope will help the country hold on to its senior scientific researchers, many of whom have considerable experience developing weapons systems. Following the U.S. invasion of Iraq, 85 percent of the country's university libraries were destroyed or looted. Organizers of the online library said that although many in the country lack reliable Internet access, an online library was nonetheless the fastest, least expensive way to provide access to scientific material. The Iraqi Virtual Science Library is initially funded by the Defense Department's Defense Threat Reduction Agency and runs on U.S. government servers, though officials said they hope to turn control of the library over to Iraqis within the next few years. Fourteen publishers are participating in the program, offering discounts of as much as 97 percent over regular subscription prices. The Iraqi Virtual Science Library provides access to articles from about 17,000 academic journals. A representative of Springer, one of the publishers involved, said that because of the discounts, the Iraqi library has more content than most U.S. libraries, which must "cherry-pick" what they will purchase.
